Global Information Assurance Certification Paper

Designing a Managed Antivirus Solution for a Large Corporate Environment

By
Collin Speice
Version 1.4 B Option 1
8/27/03
GSEC

Abstract: Designing and Implementing a successful managed antivirus solution in a large corporate environment can be a difficult task. The purpose of this paper is to describe how to design a managed antivirus solution in a large corporate environment. This paper will discuss a solution based on Symantec Antivirus Corporate Edition 8.1 (SAV 8.1) software running on Windows NT, XP and 2000 operating systems. It will not go through every technical detail, or option available, but will touch upon many of the considerations that must be taken into account when designing an Antivirus architecture. Specifically the topics that will be covered are key product features, configuration management, virus definition file distribution, and architecture design. Antivirus gateways, personal firewalls, or other integrated border protection software are not within the scope of this paper.

Antivirus Management Architecture Overview

In recent times it has become more and more evident that antivirus software is vital to an organization's security. Viruses are becoming big news even affecting people that never touch a computer. According to Alex Salkever,

> The back-to-back chaos from Blaster and SoBig caused delays in Amtrak trains, closed banks in Norway, and interrupted Internet service at department stores in Singapore. Departments at several state governments shut down to deal with infected machines, and Air Canada's check-in systems checked out under the weight of the attack." (http://www.businessweek.com/technology/content/aug2003/tc20030826_4386_tc047.htm)

There are many benefits to implementing a managed antivirus architecture. A well-designed system will allow an administrator to see the status of almost every client on the network. It is possible to see what definition files all of the clients are running, and the client's protection status. You can even push out virus definition files from the management system under the right circumstances. The management servers can create a virus sweep kicking off scans on all of the client machines with the touch of a button. Configuration management is perhaps the biggest benefit. Separate antivirus configurations can be designed for specific platforms, server or workstation types, which can be crucial in a world where you have to balance performance and security.

The concepts described in this paper are quickly being adopted by many of the leading antivirus software developers. Trend Micro gives the following insight on managed architectures:

> Management of all antivirus products running on the network must be coordinated to ensure that all virus-entry points are blocked and that virus outbreaks are stopped before they spread and overwhelm your network resources. In addition, it is essential that you can verify that all antivirus programs on the network are using the most recent antivirus pattern file,

scan engine and program version to detect the latest virus threats." (http://it.trendmicro-europe.com/global/products/collaterals/white_papers/tvcs.pdf)

The first step in building a top-notch managed antivirus architecture is to understand the different components. The six most important pieces in managed antivirus architecture are:

- Antivirus Clients (SAV 8.1 client software)
- Management Servers (SAV 8.1 server software)
- Management Console (Symantec System Center)
- Virus Definition Files
- Automatic Update Software (Live Update Client)
- Virus Definition File Host Servers (Live update servers)

Client Software

The first important piece in a managed antivirus architecture is the client software. This software resides on every machine that needs protection. The client software's job is to scan for viruses on the local system. Realtime scanning and scheduled scans are a client's two primary layers of antivirus defense. Client Software should also be able to send and receive information from a management server. According to Microsoft Corporation a user should always "Scan incoming e-mail and attachments. Practice good perimeter protection—scan files before you open them… Schedule weekly disk drive scans." (http://www.microsoft.com/security/articles/antivirus.asp) Symantec has created Symantec Antivirus Corporate Edition 8.1 (SAV 8.1) to perform these tasks.

Virus Definition Files

The most important piece in any antivirus infrastructure is the virus definition file. Clients keep their virus protection current by regularly updating virus definition files. These files contain signatures of all the known viruses and are used by the scan engine. When a new virus comes out the definition files need to be updated so the client software can detect the new virus. The definition files also give the client instructions on how to clean viruses from a file. Updating virus definition files quickly and efficiently is crucial in any business, especially in a virus situation.

Management Servers

Management servers are designed to communicate with the clients. Servers that run the management software are often referred to as "parent servers". Parent servers control their clients and manage their antivirus configurations. In a large corporate environment multiple parent servers that are strategically placed throughout the network will be needed to effectively manage all of the clients.

SAV 8.1 parent servers have the ability to manage multiple configurations for the clients that report into them. This will be discussed in depth further in this paper.

