Anti-Virus Comparative

Comparison of Anti-Malware Software for Storage 2016

Language: English
March 2016

Last Revision: 24th August 2016

Commissioned by Kaspersky Lab

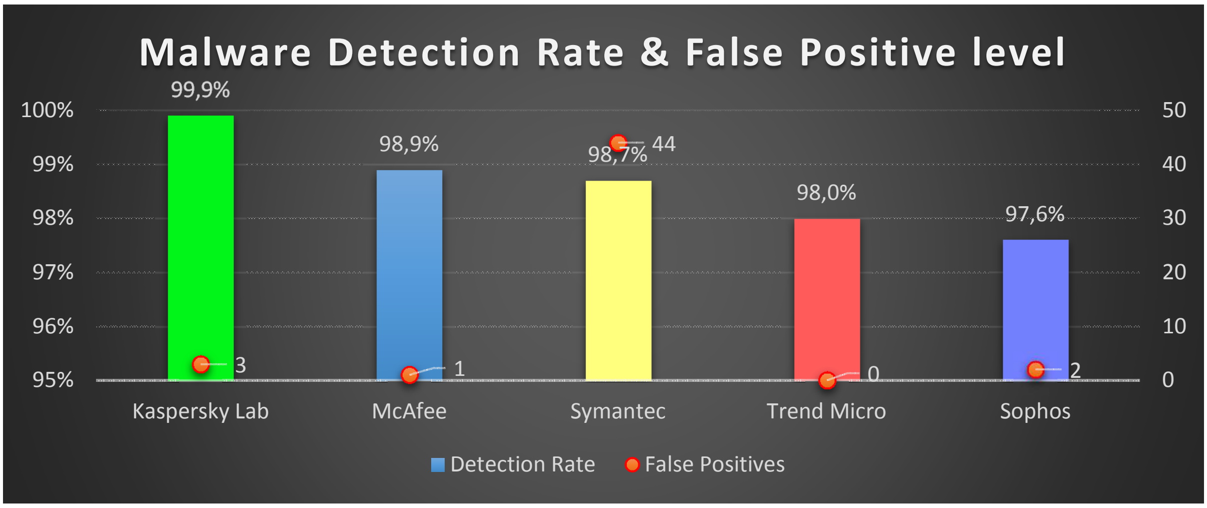
www.av-comparatives.org

Table of Contents

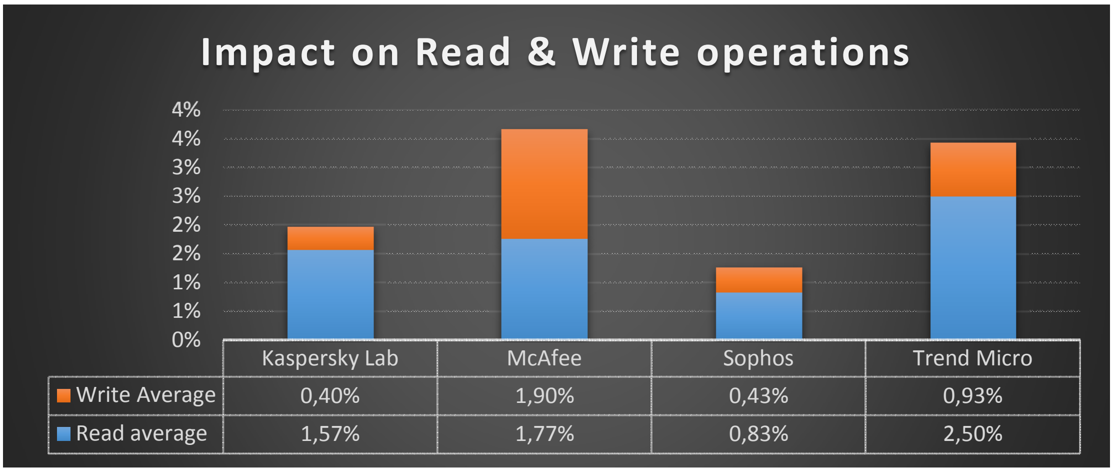
Executive Summary

The main goal of the test is to measure the anti-malware protection level and performance capabilities of solutions dedicated to secure network array storage appliances and their data.

The protection part of the test was executed according to the methodology of, and fully in parallel with, the public Online File Detection Test[1]. The results are shown on the graph below. Kaspersky Lab's product reached the highest protection level, while Trend Micro's had the fewest false positives.



The performance test measured the impact of the solution connected to the NAS while different types of load to the NAS were generated. The least impact on file operations was caused by Sophos' solution, followed by that of Kaspersky Lab.



	Kaspersky Lab	McAfee	Sophos	Trend Micro
🟧 Write Average	0,40%	1,90%	0,43%	0,93%
🟦 Read average	1,57%	1,77%	0,83%	2,50%

In conclusion, **Kaspersky Security for Storage** demonstrated the best malware detection rates, with modest impact on systems performance. For business critical infrastructure, this may result in better protection levels, while preserving high efficiency of the data storage.

[1] http://www.av-comparatives.org/wp-content/uploads/2016/04/avc_fdt_201603_en.pdf

Introduction

In corporate environments, fast-growing network storage solutions are becoming more and more popular, and malware protection for these has to be taken seriously. Many users are able to access the storage and read and write to it, and can therefore infect or be infected by the system. The bigger a corporate environment, the more users work with different corporate systems, including data storage infrastructure. A single malicious file placed on the storage can easily infect many computers on the network. To protect against this, an anti-virus solution for storage has to be considered, in addition to the obligatory end-user protection product. Such a solution is responsible for scanning files placed on the network storage and preventing users from being harmed by them. These AV-solutions work quite differently from normal end-user products, and therefore an independent test of such products is obviously valuable. As well as providing effective protection, these solutions should avoid slowing down the performance of the storage system, and therefore the solution’s impact on precious data storage resources should be considered.

The main goals of the test are thus not only to determine detection rates, but also to evaluate the effect of the security solution on the storage system’s performance.

Tested Products

- Kaspersky Security for Storage (Kaspersky Security 10 for Windows Servers)
- McAfee VirusScan Enterprise for Storage 8.0
- Sophos for Network Storage 10.3
- Symantec Protection Engine for NAS (Network Attached Storage Protection) 7.5
- Trend Micro ServerProtect Multi-Storage 6.0

All the products are enterprise-class solutions, designed to be managed in an Active Directory based environment by IT professionals, not by regular users. That said, even though ease of use is not such an important issue, significant differences in usability between products can be observed. The Kaspersky Lab and McAfee products stand out positively in this respect.

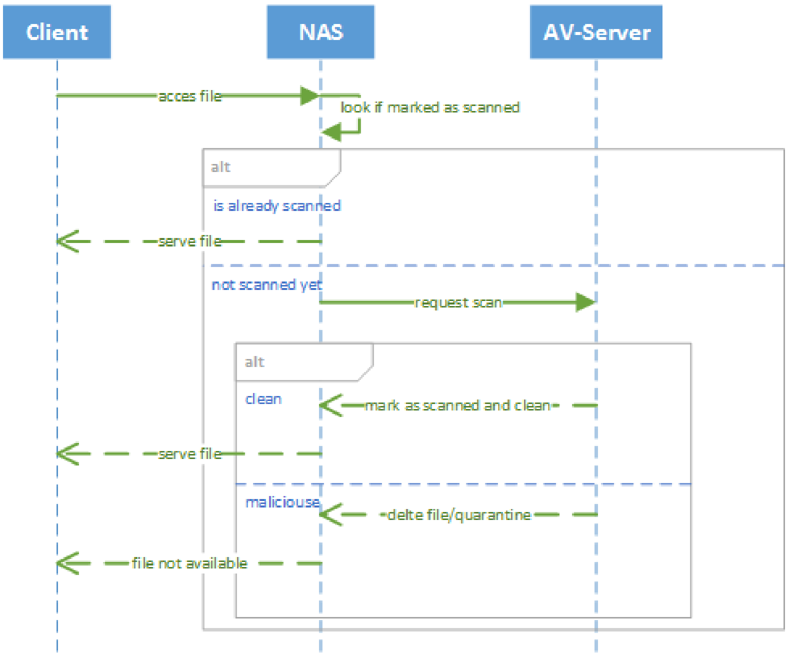
Basic Setup of an Anti-Virus for Storage Solution

To monitor a network drive, a special anti-virus server is linked to the storage via RPC (Remote Procedure Call). Files are scanned when read from the storage and the preconfigured actions are taken. To allow such a solution to work, the NAS system has to support either RPC (Remote Procedure Call) or ICAP (Internet Content Adaption Protocol) to communicate with the dedicated AV server on which the AV product is installed. These features are provided by enterprise-class storage solutions made by companies such as EMC, Hitachi, HP, IBM, NetApp, Oracle and Sun. The officially supported storage systems (as taken from the product data sheets) can be seen in the table below, but normally only one of the protocols mentioned has to be provided by the NAS to run such a solution. Our test was performed on a NetApp Storage solution, as this is supported by all the AV products.

Officially supported storage systems by manufacturer

	Kaspersky Lab	McAfee	Sophos	Symantec	Trend Micro
EMC	Yes	Yes	Yes	Yes	Yes
Hitachi	Yes	Yes	-	Yes	Yes
HP	-	Yes	-	-	-
IBM	Yes	Yes	-	Yes	-
NetApp	Yes	Yes	Yes	Yes	Yes
Oracle	Yes	-	-	-	-
Sun	-	Yes	-	-	-

In the diagram below, the standard use case is shown. If a client accesses a file on the storage, the NAS software can determine if a scan is necessary. Normally this is the case if no scan result has been provided yet, but configurations are possible where a new scan could be run after a virus definition update. If the file has been scanned previously, the NAS serves the file to the client. If this is not the case, the NAS requests a scan from the AV-Server. In the meantime, the client has to wait until the storage can mark the file as clean. In the case of a malware detection, the file will be deleted or quarantined and the client will receive an error message that the file is not accessible.



