TEST REPORT

Tolly.

#211125
August 2011
Commissioned by Sophos Ltd.

Sophos Endpoint Security and Control v9.7

Anti-virus Performance in VMware ESX Virtual Environments

Executive Summary

As IT architects scale deployments of virtual desktop infrastructure (VDI) solutions, they must be aware of the resource requirements of "always on" and high-use components such as endpoint security systems. In virtual environments, vendors can implement their solution as a client-based agent, where all processing for each client takes place on the client, a virtual appliance that handles the anti-virus (AV) workload or, possibly, some hybrid of the two approaches.

Sophos Ltd. commissioned Tolly to benchmark the performance of its new Sophos Endpoint Security and Control v9.7 within virtual environments. Specifically, this testing focused on the system resource requirements of the Sophos client-based agent when performing on-demand/on-access scanning and virus signature definition update tasks.

TEST HIGHLIGHTS

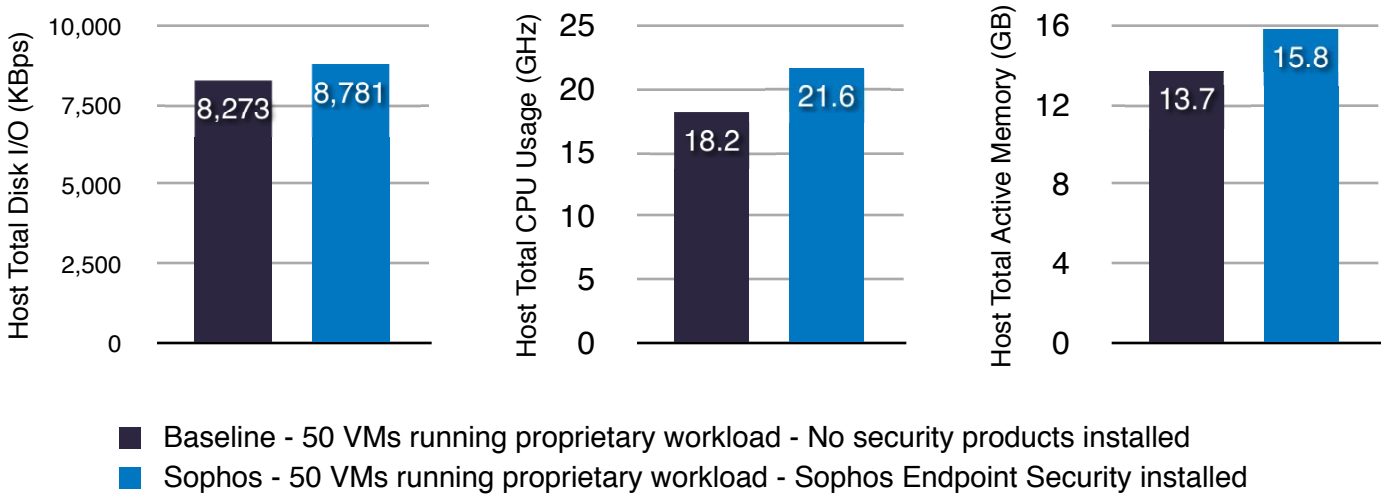
Sophos Endpoint Security and Control v9.7:

1. Demonstrated minimal impact on system and CPU usage under on-access scans compared to baseline
2. Executed key functions such as on-demand scan and signature update in a 50 VM scenario without causing an AV "storm"
3. Provided full endpoint security functionality in virtualized environments without requiring additional licensing

On-Access Anti-Malware Scan Resource Utilization

VMware ESX 4.1 Host Activity

As reported by VMware vCenter (Lower numbers represent lower load on system)



Source: Tolly, July 2011

Figure 1

Executive Summary (con't)

In the past year, Tolly has run a series of tests, across various vendor products that focused on measuring the resource impact of running endpoint security solutions in a virtualized, VMware environment.

While the test suite is evolving over time, Tolly notes that the tests run in the present project use a methodology very similar to the tests found in Tolly document #211123. Though the individual data in this report cannot be directly compared to Tolly document #211123 due to hardware differences, the similarities in methodology produces comparable results when assessing the relative impact over baseline. (Please see the Test Methodology section for details.)

