Sophos Anti-Virus distribution: Push versus Pull

Ivan Ignjatic, Sophos Plc, Oxford, England

Part #tr00092i/980410

Introduction

This document is an overview of the Sophos Anti-Virus (SAV) software distribution techniques. It discusses the effectiveness and usability of the Sophos installation tools and contrasts these against other distribution tools available on the market.

Unlike the product reviews usually carried out by magazines this document reveals the issues behind the complicated task of software distribution across local and wide area networks or across thousands of servers and workstations which a medium-sized or large enterprise is likely to have.

These issues are also very important in smaller networks since an incorrect and inefficient deployment of any package can incur severe damage and costs to any size institution.

The magazine reviews often simply mention: *"One click on the update button downloads the latest virus information over the Internet and the updates are not large, taking just a few minutes to install."*

In fact the task and the consequences of software distribution are much more complex.

It is certain that a single package installation can be accomplished in just a few minutes, but the real question is: How long will my 2,000-PC network take to update?

Additional issues to consider are:

- The cost of distribution and administration software
- The length of time required to distribute or update a package
- Maintenance effort (distribution tools which linearly increase the maintenance effort with the increase in the number of networked PCs can present a huge overhead to the administrator)
- Updating portable PCs which connect to the network infrequently
- Effects on network performance as a result of by the networked PCs being updated
- Compatibility of the software being distributed with the operating system version and other existing software
- The need to restart PCs after software installation or upgrade (a server may require a scheduled shutdown)
- Roll-back facilities (when upgrade errors occur or incompatibilities arise)
- The ease of monitoring and administering workstations
- The natural characteristic of anti-virus software to require frequent updates
- Integration with other enterprise-wide distribution tools

SAV distribution tools try to provide the most appropriate and efficient solution in all the fields covered by the above list. The tools and techniques described in this document refer to the distribution of SAV on WfW, Windows 95 and Windows NT plaforms. The tools SAV Admin and SwDeploy are currently available only for Windows NT.

Aims of the SAV distribution tools

Distribution solution as part of the product

The installation and distribution components are incorporated into the standard product. This allows even smaller establishments to distribute software easily at no extra cost.

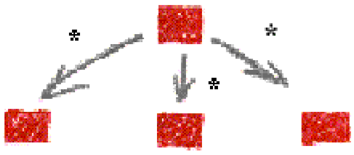
Efficient frequent updating

Just like other anti–virus products SAV requires frequent updating to ensure that high-detection rates are maintained. SAV updates are made available on a monthly basis while urgent updates can be distributed electronically as and when required.

Sophos distribution tools are tailored to handle frequent updates without imposing an undue burden on the network or its administrator.

Quick and easy updating of single and 1000+ PCs

The Sophos 'pull' technology makes use of a pro-active technique in which all clients on the network take part in a global and also parallel installation/ upgrade. In practice, a network of 1000 or more clients can be updated within 10 minutes.



Conventional software distribution methods by contrast use the so called 'full push' technique. These packages inflict a considerable time constraint on the administrators. Since only one machine is performing the 'push' on all the client machines in a sequence, the length of time required to perform cross-network installations and frequent updates is usually high. Such updates can take several days to complete on a large network.

Portable PC updating

Portable PCs can fully exploit the advantages of the 'pull' approach. When a portable connects to a network, the local copy of SAV will perform a consistency check. If a more recent version of SAV is available on the network, the portable will be updated. Also, an 'on demand' update is available as standard, if needed.

Conventional software distribution methods do not provide AutoUpgrade capabilities for portables since such PCs can not be seen by the 'push' station at all times.

Integration with enterprise-wide distribution tools

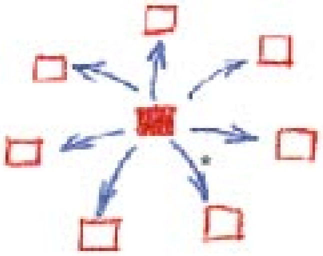
SAV installation tools have been designed to integrate easily with other enterprise-wide distribution tools such as, for example, SMS (Microsoft Systems Management Server).

Installation command line qualifiers, registry settings and the SwDeploy tool allow third party applications to deploy, update and control the way in which SAV is installed and how it functions.

SAV Admin - SAV administration tool

When used with the integrated SAV, SAV Admin aids deployment, updating, configuration and monitoring of SAV across the network.

SAV Admin acts as a front-end tool which can be used in combination with SMS or other management packages to aid SAV status monitoring and administration.