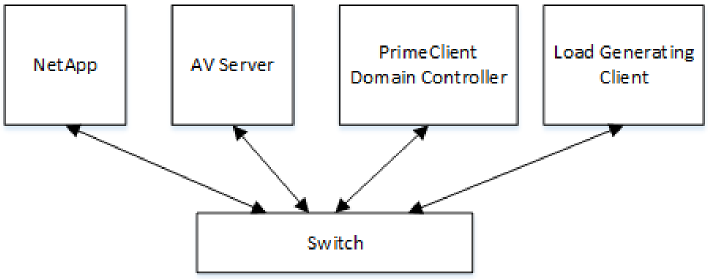
Basic sequence of a scan request

The additional time it takes to scan a file before it can be accessed by a client clearly influences the performance of the storage system and should therefore be considered.

Test methodology

Setup

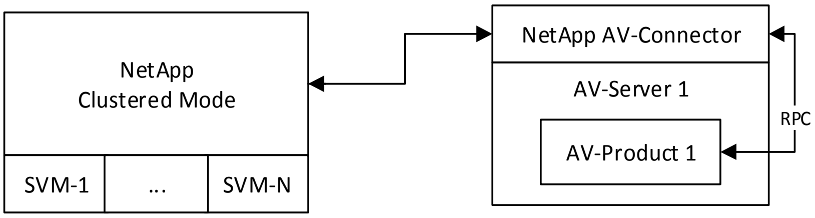
The test setup consists of clients accessing the storage, the NetApp, AV-Servers monitoring the storage and a primary client functioning as domain controller which also manages the test.



Basic Test Setup

The primary client is a Windows Server installation which takes on the role of a domain controller but is also responsible for handling the performance test. For this test, the primary client can tell the load generating client which loads to generate and records the results.

The NetApp has to be run in clustered mode (C-mode) to provide virtual storage for every scanner participating (SVM Storage Virtual Machine). This clustered mode is a NetApp installation where it is possible to split one Filer into multiple independent network shares. So we have the possibility to assign a different AV Product to each network share. With regard to the detection part, for every product a virtual server is deployed to an ESXi cluster and all tests are started at the same time. For the performance part, the AV Products are installed on a hardware server and the tests are run individually.



Basic NetApp Setup

The basic setup of an AV-Server connected with a NetApp SVM is shown in the picture above. The actual connection between storage and server is handled by NetApp. Therefore, the NetApp AV-Connector has to be installed on the server running the AV-product, to create a connection to the NetApp. The AV-Product is then pointed at the loopback address (127.0.0.1) to monitor the storage. On the NetApp, an AV-Server is assigned to an SVM via its IP/hostname. In our test case, we had five products participating, therefore the NetApp served five SVMs. To protect these SVMs, five virtual Windows Server installations were deployed on the AV Server ESXi cluster.

Hardware used: NetApp FAS25XX, two Dell R710 servers (2x2.26 GHz QuadCore Xeon E5520, 32GB RAM, 6x450GB SAS 15K) and Cisco Catalyst 2960-S 10G 48-port switch.

File Detection Test

For the file detection test part, we placed our test set of malware and clean samples on every NetApp Storage Virtual Machine while anti-virus scanning was disabled. After that, the configured anti-virus servers were connected with the NetApp and scanning was enabled. The test took place on the 3rd March 2016, in parallel with AV-Comparatives' standard File Detection Test[2]. This gave the ability to verify the test-set during standard feedback process with many vendors, and gave no advantage to any vendor. The malware test set consisted of 163,763 malicious samples. The products were tested with default settings and with cloud access enabled.

From the domain controller OS, we then attempted to copy all the test files from the NAS to the domain controller's local storage. The result could easily be evaluated by counting the successfully copied files.

The detection rates achieved were similar to the ones achieved with the respective home-user products, although not identical. This is because corporate products usually use different default settings with less-aggressive heuristics, in order to avoid false alarms and affecting performance in corporate environments, which in some cases could be important for particular deployments.

[2] http://www.av-comparatives.org/wp-content/uploads/2016/04/avc_fdt_201603_en.pdf

Performance Test

The performance test consists of three sub-tests[3]:

- **Database (DB) Benchmark**: how well a database can be sustained when stored on a NAS. This workload represents the typical behaviour of a database.

- **Video Data Acquisition (VDA) Benchmark**: how fast video streams can be captured when they are stored on NAS. The workload generally simulates applications that store data acquired from a temporarily volatile source (e.g. surveillance cameras). A stream refers to an instance of the application storing data from a single source (e.g. one video feed). Each stream corresponds to roughly a 36 Mb/s bit rate, which is in the upper range of high definition video.

- **Virtual Desktop Infrastructure (VDI) Benchmark**: the number of virtual desktops that can be maintained when stored on NAS. This workload simulates a steady-state, high-intensity knowledge worker in a VDI environment that uses full clones. This workload does not simulate a linked-clone environment. This is the behaviour that was seen in traces between the hypervisor and storage when the VMs were running on ESXi, Hyper-V, KVM and Xen environments.

	Operations mix:
DB	operations with database (Random Read (79%), Random Write (20%), Read (1%) over blocks of 8192 bytes (99%) and 1048576 bytes (1%)), and operations with log writing (Write (80%), Random Write (20%) over blocks of 8192 bytes (100%)).
VDA	operations set1 (Write (100%), Random Write (20%), Read (1%) over blocks of 8192 bytes (99%) and 1048576 bytes (1%)), and operations set2 (Read (5%), RMW (2%), Create (1%), Stat (2%) over blocks of 8192 bytes (100%)). Read operations are done over blocks of 65536 bytes (15%), 131072 byte (10%), 262144 bytes (20%), 524288 bytes (35%), 1048576 bytes (20%). Write operations are done over blocks of 32768 bytes (5%), 65536 bytes (10%), 131072 bytes (10%), 262144 bytes (25%), 524288 bytes (25%), 1048576 bytes (25%)
VDI	Read (6%), Write (9%), Random Read (20%), Random Write (64%), Access (1%). Operations are done over blocks of 512 bytes (1%), 2048 bytes (1%), 2560-3584 bytes (1%), 4096 bytes (20%), 4608-7680 bytes (1%), 8192 bytes (4%), 8704-15872 bytes (4%), 16384 bytes (42%), 16896-32256 bytes (3%), 32768 bytes (14%), 33280-65024 bytes (1%), 65536 bytes (6%), 66048-126976 bytes (1%), 131072 bytes (1%).

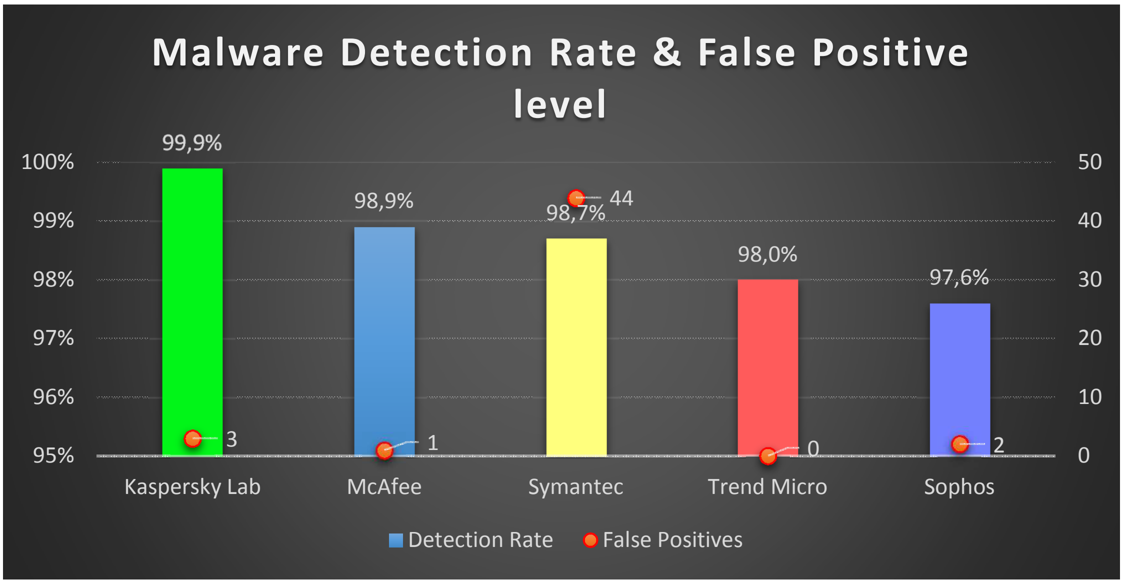
[3] Details can be found here: https://www.spec.org/sfs2014/docs/usersguide.pdf

Detailed results

File Detection Test

The table and graph below show the malware detection rates and the number of false alarms produced by the solutions. The table and graph are sorted by detection rate.