Tolly engineers found that the Sophos solution was able to complete all of the tests involving 50 VMs without triggering any AV "storms". (Analysts use the term "storm" to describe a situation where many virtual machines initiate resource-intensive tasks simultaneously. This detracts significantly from the resources available to other virtual machines on the same host.)

While AV storms can result in a server becoming unusable, the performance of on-access scanning will impact users throughout their workdays. Typically, AV software provides real-time protection by scanning a file every time it is open or saved. To provide the best day-to-day user experience, a low-impact scanner is desirable.

For on-access scanning, Tolly engineers found that the Sophos solution increased the baseline disk I/O utilization for running the proprietary workload by only 6%. (See Figure 1).

Sophos Ltd

Sophos Endpoint Security and Control 9.7

VMware Anti-virus System Performance

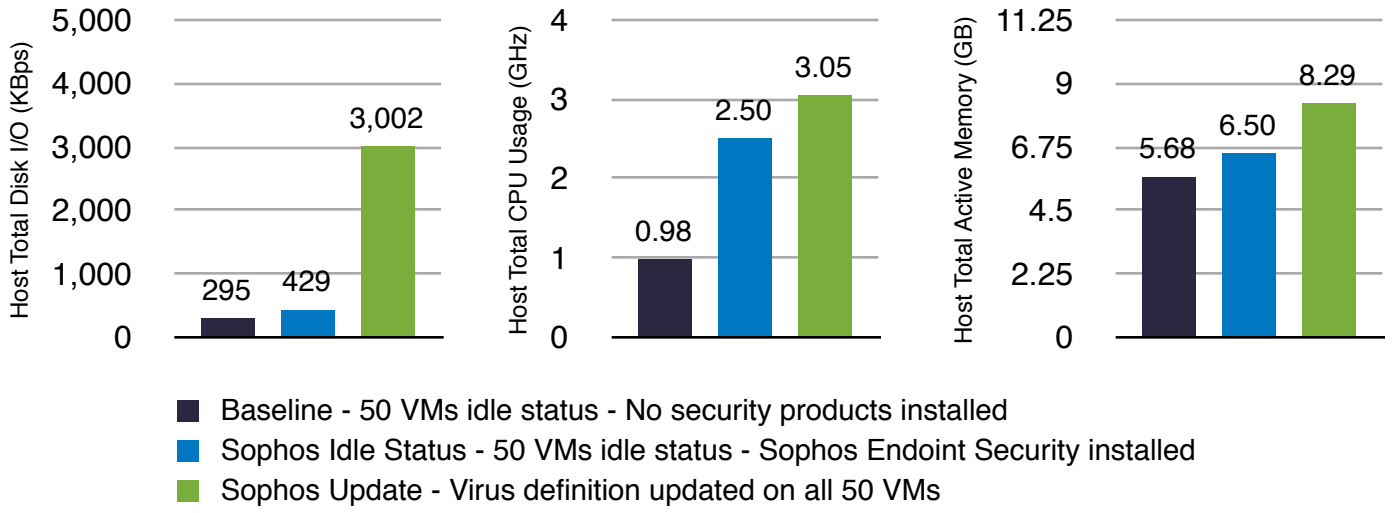
Tested July 2011

Testing encompassed various scanning and system update functions and was performed using 50 Microsoft Windows 7 (64-bit) virtual machines. Tolly engineers measured critical system resources, disk input/output (I/O), CPU consumption and

Virus Definition Update Resource Utilization

VMware ESX 4.1 Host Activity

As reported by VMware vCenter (Lower numbers represent lower load on system)



Note: 50 VMs were powered up randomly during a 1 hour period prior to the commencement of the definition update. Update interval was set up as 1 hour in the Sophos management console. The total test duration was 1 hour and 15 minutes to allow all VMs finished the virus definition update.

Source: Tolly, July 2011

Figure 2

memory usage at both the virtual machine and VMware host (physical server) levels.

The Sophos solution provides real-time constant scanning, as well as on-demand options with their Sophos Virtualization Scan Controller (SVSC), thus avoiding excessive resource usage and AV "storms".

Sophos Endpoint Security and Control v9.7 demonstrated that it provides low impact on-access scanning and signature update services. The concurrent scanning is able to be optimized via configuration settings to ensure scans are completed in a particular time frame, for example "quiet hours," without compromising the host's performance or stability.