Management Console Software

Special software is needed to connect to and view all of the parent servers in a network. Symantec created the Symantec System Center or SSC to manage parent servers. The software can reside on the parent server itself or a workstation. The SSC allows an administrator to configure the management servers from one centralized view. The SSC also allows the user to view all of the clients under the parent servers, or see properties such as Protection Status, Client IP addresses and virus detections. An administrator can assign configurations, scheduled scans, push virus definitions and set off virus sweeps using the SSC.

Automatic Update Software

In a well-designed antivirus architecture the clients will automatically update virus definition files on a regular basis. Symantec's answer to this is Live Update. The Live Update software downloads virus definitions automatically. Live update is configurable from the management servers. An administrator can set up a live update schedule that best fits their network and security needs. Live update can be configured to connect a host server of the administrators choosing.

In the past Live Update was the most feasible way to distribute definition files to large amounts of clients. This is because live update downloads incremental updates, which are relatively small thus reducing network traffic. Live update software is included in the SAV 8.1 client installs. The virus definition manager in the Symantec System Center can create a customized live update schedule for all of the clients reporting to that parent server. Symantec has also created a randomizer so all of the clients will update at different times within a specified window. Live update can be configured to download files from Symantec's website, or internal servers.

Host Server for Virus Definition Files

Internal virus definition host servers are the final component in a managed antivirus architecture. These servers simply host the virus definition files for the clients to download. Live update simply makes a connection to the server and determines whether new definition files are posted. If they are, the client downloads and applies them. Live update can connect directly to the Symantec website to download definitions, however this poses a risk for a large corporation. Virus definition files should always be tested before they are distributed company wide because they have the potential to crash systems. This concept is covered later in this paper.

Key Product Components

The next step in designing management architecture is to understand the key product components, which are as follows:

- Realtime protection
- Scheduled scans
- Feature lock down
- Alert Management System (AMS)
- Virus definition file distribution

Realtime Protection

Realtime protection is the primary level of antivirus defense on a computer system. Realtime protection works by scanning files when they are manipulated in some way. There are several options that need to be considered when configuring realtime protection. SAV 8.1 clients offer the following configurable options:

- Realtime Protection – This option can be enabled or disabled.
- File Types – This option allows a user to designate what types of files are scanned with realtime protection. Scanning all files, program files or document files are all options. An antivirus administrator can even designate that only certain file types are scanned.
- Scan Files when – This option allows a user to designate when a file is scanned. The default is to scan whenever a file is created, opened, moved, run, copied or run. This can be changed to only scan files when they are created.
- Heuristics – Allow realtime protection to look for virus like activity. Heuristics could theoretically catch viruses that have not been discovered yet. You can set the sensitivity to minimum, default, or maximum protection. The higher the protection the greater the risk becomes for false positives.
- Exclusions – This feature allows you exclude certain file types, or specific files and folders from being scanned. Exclusions are extremely important when troubleshooting performance issues.
- Automatic Enabler – This is a new feature for SAV 8.1. This option allows a user to turn off realtime protection for a specified period of time. The client will automatically turn on realtime protection after the time limit has been met.
- Actions for a detected virus – This determines what actions are taken when a virus is found. Symantec allows an administrator to configure a primary and secondary action for macro and non-macro viruses.

There are other realtime protection options available that have not been mentioned because they will most likely not affect your architecture, but they should be looked at as well.

Scheduled Scans

Scheduled scans are the next layer of protection on a client. A scheduled scan is a full system scan that runs periodically to check the whole file system for viruses. Scheduled scans can be very valuable because a new virus may sneak past realtime protection. Once new definitions are applied that catch the virus a scheduled scan would need to be run to detect it. Scheduled scans have all of the options listed for realtime scanning with a few additional options. You can set up scheduled scans from the management servers. Here is a list of the key options when creating a scheduled scan for SAV8.1:

- Scan Frequency – A scheduled scan can be set up daily, weekly, or monthly
- Scan Time – A scan time must be configured.
- Throttling Options – This option allows a user to designate how much resources the scan uses when the system is idle or in use.
- Missed Events – This option will automatically start a missed scan within a certain period of time. This scan will start when the system is brought back online.
- Remote Options – This option determines whether or not a scheduled scan status bar pops up on the screen. It also determines whether or not a user can stop or pause a scan.
- Storage Migration Options – These options determine how backed up files are scanned.