AV product for NAS		Vendor	Consumer product[4]		
Detection Rate	**False Alarms**		Detection Rate	False Alarms	Related awards[5]
99.9%	3	**Kaspersky Lab**	99.9%	3	ADV+
98.9%	1	**McAfee/Intel**	98.9%	1	ADV
98.7%	44	**Symantec**	99.1%	44	STD*
98.0%	0	**Trend Micro**	98.4%	0	ADV
97.6%	2	**Sophos**	97.6%	2	STD



The table also shows the results of the consumer products made by the participating vendors in the same Online File Detection Test[6] executed in parallel with this test. Results for the Symantec product can be found in a separate report[7]. (*) It could be noted that the false positive level of Symantec's product turned out to be rather high, which in the public File Detection Test would have caused the award given to be downgraded from ADV (Advanced) to STD (Standard). Considering the number of new malicious programs being discovered every day by security vendors, the higher malware-detection rates are, the greater is the protection from most advanced cyber threats.

[4] Results are taken from the public comparative Online File Detection Test of March 2016

[5] Values from column „Related Awards" are valid to the tested security products for storage based on File Detection Test methodology.

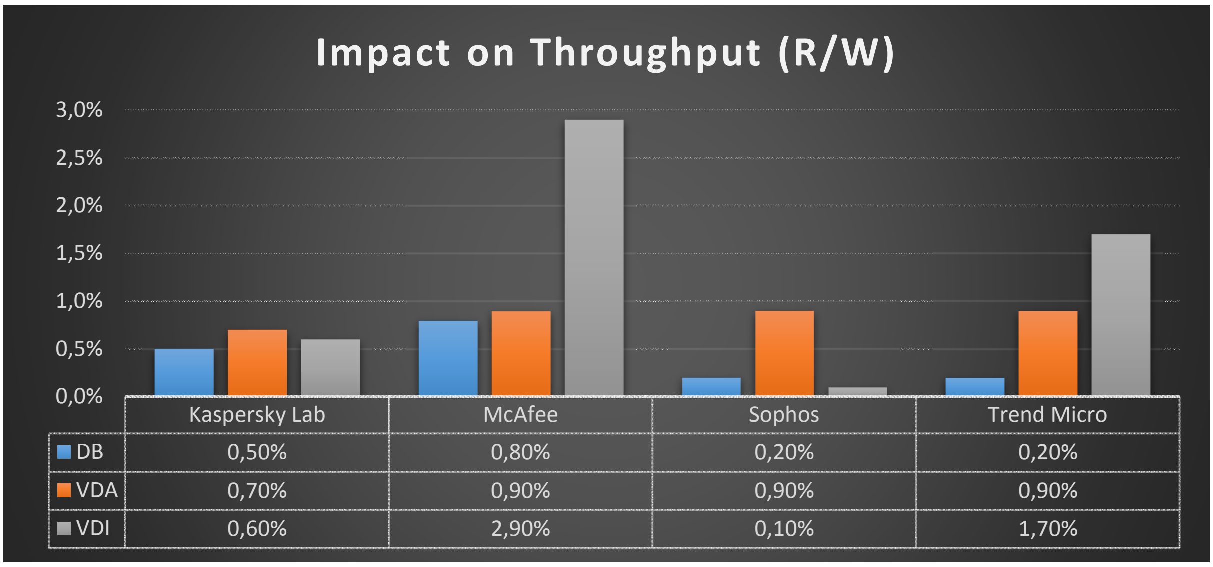
[6] http://www.av-comparatives.org/wp-content/uploads/2016/04/avc_fdt_201603_en.pdf

[7] http://www.av-comparatives.org/wp-content/uploads/2016/04/sp_ext_symantec_201603_en.pdf

Performance Test

In the case of ***Symantec***, none of the tests (DB, VDA, VDI) produced valid results. The log files lead to the assumption that the Symantec product may handle the files via the CIFS protocol in an unconventional way, which could lead to increased delay and to a crash of the subsystem. We have thus decided not to include any data for Symantec in the results below.

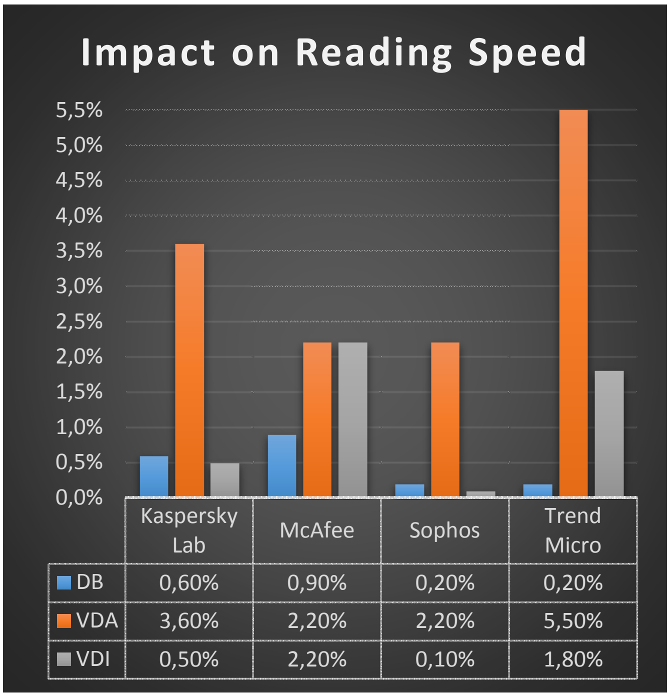
Impact on Throughput (Read/Write)



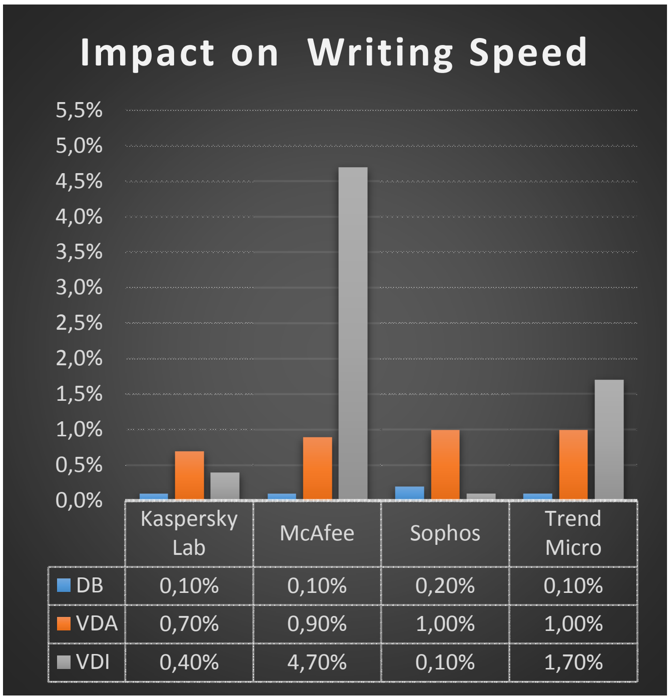
	Kaspersky Lab	McAfee	Sophos	Trend Micro
🟦 DB	0,50%	0,80%	0,20%	0,20%
🟧 VDA	0,70%	0,90%	0,90%	0,90%
⬜ VDI	0,60%	2,90%	0,10%	1,70%

The table and graph above show the decreased throughput rates (read/write combined) for the four subtests (lower is better).

The next page shows the results split into “Reading Speed” and “Writing Speed”.



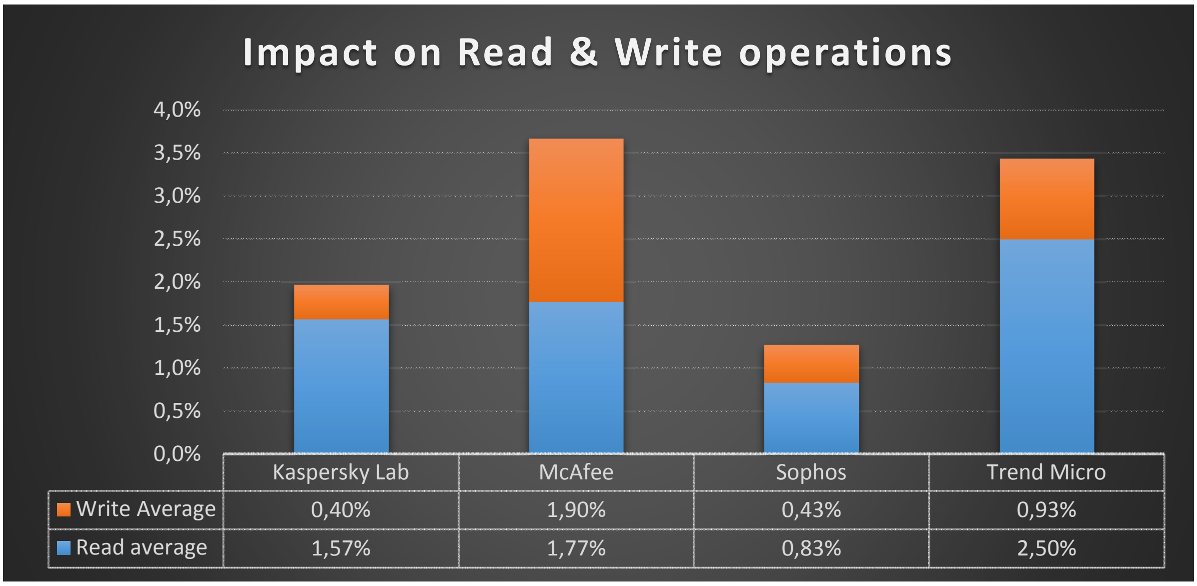
	Kaspersky Lab	McAfee	Sophos	Trend Micro
🟦 DB	0,60%	0,90%	0,20%	0,20%
🟧 VDA	3,60%	2,20%	2,20%	5,50%
⬜ VDI	0,50%	2,20%	0,10%	1,80%