This evaluation found that the Sophos approach utilizing a client-based agent performs as promised, with very low impact on on-access performance and proven ability to avoid AV "storms," all with the full protection offered by running anti-virus on each client.

Test Results

On-Access Anti-Malware Scan

Throughout the work day, the endpoint security solution is invoked automatically to scan files and other system resources as they are accessed.

For this test, a script exercising various Microsoft Office functions and file transfers was run on all 50 VMs and resources were measured at a VMware host level. (See Figure 1.)

Compared with a baseline where the workload was run without any endpoint security product installed, Sophos demonstrated resource overhead that never exceeded a 20% increase.

The increase in disk I/O was minimal at 6%. Overall demand for memory increased by 15% and for CPU by 18.68%.

Signature Update

Endpoint security systems periodically retrieve updated information, referred to as "signatures," that assist in effectively identifying and eliminating new threats.

IT administrators are rightly concerned with the performance impact on VMware host servers if multiple signature updates are run simultaneously.

Tolly engineers confirmed that the signature update process ran effectively and to completion without triggering an anti-virus storm. Engineers measured the resource impact of each VM's update on the host. (See Figure 2.) The Sophos approach for avoiding an AV storm is separating the power on time of each VM. Then, each VM will check-in to the Sophos Enterprise Console to see whether there is a new update with a configurable interval.

Tolly configured the update interval as 1 hour and then as "random-start" all 50 VMs in 1 hour. As a result, all 50 VMs were projected to update in 1 hour with different start times. Tolly engineers verified that the virus definition update process on each VM took 1 to 2 minutes.

Compared with the baseline, disk I/O is understandably high given that the purpose of the task is to retrieve signature data to be stored locally on the VM.

During this task, the increase over the baseline of an idle system with the Sophos solution installed is 22% for CPU and 27.5% for memory. No AV storm was observed.

Sophos Virtualization Scan Controller

Sophos Virtualization Scan Controller (SVSC) management software is designed to overcome resource issues when running concurrent scheduled scans across virtual machines, and is accessible free of charge to existing Sophos customers.

In this Tolly test, each VM took 20 to 30 minutes to finish the full scan. Administrators can configure the number of concurrent scanning VMs and other parameters in SVSC to balance the total amount of time to finish scanning all VMs and the performance impact on the host.

Source: Tolly, July 2011

In a live environment, configuring all virtual machines to perform scheduled scans at the same time can cause a large resource overhead for the physical host machine. The Sophos Virtualization Scan Controller helps to avoid this by giving administrators the flexibility to configure their scanning options to spread the scanning load, for example:

- Time windows for scans (e.g. Earliest scan start time and latest scan start time)
- Days of the week on which scans should be performed
- Maximum number of concurrent scans

Source: Sophos Ltd.