Feature Lock Down

A good managed system allows an administrator to set antivirus policy rather than users. Well-designed client software should have the ability to be locked down meaning that the end user cannot change key settings. In SAV 8.1 software all of the realtime and scheduled scan features can be completely locked down so the average user cannot change them. This can be a great help in implementing an antivirus policy across an enterprise.

Alert Management System

Alerting is one of the most important features in a centralized management system. "Time is of the essence when new viruses are discovered in the wild. Admins must implement mitigations and update signatures before the virus or worm enters the network. Most management consoles come with alerting mechanisms that tell admins when their AV devices encounter a threat." (http://infosecuritymag.techtarget.com/2002/may/commandcontrol.shtml) Symantec has included an alerting system in their product.

Symantec's AMS system allows a client to send alerts for various triggers. The triggers for an alert are as follows:

- Configuration cchange

- Symantec Antivirus startup / shutdown
- Scan start / stop
- Virus behavior detected
- Virus definition file updated
- Virus found

Once one of the above events is triggered an alert or automatic action will take place if configured to do so. Sending an email, page or SNMP trap can be very valuable. Some alerting is more viable than others in a large network environment. For example sending a page to someone every time a virus is found may not make sense, but sending an email to an account may be a good way to track virus detections.

Virus Definition File Distribution

This whole system would be useless if the clients were never updated with current virus definition files, the key to virus protection. According to David Williams, "it is important to remember that these systems are only as good as their virus definitions. Too often, organizations forget to regularly update their antivirus definitions even though definitions determine which viruses an antivirus application will detect and remove." (http://techrepublic.com.com/5100-6270-1032333.html)

Live Update and Virus Definition Transport Method (VDTM) are the two ways antivirus definition files are distributed to SAV 8.1 Clients. Virus Definition Transport Method or VDTM is a very powerful delivery tool for definition files. VDTM allows definition files to be pushed from the management severs directly to the clients. Previous versions of VDTM were limited because they pushed out the whole virus definition file, which can be close to 5 megabytes. It was simply not feasible to update a large organization's definition files using solely VDTM because of network bandwidth limitations. The new and improved VDTM pushes incremental updates that are very small similar to live update. This is by far the most significant improvement from Norton Antivirus Corporate Edition 7.6. Incremental VDTM updates will allow much more control because definitions can be pushed down by the administrator rather than waiting for clients to update on their regular live update schedule.

Configuration Management

Configuration management can be extremely valuable in a large enterprise. Good configuration management is vital in creating an antivirus policy that can be applied across an entire organization.

> Centralized AV management enables efficient enforcement of security policies by providing mechanisms for routinely applying patches and upgrading software, scanning systems for malware, and configuring AV application settings...Because AV tasks can

impede productivity and functionality, users will often disable scanners or cancel periodic scans. Centralized management gives admins the ability to monitor the status of AV scanners and enforce an organization's AV policy." (http://infosecuritymag.techtarget.com/2002/may/commandcontrol.shtml)

Configuration management also addresses the performance versus security balance. Virus scanning software hooks into the operating system at such a low level that special configurations may be needed for servers running certain applications. For example Realtime scanning exclusions may need to be configured to offset a corruption, or performance issue.

Multiple Configurations

A good management system should allow the administrator to implement multiple configurations from one management server. Previous versions of the SSC forced every client under a parent server had to share one configuration. A client's configuration could be changed individually, but this had a lot of administrative overhead associated with it. Symantec has made a very important improvement by developing the concept of Client Groups.

Client groups allow an administrator to create a hierarchy within the management architecture. It is now possible to manage several configurations from every parent server in your design. Simply create a new client group for every unique configuration and assign clients to the appropriate group. Client groups can span over several parent servers as well. If you are planning a rollout for a large company make sure to define all of the client groups prior to implementation. Assigning the correct parent server and client group to a client is much easier using a script when the clients are installed than moving machines around after the rollout.