	Kaspersky Lab	McAfee	Sophos	Trend Micro
🟦 DB	0,10%	0,10%	0,20%	0,10%
🟧 VDA	0,70%	0,90%	1,00%	1,00%
⬜ VDI	0,40%	4,70%	0,10%	1,70%

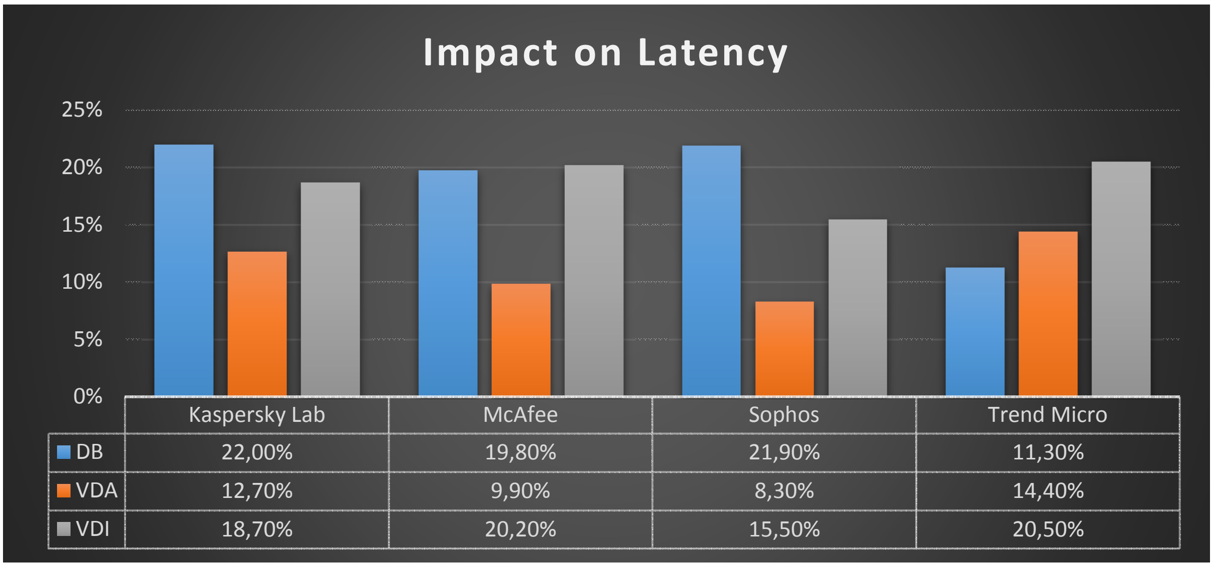
In some business scenarios, Write operations are of more importance from a performance perspective, whilst in others it will be Read operations.

The following graph allows the estimation of the necessary characteristics on an average I\O load.



	Kaspersky Lab	McAfee	Sophos	Trend Micro
🟧 Write Average	0,40%	1,90%	0,43%	0,93%
🟦 Read average	1,57%	1,77%	0,83%	2,50%

Impact on Latency



	Kaspersky Lab	McAfee	Sophos	Trend Micro
🟦 DB	22,00%	19,80%	21,90%	11,30%
🟧 VDA	12,70%	9,90%	8,30%	14,40%
⬜ VDI	18,70%	20,20%	15,50%	20,50%

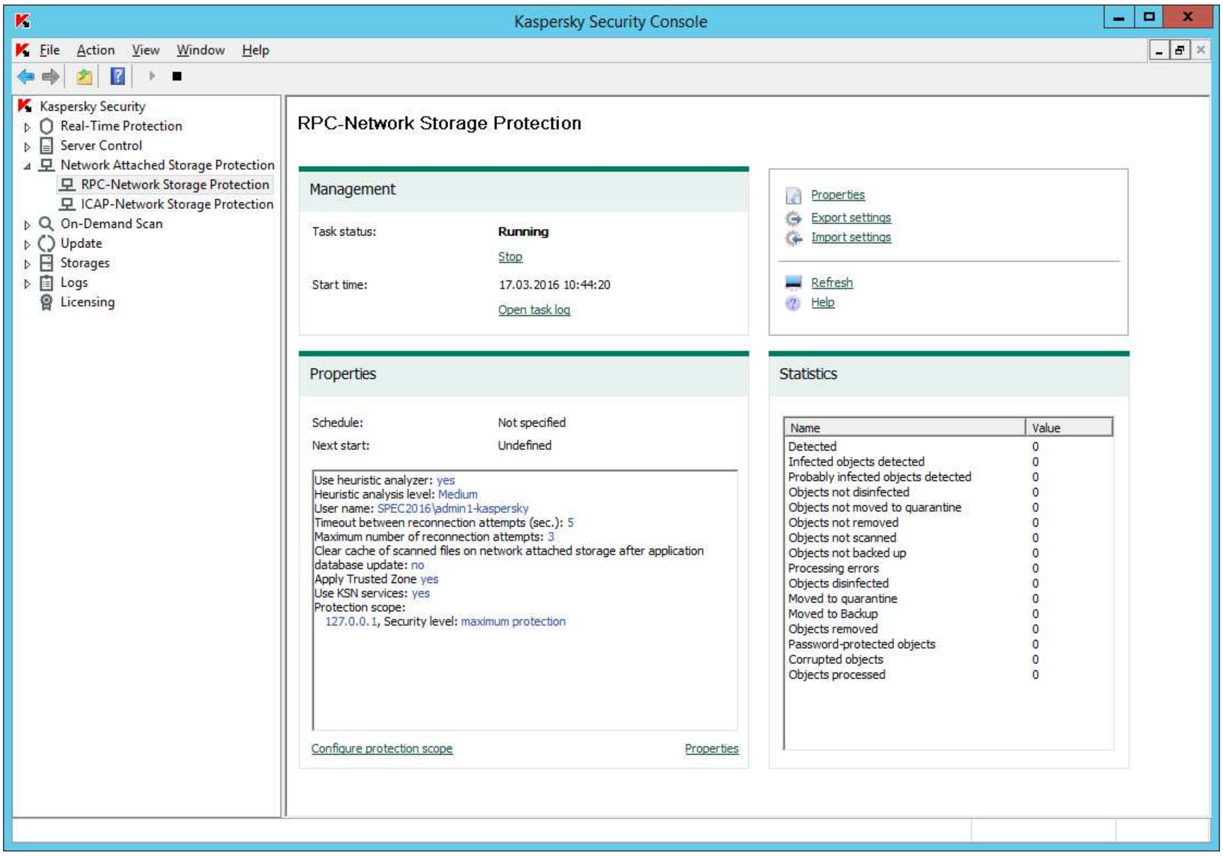
The table and graph above show the increased latency (lower is better) during the four subtests.

It is critical to keep in mind that performance impact should not be taken into consideration without the detection rates. Higher detection rates means more protective technologies being in place and deeper investigation of the each individual scanned object. Thus slightly higher impact on systems performance may be expected for those security solutions that have high detection rates.

Product Notes

Kaspersky Security for Storage

The Kaspersky Lab product is specially designed to protect corporate servers and network attached storage. The solution consists of the protection engine itself (Kaspersky Security 10 for Windows Server), and a security console to manage it (Kaspersky Security Center). A simple Plug-in Wizard is used to link both parts.



RPC-Network Storage Protection

Management

Task status: Running

Start time: 17.03.2016 10:44:20

Properties

Schedule: Not specified

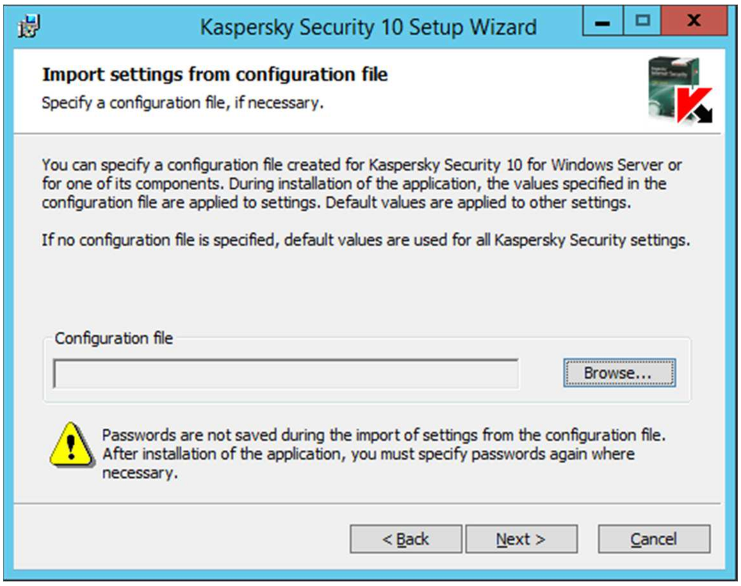
Next start: Undefined

Use heuristic analyzer: yes
Heuristic analysis level: Medium
User name: SPEC2016\admin1-kaspersky
Timeout between reconnection attempts (sec.): 5
Maximum number of reconnection attempts: 3
Clear cache of scanned files on network attached storage after application database update: no
Apply Trusted Zone yes
Use KSN services: yes
Protection scope:
127.0.0.1, Security level: maximum protection

Statistics

Name	Value
Detected	0
Infected objects detected	0
Probably infected objects detected	0
Objects not disinfected	0
Objects not moved to quarantine	0
Objects not removed	0
Objects not scanned	0
Objects not backed up	0
Processing errors	0
Objects disinfected	0
Moved to quarantine	0
Moved to Backup	0
Objects removed	0
Password-protected objects	0
Corrupted objects	0
Objects processed	0

The wizard used to install the security engine is a simple one, and can be used to turn some security features on or off. Additionally, it is possible to provide a configuration file to easily propagate the desired setting among multiple installations.