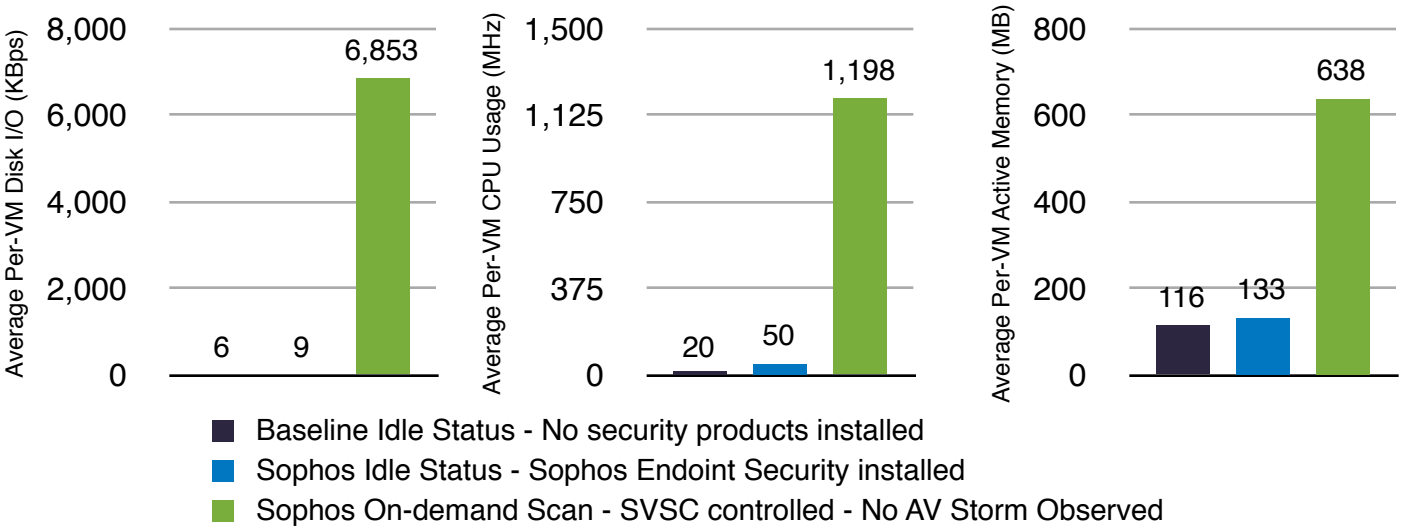
On-Demand Anti-Malware Scan

For any number of reasons, an IT security administrator may decide to initiate full scans on dozens of clients "on demand." Such tasks can be resource-intensive by nature, and if run simultaneously, place an unacceptable load on the VMware host system and degrade the overall virtualization system performance.

On-Demand Anti-Malware Scan Resource Utilization

VMware ESX 4.1 Average Per-VM Performance

As reported by VMware vCenter (Lower numbers represent lower load on system)

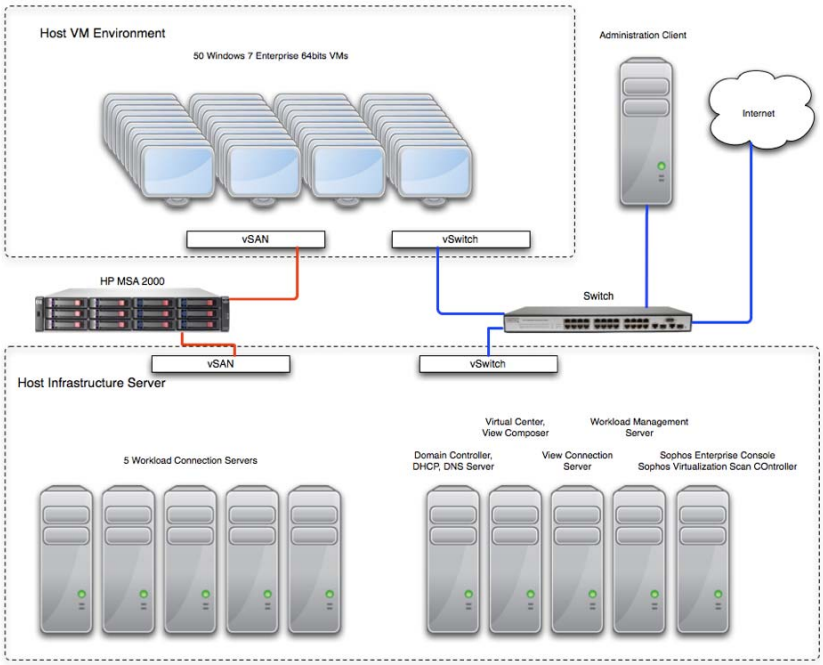


Note: 1. Windows 7, 64-bit installations. Systems instructed to scan 50 VMs. Results average of 10 VMs.
2. Sophos Virtualization Scan Controller (SVSC) was used on the Sophos management server to scan all 50 VMs one at a time. The scan time on each VM was between 20 to 30 minutes. No AV storms observed during the test.
3. As the number of concurrent scanning VMs can be configured in SVSC, single VM's on-demand scan impact is represented. Administrators can configure the SVSC based on their host environment.

Source: Tolly, July 2011

Figure 3

Virtualized Anti-virus Test Environment



Source: Tolly, July 2011

Figure 4

Protection and Performance: Client-Based Scanning Model vs. Central Security Appliance

There are two fundamental ways that security software tends to be implemented, either as a client-based agent or as a virtual appliance (where protection is provided centrally).

While both models have strengths and weaknesses, the fundamental difference is where the scanning protection takes place. With the client-based agent, each VM has its own dedicated scanner, and this dedicated scanning resource is tasked with protecting only one VM. The result of this is faster real-time protection as there is no need for an-access scanning tasks to queue.