Workstation Management

Most of the clients in any large network setting will be workstations. It is important to have a well-designed architecture that accommodates them. Make sure the configurations you choose fit well with your support system. For example if you choose to run scheduled scans at noon on Wednesday chances are a lot of people will be complaining about slow PC performance. Typically most users will be curious about any pop up messages so make sure you have clear messages and directions especially for the message that pops up when a virus is detected. Setting up missed events for scheduled scans can also cause an increase in call volume because they could cause scans to kick off when a user first boots their machine.

Server Management

Antivirus configurations for servers usually need to be much more diverse than with workstations. The first thing to do is get a list of all the different server types

in your environment. Take a good look and mark down which types are business critical and which ones may have potential performance issues. In most enterprises there are going to be servers that need special attention when it comes to their antivirus configurations. Antivirus software can impede performance or even corrupt data in certain circumstances. Microsoft explains why there can be performance problems related with antivirus software in the following text:

> For antivirus solutions to be effective at scanning computer data, they must work closely with the underlying operating system. Many antivirus vendors today individually develop their own file system filter driver to enable on-access scanning functionality. This driver is usually invoked for every file access. A defective driver can be responsible for reliability and performance problems on users' machines including system failure, data corruption, and performance degradation. "
> (http://www.microsoft.com/security/download/virus_protection.doc)

Make sure that you address possible performance issues prior to rolling out. Here are some server types that may need individual attention.

Business Critical Servers

Your company's business critical servers should be a priority when it comes to antivirus protection. High-risk servers such as web, or email servers should also be added to this category. It may be a good idea to update all business critical servers on a more aggressive schedule than the rest of the company. VDTM can accomplish this if the proper architecture and groups are set up for it. Keep this in mind when designing the architecture.

Database Servers

Servers that manipulate large amounts of data can often have performance problems with antivirus software. Setting up appropriate exclusions can minimize impact, but it does introduce risk. Always analyze the risk to see if it acceptable before making changes for performance. Many of your company's business critical servers will most likely be database servers.

Email Servers

Email servers should always get special consideration when it comes to antivirus software because of the threat of viruses that spread through email. Separate software may be needed to protect the mail application your company is using. For example SAV 8.1 was not designed to scan exchange mailboxes. In certain instances scanning a mailbox can cause data corruption and compromise an exchange server. File exclusions are the best way to minimize this risk. Symantec makes software designed specifically to scans exchange mailboxes. SAV 8.1 should be implemented to protect the exchange server's operating system from viruses. The following is an example of a possible problem with an email server:

The protection of the Exchange server is the role of a product like Symantec AntiVirus/Filtering for Microsoft Exchange (SAVFMSE). Certain folders must be excluded from scanning by Symantec AV. If Symantec AV scans the Exchange structure or the SAVFMSE temp folder, it can cause false positive virus detections, unexpected behavior on the Exchange server, or damage to the Exchange databases. This is true of all antivirus programs running on Exchange servers. (http://service1.symantec.com/SUPPORT/ent-security.nsf/docid/2002090916040948)

Large File Servers

Large file servers may have problems completing scheduled scans within a timely manner. You may need to spread the scheduled scan over several days by setting up separate scans for different portions of the drives.

Servers Running other Antivirus Products

Many companies don't put all their eggs in one basket. Having different vendors for different AV products is a common practice many companies follow. Make sure the antivirus software that protects the operating system works with the other antivirus product. Competing vendor software does not always work well together.

SMS Servers

SMS servers may experience issues with antivirus software. Once again setting proper exclusions after you evaluate the risk should minimize the impact.

The goal of examining all of the servers mentioned above is to get an idea of the potential configurations that will be needed. This information will help you organize the antivirus structure into a logical well-planned design. The following checklist should also get you thinking about workstations, server types and business areas that may need special attention.

Checklist

- When should a scheduled scan occur?
- Should a scan status box appear when a scheduled scan is running?
- Should the user have the ability to cancel a scheduled scan?
- What is the maximum time a scan should take?
- Is there a large percentage of off shift workers that may be impacted by nightly scan?
- Do users turn off their workstations at night?
- Do users take their laptops home?
- Should a virus-infected file be deleted if it can't be cleaned?
- Is VDTM, Live Update, or a combination best updating definition files?
- Is live update appropriate for non-emergency situations?
- Should missed events be enabled?