SAV Admin is a 'minimal push' tool. While deploying an initial installation of SAV, SAV Admin copies the minimal number of components to the client enabling the package to perform the first 'pull' installation from the server onto the client.

It is this approach combined with the 'pull' updating methods which provides the most effective and comprehensive distribution solution.

SwDeploy

Additional SAV tools are also available. SwDeploy can integrate with other third-party management tools to provide the equivalent of the 'minimal push' stage of SAV Admin.

SwDeploy is a command-line based utility that lets administrators perform initial client installations and retrieve the status of remote SAV. It includes SwServ, which manages NT services remotely and SwHive, which remotely updates SAV configurations.

SAV distribution principles

SAV software distribution can be viewed as a three stage process:

1. Obtaining SAV software and updates

SAV software and updates are sent to customers monthly on CD-ROM, floppies or via the Internet, while urgent virus updates can be obtained from Sophos electronically.

SGET is an Internet download tool which can be used to poll the Sophos web site automatically for the latest AV updates.

2. Installing SAV

SAV can be installed directly onto individual PCs from floppies, CD-ROM or an Internet download. This is called 'local installation'. The alternative is called 'central installation' which allows workstation installation and updating to be performed from one point.

Both local and central installations will be described in more detail in the following sections.

3. Monitoring the status and configuring SAV

SAV Admin, SwDeploy and other third-party applications can be used to carry out this process remotely from one or several administration points.

Local installation

This stage is carried out by the conventional installation applications. SAV provides methods to install all products manually from floppies, CD-ROM or a central installation. Unattended installation/upgrade mode is only supported when installing from a central installation.

The SAV setup program automatically performs the following tasks as part of a local installation:

- Deactivates previous version components (closing running GUI programs, stopping services, etc)
- Modifies the existing PC state (deletes obsolete files, overwrites existing files and copies in new files from source, creates shares, services, security permissions, links to programs, etc)
- Activates the new package version (starting drivers, services, GUI applications, etc)

The package files are obtained by copying files from the installation source using the 'pull' method.

Central installation

A central installation is a set of installation files and configuration information (installation, update and other configuration settings).

The central installation is stored in a platform-independent format, and can be pushed across the network by almost any deployment tool to desired locations. A central installation can be placed on any file system, server or even a local workstation.

Most importantly the central installation should be accessible by all clients installing and updating the specific product. The SAV setup program provides options to create and update central installations as standard.

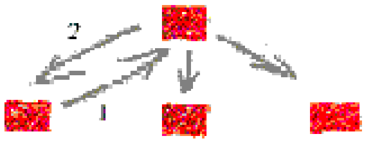
For more information on effective creation and deployment of central installations see the section 'Distribution planning and design'.

The AutoUpgrade feature

The AutoUpgrade feature provides an efficient approach to updating. It ensures that all networked as well as portable PCs are kept up to date with the version stored in the central installation, with minimal administration effort.

AutoUpgrade has been designed to avoid any linear increase of the network load and maintenance effort with the increase in the number of client PCs.

AutoUpgrade feature performs two tasks:



1. Update check

Each client PC running SAV performs frequent checks to determine whether a more recent version is available in the central installation.

2. Update initiation

When an update check returns a positive answer, the local installation update is initiated. AutoUpgrade makes use of the 'pull' technology in which all clients on the network take part in a global and parallel upgrade.

The efficiency of AutoUpgrade complements the 'minimal push' distribution method of the administration tools, SAV Admin and SwDeploy. These two tools give the network administrator full control over SAV and provide efficient simple software distribution and updating.

Distribution planning and design

As part of the planning and design process a number of important decisions have to be made. The choice of these characteristics will influence the efficiency of the distribution methods.

- Depending on the latest product release information, the administrator may have to schedule servers and workstations to be restarted.
- The distribution of central installations should be scheduled for the most convenient time. Client PCs will auto-upgrade as soon as the central installation deployment is complete.
- Auto-upgrading across slow network links or dial-up lines should be avoided (slow links are usually expensive). Using the AutoUpgrade feature on the local area network is much more efficient.
- It is advisable to control the overall number of PCs installing from a single central installation. It is also beneficial to bridge network bottlenecks by pushing a central installation across once, for example, over a slow network connection. This will let the PCs on the other side of the network install quickly from the new/updated central installation.
- The actual number of PCs that can update efficiently from a single central installation can be high (typically 1000 PCs), but the maximum number will depend on the network topology and other factors.
- Placing individual central installations closer (in network terms) to the relevant workstations can reduce or eliminate the impact of auto-upgrading on the network. This can let administrators closely control the way in which the load is generated on the network.
- To complement the AutoUpgrade feature, network protocols designed for local-area networks and those which can multicast to multiple PCs should be enabled. This is opposed to the protocols which are routed (NetBEUI is preferred over TCP/IP). Reductions in network load of up to 46% can be achieved when using the suggested protocols (for the test results on which the above figures are based refer to Appendix A of this document).
- SAV supports roll-back to previous versions. In this case, the administrators can distribute the previous version central installation. All the PCs will automatically roll back to the selected version.
- It is desirable to perform a trial distribution of SAV prior to an enterprise-wide deployment. This gives the administrator an opportunity to identify any potential incompatibilities between the latest releases of software products, operating systems and file systems. Such a trial can be also used to measure the impact of SAV distribution on network performance.