Import settings from configuration file

Specify a configuration file, if necessary.

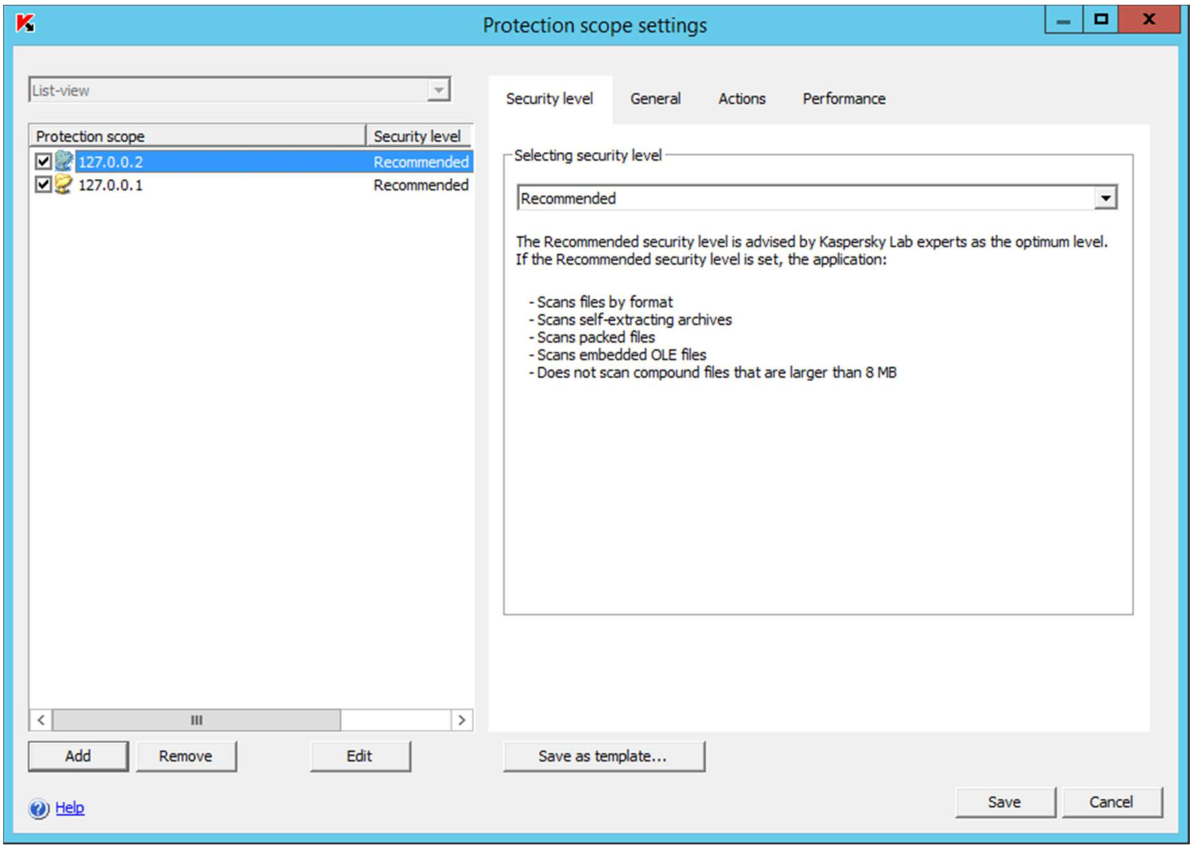
You can specify a configuration file created for Kaspersky Security 10 for Windows Server or for one of its components. During installation of the application, the values specified in the configuration file are applied to settings. Default values are applied to other settings.

If no configuration file is specified, default values are used for all Kaspersky Security settings.

Configuration file

Passwords are not saved during the import of settings from the configuration file. After installation of the application, you must specify passwords again where necessary.

The installation of the console also uses a simple wizard, the only decision that can be made is to allow remote management of the console.



Protection scope	Security level
☑ 127.0.0.2	Recommended
☑ 127.0.0.1	Recommended

Selecting security level

Recommended

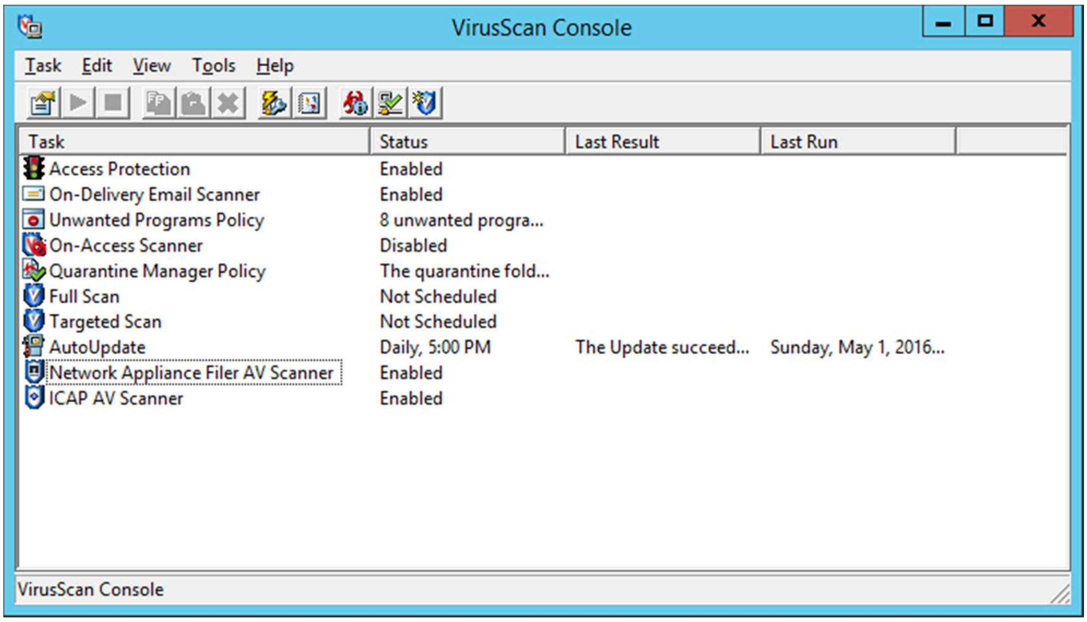
The Recommended security level is advised by Kaspersky Lab experts as the optimum level. If the Recommended security level is set, the application:

- Scans files by format
- Scans self-extracting archives
- Scans packed files
- Scans embedded OLE files
- Does not scan compound files that are larger than 8 MB

After the installation is complete, the management console can be accessed, which gives a clear system overview. To protect the storage, the protection scope for “RPC-Network Storage Protection” can be configured under the Tab “Network attached Storage Protection”. For our test, the loopback address was added to a list of protected IPs. It is possible to set different security levels for all the IPs in the protections scope.

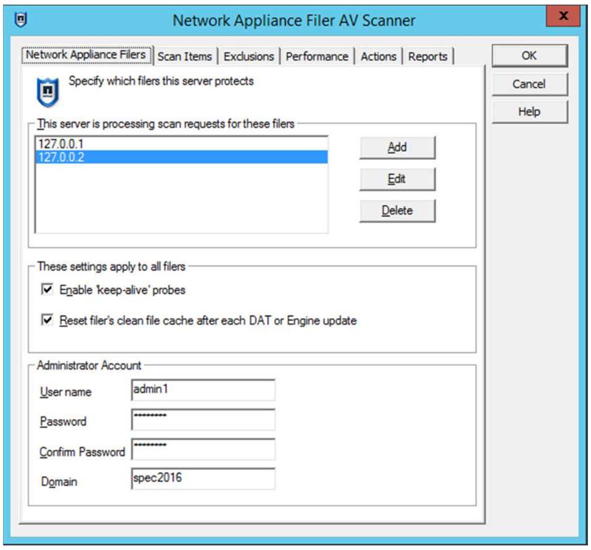
McAfee VirusScan Enterprise for Storage

The McAfee product is provided as an additional installation to their enterprise product, and is specially designed to manage storage protection. The installer therefore requires an existing VirusScan Enterprise installation on the server, which will be checked by the wizard.



Task	Status	Last Result	Last Run
Access Protection	Enabled		
On-Delivery Email Scanner	Enabled		
Unwanted Programs Policy	8 unwanted progra...		
On-Access Scanner	Disabled		
Quarantine Manager Policy	The quarantine fold...		
Full Scan	Not Scheduled		
Targeted Scan	Not Scheduled		
AutoUpdate	Daily, 5:00 PM	The Update succeed...	Sunday, May 1, 2016...
Network Appliance Filer AV Scanner	Enabled		
ICAP AV Scanner	Enabled		

The installation of VirusScan Enterprise is a basic wizard without any important decisions to be made. The installation of the VirusScan Enterprise for Storage extension only requires the user to accept the license agreement and select an installation directory.