- Should automatic enabler be used?
- What scheduled scan settings will work best with the backup system that is in place?
- What types of messages should the user see?
- Should the user have the ability to manually live update the machine?
- What realtime protection options need to be locked down?
- What time should live update be scheduled to run?
- Does live update need to be randomized during a specific time window to minimize network traffic?
- What servers are “business critical”?
- What servers may have potential performance issues?

Hopefully these questions sparked some ideas that will help determine the configurations that will be needed in your workplace. Once you have a good idea of the types of configurations you will be able to move onto the next step, which is designing the actual infrastructure.

Designing an Antivirus Infrastructure

Designing an antivirus architecture requires an analyst to look at several different factors. The following are all key factors when designing an antivirus architecture:

- Network architecture and geography
- Management server architecture
- Virus definition file distribution architecture
- Testing architecture

Network Architecture

Once all of the Server and Workstation management needs are understood it is time to take a serious look at the environment you are trying to protect. The fist step is to analyze the companies network design. A well-designed architecture will balance cost, network impact, and administration. Here is a list of questions that will help design a management server architecture that fits into a company’s network.

- What are the main regions or segments the network is split into?
- How many workstations are located in each region?
- How many servers are located in each region?
- Where are the network traffic bottlenecks and low bandwidth areas?
- What areas are heavily secured with firewalls?
- Are there any areas that do not have connectivity with the rest of the network?
- What types of network traffic are allowed on the network?
- Is UDP Traffic filtered at any point in the network?

- What types of machines are located in each region? Is there an area that is predominately servers or workstations?
- How will VDTM affect the network?
- How will Live Update affect the network?

The next step in the design process is to determine the management server architecture based upon your network architecture and configuration needs.

Management Server Architecture

The most difficult part is to decide where to physically put the management servers in a network. Dividing the network into regions and listing the amount of nodes in each region can be very helpful. Follow your company's network hierarchy from the bottom up. Try to divide the regions by the bottlenecks and major segments in the network. Keep administration in mind, putting parent servers in too many regions will make your environment more difficult to manage. Implementing too few parent servers may make it hard to apply good configuration management or cause an impact to the network.

Parent servers should be placed in the network at a high enough level that allows large numbers of clients to report to them without impacting network performance at an unacceptable level. Keep network traffic in mind. If your company has a network performance team make sure to utilize their expertise. Management server communications and virus definition file downloads can take up large amounts of bandwidth when you're dealing with hundreds of thousands of computers!

Capacity Planning

The next step is to decide how robust your servers need to be. Make sure to determine the maximum capacity of the parent servers you are going to implement. Make sure the servers are on network segments that can handle all of the client communications. Once you know the maximum capacity of the servers everything else is going to start to fall into place.

Configuration Management Design

Keep management in mind when you are designing the architecture. Define the number of unique antivirus configurations that need to be created for workstations and servers before you start designing. Splitting up parent servers may make sense, for example have separate servers managing your workstations and servers. Determine what groups will need to be created on each parent server. Creating too many client groups will add to administrative overhead and will be very difficult to implement. Remember, clients are assigned to the parent servers. If you create 100 separate client groups you will need to assign the clients to them appropriately. In a network with over 100,000 clients this may prove to be very difficult.

Regional Architectures

Each major region of the network should be treated like it is it's own entity. A separate antivirus architecture should be made for each region. For example if you divide your network into three major regions, you will most likely need to make three separate architectures. When I refer to architecture it may mean only one parent server for a smaller network, or more depending on the size of organization. Determine the number of servers and workstations in the region and plan the number of parent servers accordingly.

Virus Definition Update Architecture

The way you distribute definition files will be one of the last components in your design, but one of the most important You may want to update high priority servers on a more aggressive update schedule than the rest of the organization. To do this you would probably want to keep the high priority servers separated from the rest of the clients by putting them into their own group or parent server. You need to keep bandwidth in mind if you are planning on using VDTM company wide during virus outbreaks.