Conclusion

SAV makes use of a number of different distribution methods to achieve efficient deployment and reduce the maintenance effort.

SAV specifically avoids the use of the ‘full push’ technique, providing the effective pro-active ‘pull’ method. The ‘minimal push’ tools (SAV Admin and SwDeploy) have been developed to give the administrator a sufficient level of control over the distribution and configuration tasks.

The SAV distribution tools are an integrated part of the product and tailored to the specification of the targeted platforms. Overall, careful planning prior to the distribution and administration throughout the version life-cycle are the key elements to the successful SAV distribution.

Appendix A. Impact of SAV ‘pull’ updating on the network

In general, predicting network load is a highly speculative exercise. Simplistic theoretical analysis bases the calculation on the result of one update projecting the single update figure over the number of anticipated network PCs:

$$nl=sf*n$$

(*nl* is the overall network load, *sf* is the number of frames sent over the network during a single PC upgrade, *n* is the number of PCs to be updated)

Using the above formula and considering the features of the ‘pull’ technique it might be concluded that the parallel and simultaneous upgrading of multiple clients could have a negative impact on the network in terms of network load and overall throughput.

However, contrary to the theoretical figures, many existing SAV users are regularly distributing SWEEP for Windows NT and Windows 95 to thousands of workstations, with the monthly update task completing within about 10 minutes, without presenting high network utilisation. This agrees with the test results carried out as part of the network load measurement exercise outlined below.

Test configuration

SWEEP for Windows 95 was distributed from a Windows NT 4.0 server with a shared SWEEP for Windows 95 central installation. The workstations were running Windows 95 with Microsoft Network client and the NetBEUI protocol enabled. The network was 10 Mb/s Ethernet. Microsoft Network Monitor was used for measuring the performance.

Single update load tests

The network was at a 0% load before initiation of the update process. The results for a single SWEEP for Windows 95 update were (first run):

1,319	frames transferred
1,002,790	bytes transferred (sb1)
12.55s	update duration
~22%	network load
760.26	average frame size (bytes)

The results for a single SWEEP for Windows 95 update were (second run, different PC):

1,382	frames transferred
1,013,158	bytes transferred (sb2)
16.73s	update duration
~22%	network load
732.60	average frame size (bytes)

Dual SWEEP for Windows 95 update load

The network was at a 0% load before initiation of the update process. The results for a parallel upgrade of two SWEEP for Windows 95 clients were:

Total figures (sent from the server):

1,623	frames transferred (including multicast)
995,014	bytes transferred (pbt) (including multicast)
8.42s	update duration
~31%	network load
613.07	average frame size (bytes)

Total sent to the first PC:

1,422	frames transferred (including multicast)
940,265	bytes transferred (pb1) (including multicast)
8.42s	update duration
~31%	network load
661.22	average frame size (bytes)

Total sent to the second PC:

200	frames transferred (including multicast)
54,625	bytes transferred (pb2) (including multicast)
5.31s	update duration
~31%	network load
273.12	average frame size (bytes)

The correctness of the results is indicated by sb1≅sb2, pbt≅pb1+pb2, pbt≅sb1≅sb2.

The test figures illustrate the fact that the actual number of frames sent over the network does not increase linearly with the number of PCs updating simultaneously. The number of frames sent to an additional PC is reduced due to the boadcast features of the NetBEUI protocol.

One of the most important conclusions is that the number of frames sent over the network during a parallel upgrade <u>*cannot*</u> be calculated by the simplistic formula

$$nl=sf*n.$$

Instead, *pf* (the number of extra frames sent during a parallel upgrade) on an additional PC can be as low as *sf*0.15*.

Note that these figures will vary depending on the network specification and other network traffic. The actual upgrade results can be different if the testing is performed on other network topologies.