Specify which filers this server protects

This server is processing scan requests for these filers

127.0.0.1
127.0.0.2

These settings apply to all filers

☑ Enable 'keep-alive' probes

☑ Reset filer's clean file cache after each DAT or Engine update

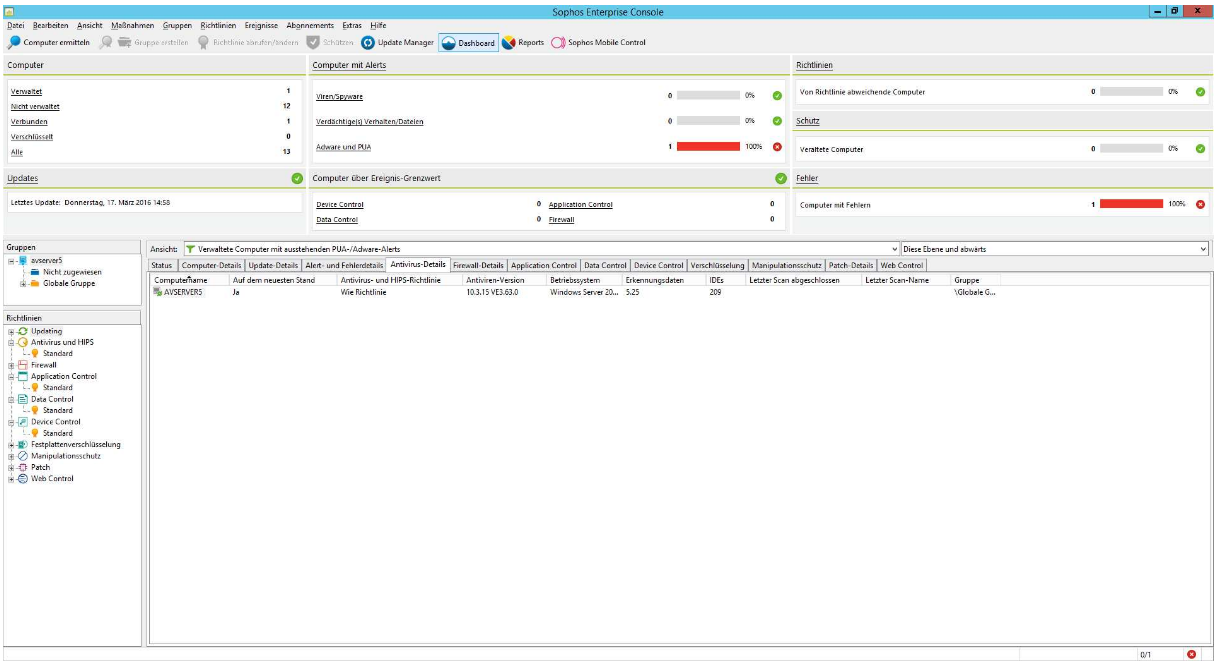
Administrator Account

User name: admin1
Password: ********
Confirm Password: ********
Domain: spec2016

The console is clearly arranged, and it is easy to enable/disable different protection types. The management of monitored storage can be found under the "Network Appliance Filer AV Scanner" menu item. The storage unit to be protected can be added to a list, and an administrator account has to be assigned. There is one security configuration which is applied to all assigned storage units.

Sophos for Network Storage

The Sophos management console is a comprehensive program designed to handle all the anti-virus installations in an Active Directory environment. Therefore, the management of the console is quite complicated.


Sophos Enterprise Console
Datei Bearbeiten Ansicht Maßnahmen Gruppen Richtlinien Ereignisse Abonnements Extras Hilfe
Computer ermitteln
Gruppe erstellen
Richtlinie abrufen/ändern
Schützen
Update Manager
Dashboard
Reports
Sophos Mobile Control

Computer

Verwaltet	1
Nicht verwaltet	12
Verbunden	1
Verschlüsselt	0
Alle	13

Computer mit Alerts

Viren/Spyware	0	0%
Verdächtige(s) Verhalten/Dateien	0	0%
Adware und PUA	1	100%

Richtlinien

Von Richtlinie abweichende Computer	0	0%

Schutz

Veraltete Computer	0	0%

Updates

Letztes Update: Donnerstag, 17. März 2016 14:58

Computer über Ereignis-Grenzwert

Device Control	0	Application Control	0
Data Control	0	Firewall	0

Fehler

Computer mit Fehlern	1	100%

Ansicht: Verwaltete Computer mit ausstehenden PUA-/Adware-Alerts

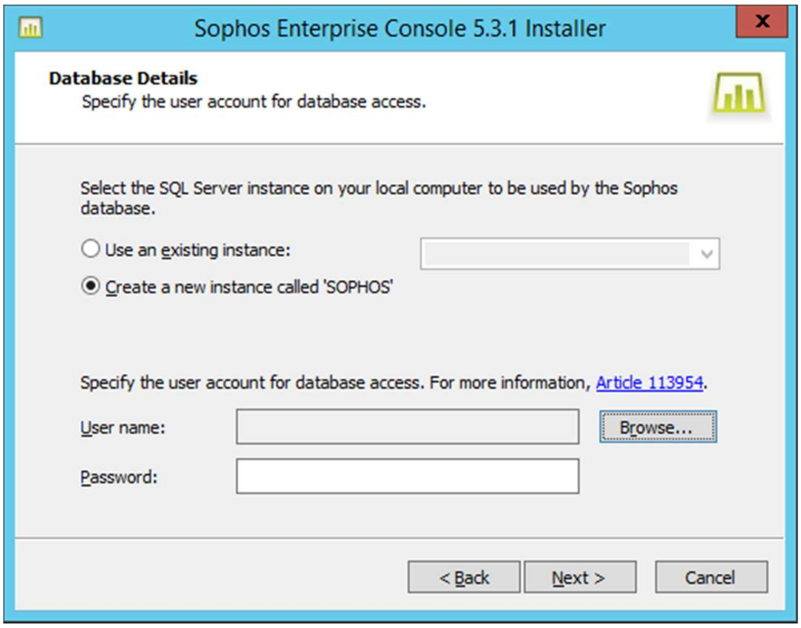
Diese Ebene und abwärts

Status | Computer-Details | Update-Details | Alert- und Fehlerdetails | Antivirus-Details | Firewall-Details | Application Control | Data Control | Device Control | Verschlüsselung | Manipulationsschutz | Patch-Details | Web Control

Computername	Auf dem neuesten Stand	Antivirus- und HIPS-Richtlinie	Antiviren-Version	Betriebssystem	Erkennungsdaten	IDEs	Letzter Scan abgeschlossen	Letzter Scan-Name	Gruppe
AVSERVER5	Ja	Wie Richtlinie	10.3.15 VE3.63.0	Windows Server 20...	5.25	209			\Globale G...

0/1

The installation of the product is quite an extensive procedure. Amongst other things, a Microsoft SQL Server installation is necessary to store security information. Additionally, domain users for the database and the update manager have to be created.



Database Details

Specify the user account for database access.

Select the SQL Server instance on your local computer to be used by the Sophos database.

○ Use an existing instance:

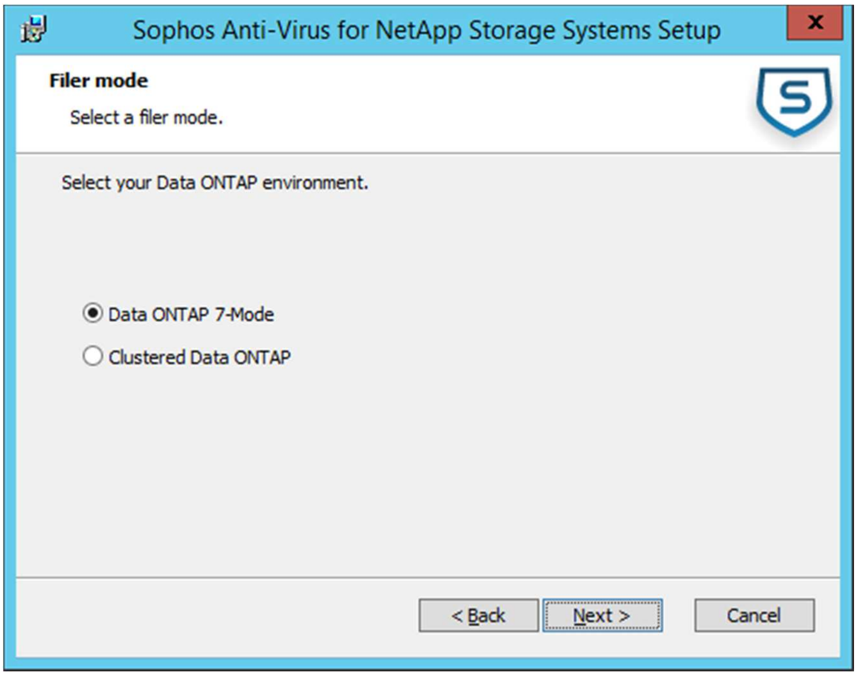
● Create a new instance called 'SOPHOS'

Specify the user account for database access. For more information, Article 113954.

User name:

Password:

After finishing this installation, the Sophos Enterprise Console is installed on the computer. At the first start-up, a wizard shows up that helps the admin to download the necessary software to protect the system. In our case, we only needed anti-virus protection for Windows. Additionally, computer groups can be generated according to the Active Directory environment. If this is not used, computers can be assigned to groups manually. A group of computers can be assigned to "software-subscriptions". So, after adding our server to a group which is subscribed to the anti-virus product, we started an automatic installation of the product on the server.



Sophos Anti-Virus for NetApp Storage Systems Setup

Filer mode

Select a filer mode.

Select your Data ONTAP environment.