Placing the virus definition host servers in the correct place is also important. Make sure the servers are scaled to handle the amount of traffic that will be going to them. Redundant systems may be a good idea when implementing an internal Live Update host server. If one system goes down you don't want to be unable to update definitions. Think about using non-windows based operating systems for your live update servers because they may not have the same vulnerabilities as the rest of the organization. If you split up your parent servers based on network capacity you will most likely need to do the same for the live update servers. Look at putting the Live Update servers in the same regions as the parent servers.

Testing

Never update virus definition files in your production network before testing them. A separate architecture should be created that allows and administrator to test virus definition file updates, scan engine updates, and other fixes. Take testing definition files seriously, a corrupt set can reap havoc in large network. A well-planned test center architecture should allow you to test definitions on a small amount of machines first. Once initial testing has completed they should be distributed to a larger portion of test equipment or perhaps an entire test center. Testing is necessary even during a virus outbreak. The following example illustrates that testing should not be taken lightly:

> Symantec also found itself in hot water on Monday after customers using Symantec AntiVirus Corporate Edition reported that an automated antivirus definition update from the Cupertino, Calif.-based company caused the antivirus software to fail. Symantec's antivirus software would not start on desktop systems that installed the faulty update, leaving some customers without antivirus protection on desktops and servers running

the software.
(http://www.infoworld.com/article/03/06/25/HNsymantecunderfire_1.html)

Conclusion

A well-designed centrally managed antivirus solution is essential in protecting an organization against viruses. Managed architectures offer benefits such as configuration management, reporting, and alerting. Managed AV solutions aid in the distribution of virus definition files, which need to be constantly updated to keep protection current. Most companies are moving towards managed solutions because of these benefits.

> Centralized AV management solutions aim to provide enterprises with a bird's-eye view of their AV defenses and granular command and control. The basic feature set of all AV management suites is the ability to see all users on the network, know what application versions they're running, efficiently and expediently update virus signatures and policies, and receive alerts and other reports.
> (http://infosecuritymag.techtarget.com/2002/may/commandcontrol.shtml)

Designing an architecture can become difficult very quickly if some key concepts are unclear. It is essential to understand the main components and functionality of the software you plan to implement prior to designing the architecture. Keep network capacity, antivirus policy needs and virus definition distribution in mind when creating the design. Business critical and other potential problem servers should be given special attention. Define the areas that need separate antivirus configurations and your design will be successful.

References

Koziol, Jack. “Command and Control” Information Security. May 2002
URL: http://infosecuritymag.techtarget.com/2002/may/commandcontrol.shtml (27 Aug. 2003)

Microsoft Corporation. “Improving Virus Protection for Customers” 10 June 2003
URL: http://www.microsoft.com/security/download/virus_protection.doc (26 Aug. 2003)

Microsoft Corporation. “Security and Privacy for Home Users.” 2 April 2002
URL: http://www.microsoft.com/security/articles/antivirus.asp (26 Aug. 2003)

Roberts, Paul “Symantec under fire for bugs, flaws” 25 June 2003
http://www.infoworld.com/article/03/06/25/HNsymantecunderfire_1.html (26 Aug. 2003)

Salkever, Alex. “The Ever-Growing Virus Crisis.” 26 August 2003
URL:
http://www.businessweek.com/technology/content/aug2003/tc20030826_4386_tc047.htm (26 August 2003)

Symantec Corporation. “How to prevent Symantec AntiVirus Corporate Edition from scanning the Microsoft Exchange directory structure” 9 September 2003
URL: http://service1.symantec.com/SUPPORT/ent-security.nsf/docid/2002090916040948

Symantec Corporation. “Symantec Antivirus Corporate Edition Administrator’s Guide”
URL:ftp://ftp.symantec.com/public/english_us_canada/products/symantec_antivirus/symantec_antivirus_corp/8.1/manuals/sav8.1_admin.pdf

Trend Micro. “The Need for Centralized Antivirus Management to Protect Against Internet
Aware Computer Viruses”
URL: http://it.trendmicro-europe.com/global/products/collaterals/white_papers/tvcs.pdf (26 Aug 2003)

Williams, David. “Client vs. Server Protection” 16 April 2001
http://techrepublic.com.com/5100-6270-1032333.html (26 Aug. 2003)