With the central security appliance, there is only one scanning agent to provide on-access scanning protection. For example, for the 50 virtual machines referenced in this report, there is one scanner. Therefore there may be occasions where scanning slows as a result of a) file information being sent between the virtual machines and the central scanning appliance and b) files being queued for scanning.

The central scanning appliance model, by design, should provide lower impact on updating (there is only one scanning agent to update) and naturally avoids anti-virus (AV) storms by carrying out full, on-demand scans one virtual machine at a time.

Some vendors, such as Sophos have refined their client-based agent model to provide a way for on-demand scans to be scheduled in order to avoid AV "storms". Sophos uses a flexible (and free) add-on called the Virtualization Scan Controller to achieve this. Utilizing this hybrid approach appears to match the main benefit offered by the centralized scanning appliance model (i.e. to avoid AV "storms"), while retaining the benefit of each virtual machine having a dedicated scanner for fast on-access protection.

Source: Sophos Ltd.

System Under Test

Vendor	Product	Components	Implementation
Sophos Ltd.	Endpoint Security and Control v9.7	Sophos Enterprise Console v4.7 Sophos Virtualization Scan Controller v1.0 Sophos Anti-Virus v9.7 Sophos Client Firewall v2.7	Client agent solution. Sophos Virtualization Scan Controller (SVSC) manages the number of concurrent scanning VMs.

Source: Tolly, July 2011

Table 1

VMware Performance Host Testbed Components

Component	Version/Build
VMware ESX	4.1.0 build 348481
VMware vCenter Server	4.1.0 build 258902
VMware View Composer Server	2.6
VMware View Connection Server	4.6.0 build 366101
Server Hardware	2x Xeon x5680 (Hexacore) running at 3.33GHz with 192GB of DDR3 RAM (Total of 24 logical cores)
Storage Area Network	HP StorageWorks MSA connected via 4GB FibreChannel
Guest VM Resources	1GB RAM and 1 vCPU
Guest Operating System	Microsoft Windows 7 Enterprise 64-bit

Source: Tolly, July 2011

Table 2

The Sophos Virtualization Scan Controller allows scans to take place one at a time (as with the virtual appliance solution) but also permits concurrent scans, thus allowing administrators to optimize their system to complete scans in as short amount of time as possible without seriously impacting performance.

For this test, each system was instructed to perform an on-demand scans on all 50 VMs. The Sophos Endpoint Security and Control v9.7 is able to handle on-demand scanning initialization on multiple VMs at once without the risk of an AV Storm.

Test Methodology

All tests were based on tests found in Tolly document 211123. The goal and methodology of each test were the same. Execution was modified to account for the

manner in which Sophos handles requests from multiple VMs. See Table 2 for details of the VMware virtual server environment used in this test.

About Tolly...

The Tolly Group companies have been delivering world-class IT services for more than 20 years. Tolly is a leading global provider of third-party validation services for vendors of IT products, components and services.
You can reach the company by email at sales@tolly.com, or by telephone at +1 561.391.5610.

Visit Tolly on the Internet at:
http://www.tolly.com

All 50 Windows 7 (64-bit) virtual machines were deployed as linked clones using VMware View 4.6. See Table 1 for details of the system under test.

On-Demand Anti-Malware Scan

All VMs were in idle status. Sophos On-demand Scan tool was used on the Sophos Enterprise Console server. Administrators can configure the number of concurrent scanning VMs and the amount of time to allow each VM to scan.

Tolly engineers used the default setting which allows 1 concurrent VM to scan and 30 minutes for each VM to scan. The tool then monitored the scan time for each VM and the time was adjusted to allow each VM to complete the scan. Engineers isolated each VM run and averaged that data to generate the per-VM results.

On-Access Anti-Malware Scan

Each VM was running the same workload with Microsoft Word, Excel, PowerPoint, Internet Explorer, Adobe Reader and network file transfers. The test duration was 40 minutes.

Signature Update

All VMs were in idle status. The update interval for each client was configured as 1 hour in the Sophos Enterprise Console. All 50 VMs were powered on randomly within 1 hour. The duration of the entire test was 1 hour and 15 minutes.

211125-tp-1-kt-jt-yx-mts - 26Aug2011-VerR