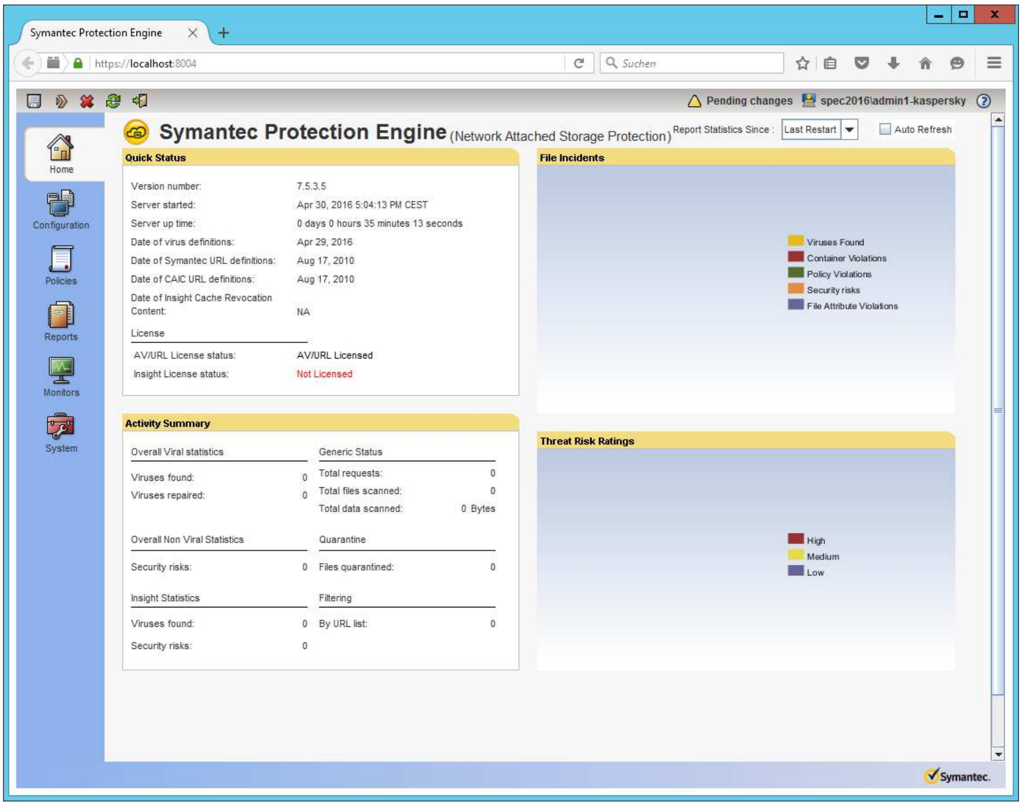
● Data ONTAP 7-Mode

○ Clustered Data ONTAP

After installing the actual malware protection, it is possible to manually install the storage protection via a wizard. In the wizard we selected the NetApp mode (Clustered Mode) and provided the appropriate user credentials. This connected the storage with the AV-server.

Symantec Protection Engine for NAS (Network Attached Storage Protection)

The Symantec Protection Engine is specially designed as a network attached storage protection product. The management console is implemented as a Java web app, and is therefore accessible via the browser. The management console is easy to use, and all the configurations are easy to understand. However, the small buttons on the top left of the console, from which configurations can be saved, applied and cancelled, are easy to overlook, and so it took us some time to notice that a configuration has to be saved to take effect.



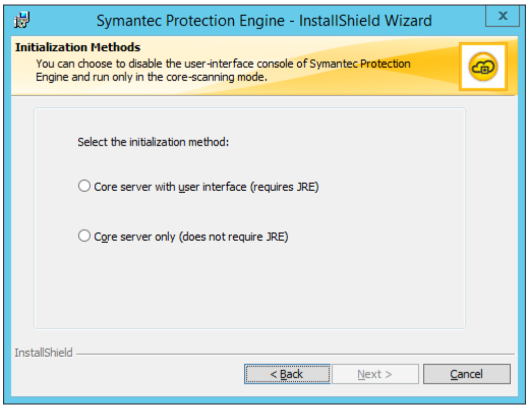
Quick Status

Version number:	7.5.3.5
Server started:	Apr 30, 2016 5:04:13 PM CEST
Server up time:	0 days 0 hours 35 minutes 13 seconds
Date of virus definitions:	Apr 29, 2016
Date of Symantec URL definitions:	Aug 17, 2010
Date of CAIC URL definitions:	Aug 17, 2010
Date of Insight Cache Revocation Content:	NA
License	
AV/URL License status:	AV/URL Licensed
Insight License status:	Not Licensed

Activity Summary

Overall Viral statistics		Generic Status	
Viruses found:	0	Total requests:	0
Viruses repaired:	0	Total files scanned:	0
		Total data scanned:	0 Bytes
Overall Non Viral Statistics		Quarantine	
Security risks:	0	Files quarantined:	0
Insight Statistics		Filtering	
Viruses found:	0	By URL list:	0
Security risks:	0		

The Symantec Protection Engine can be installed simply via a wizard. Symantec offers the options of installing only the core server, or also adding the user interface to the installation. The latter requires a Java Runtime Environment Installation. The user interface will be available as a Java Applet, which is served via a web server. It is possible to authenticate either via the Windows Active Directory authentication, or via a Symantec Protection Engine based solution.



Initialization Methods

You can choose to disable the user-interface console of Symantec Protection Engine and run only in the core-scanning mode.

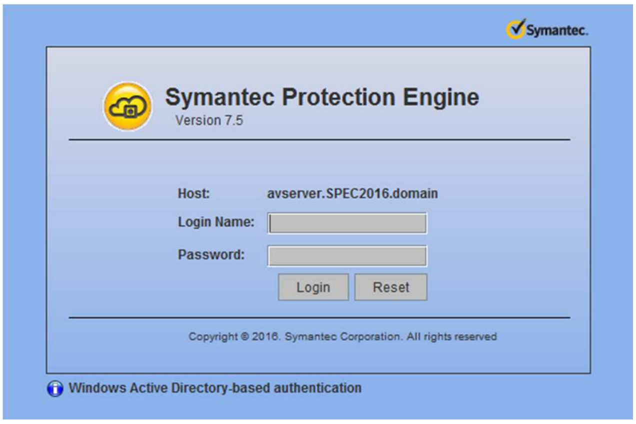
Select the initialization method:

○ Core server with user interface (requires JRE)

○ Core server only (does not require JRE)

For simplicity, we chose the Active Directory authentication, which only requires the specification of a user group that is allowed to access the user interface. In the next steps, we enabled/disabled some security options such as URL-filtering, and set the ports via which the web server will be accessed. After this configuration, the setup is finished and the wizard installs the product.

After the installation completes, the protection engine runs as a service on the server. In our test, it was necessary to set a special user with which the service is run. The protection engine can now be managed via the user interface, which is accessed through the configured port on this machine.



Symantec Protection Engine
Version 7.5

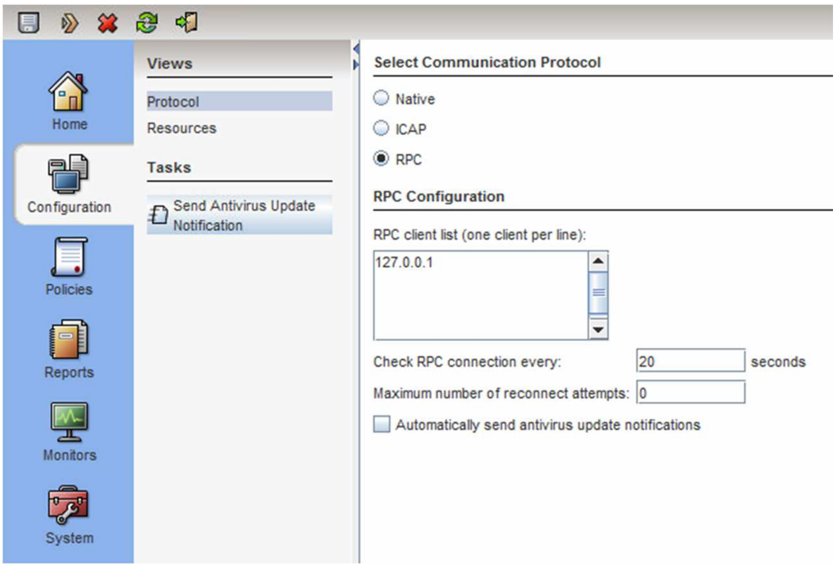
Host: avserver.SPEC2016.domain
Login Name:
Password:

Copyright © 2016. Symantec Corporation. All rights reserved

Windows Active Directory-based authentication

To access the user interface, a browser is needed that allows the activation of the Java runtime environment. The interface can now be accessed via the browser under https://localhost:8004, whereby the port used is configurable, and the https protocol is necessary. Of course, it is also possible to access the web interface from any other computer that has network access to the server. This makes the remote management of the protection engine very easy.

Connecting the protection engine with the storage is straightforward. Under “configuration” we were able to configure the protocol and the resources used. We simply chose the RPC protocol, and assigned the loopback address as a client. After saving the configuration, a manual restart of the service is necessary for the protocol to take effect.



Select Communication Protocol

○ Native
○ ICAP
● RPC

RPC Configuration

RPC client list (one client per line): 127.0.0.1

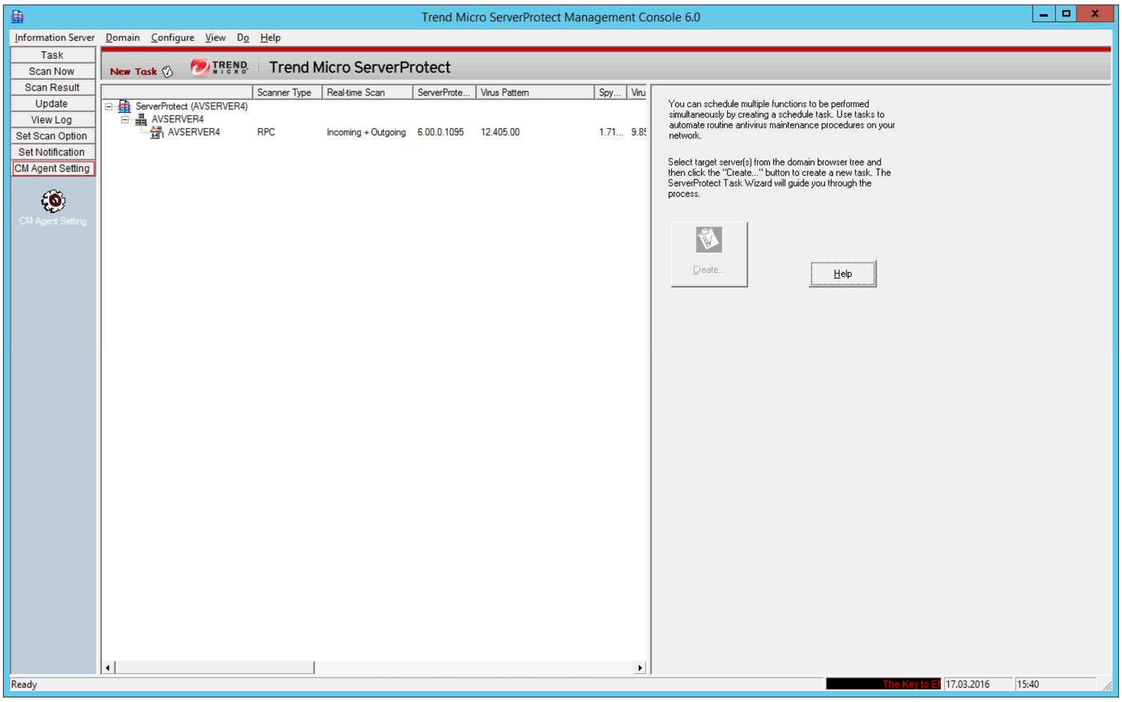
Check RPC connection every: 20 seconds

Maximum number of reconnect attempts: 0

□ Automatically send antivirus update notifications

Trend Micro ServerProtect Multi-Storage

Trend Micro ServerProtect is a product designed to secure corporate servers. The management console, in comparison with the other products, can be quite confusing. We found the navigation quite puzzling, and often it is not clear which menu point is selected. With small screen resolutions, we completely missed the actual settings, as these were not displayed. However, after studying the console for some time, we were able to perform the necessary configuration.

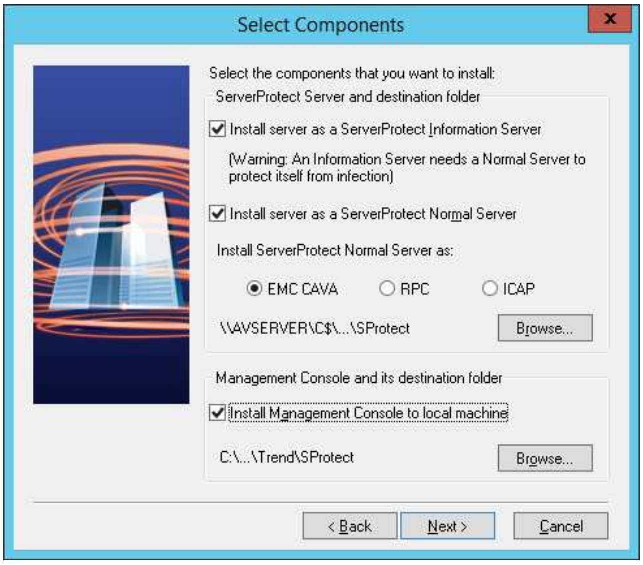


	Scanner Type	Real-time Scan	ServerProte...	Virus Pattern	Spy...	Viru
ServerProtect (AVSERVER4)						
AVSERVER4						
AVSERVER4	RPC	Incoming + Outgoing	6.00.0.1095	12.405.00	1.71...	9.8

You can schedule multiple functions to be performed simultaneously by creating a schedule task. Use tasks to automate routine antivirus maintenance procedures on your network.

Select target server(s) from the domain browser tree and then click the "Create..." button to create a new task. The ServerProtect Task Wizard will guide you through the process.

The product is installed simply via a wizard, which nonetheless needs some advanced configuration. During the installation process it is necessary to choose which protocol should be handled by the server. Therefore, we installed a so-called RPC Server. It is also necessary to provide user credentials with administrator rights during the installation process, and to set a password to access the management console.



Select the components that you want to install:

ServerProtect Server and destination folder

☑ Install server as a ServerProtect Information Server

(Warning: An Information Server needs a Normal Server to protect itself from infection)

☑ Install server as a ServerProtect Normal Server

Install ServerProtect Normal Server as:

● EMC CAVA ○ RPC ○ ICAP

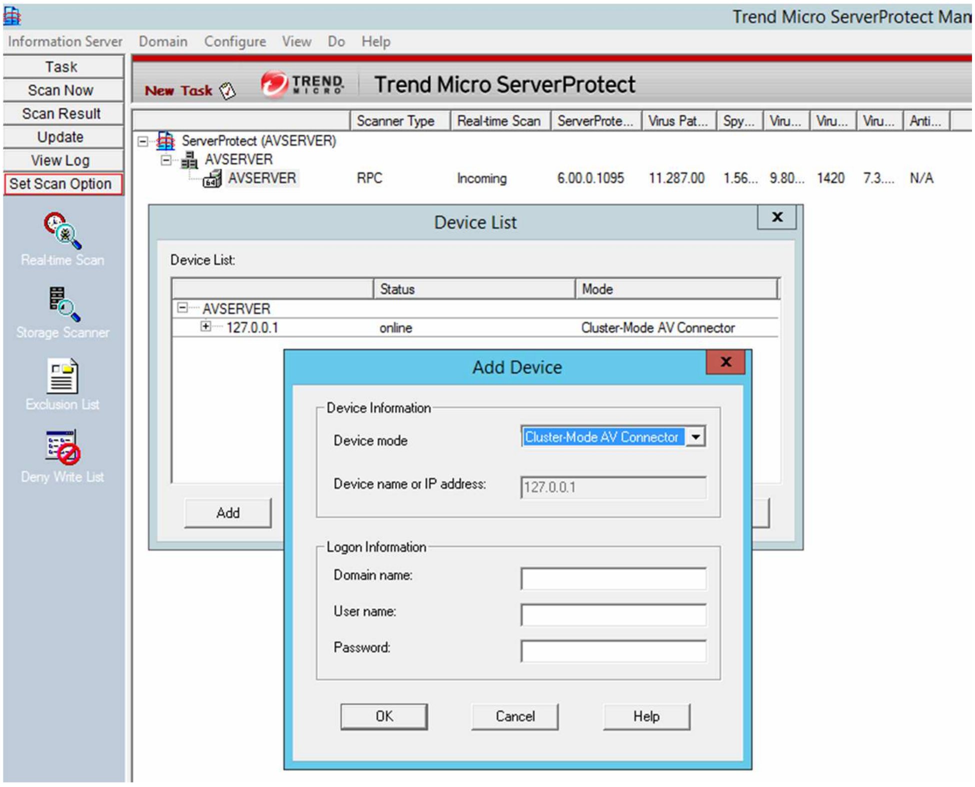
\\AVSERVER\C$\...\SProtect

Management Console and its destination folder

☑ Install Management Console to local machine

C:\...\Trend\SProtect

After the installation, the security console can be accessed, which requires the administrator to log in with the pre-configured password. To connect to the storage, we had to right click on the RPC AV Scanner installation, which is listed in the main view. There we could select the device list, which shows a list of devices monitored by the server. We simply added a new device in clustered mode, which already had the loopback address assigned. Additionally, the logon information of the privileged user on the NetApp had to be set.



	Scanner Type	Real-time Scan	ServerProte...	Virus Pat...	Spy...	Viru...	Viru...	Viru...	Anti...
ServerProtect (AVSERVER)									
AVSERVER									
AVSERVER	RPC	Incoming	6.00.0.1095	11.287.00	1.56...	9.80...	1420	7.3....	N/A

Device List:

	Status	Mode
AVSERVER		
127.0.0.1	online	Cluster-Mode AV Connector

Device Information

Device mode: Cluster-Mode AV Connector

Device name or IP address: 127.0.0.1

Logon Information

Domain name:

User name:

Password:

Copyright and Disclaimer

AV-Comparatives and its testers cannot be held liable for any damage or loss, which might occur as result of, or in connection with, the use of the information provided in this paper. We take every possible care to ensure the correctness of the basic data, but a liability for the correctness of the test results cannot be taken by any representative of AV-Comparatives. We do not give any guarantee of the correctness, completeness, or suitability for a specific purpose of any of the information/content provided at any given time. No one else involved in creating, producing or delivering test results shall be liable for any indirect, special or consequential damage, or loss of profits, arising out of, or related to, the use or inability to use, the services provided by the website, test documents or any related data.

For more information about AV-Comparatives and the testing methodologies, please visit our website.

AV-Comparatives (August 2016)