Global Information Assurance Certification Paper

Implementing A Norton AntiVirus Managed Infrastructure

by
Rodney Lynxwiler
GSEC
version 1.3
original submission
SANS Peachtree

Abstract

The purpose of this paper is not to go into a history of viruses, or even spend paragraphs describing how viruses work. I'd like to concentrate on some of the practical aspects of rolling out a managed antivirus solution to a large company, specifically for workstations and servers. If you spend any time at all perusing vendor documentation, you know there are holes, gaps and sometimes large crevices of missing information that are needed to make the practical decisions. That, coupled with the typical corporate politics and red tape, can send you into a tailspin! But, with some planning, forethought and good advice from people who have gone through it before, successful managed antivirus protection can be implemented. And, just think of how good it will feel when the next virus is thwarted before it has a chance to negatively impact the company's resources.

This paper will examine how to roll out a centrally managed antivirus solution using Symantec's Norton Antivirus Corporate Edition 7.6. We will go beyond the general implementation guidelines to the detailed considerations and lessons-learned. We will specifically examine rolling this infrastructure to a large enterprise environment, with many different physical locations throughout the country and well over 100,000 total nodes. We'll look at four considerations: Client configurations, updating definitions, reporting and network traffic. Antivirus protection at the workstation and server level is still a key element in the total defense plan against viruses.

"The bottom line is that malicious code events are on the rise, both in frequency and alleged financial damages…" (Wired, 1/2002)

Many papers have been written on malicious code and there is some great information on the different types of viruses, vulnerabilities and strategies that are used by "the dark side." In general terms, this information is good and beneficial. It helps those who are fairly new to the information security field understand the enemy and how to protect against some of the more common attacks. In specific terms, it helps us all to be smarter geeks.

But, when it comes right down to it, how does a person take his or her knowledge of viruses and vulnerabilities and actually roll out a solution that will protect the company? Worse yet, roll out that solution to a large company, with more than 100,000 nodes and multiple locations across the country. Want more punishment? Roll out multiple solutions in the same timeframe to the same company and be expected to develop a centralized reporting mechanism.

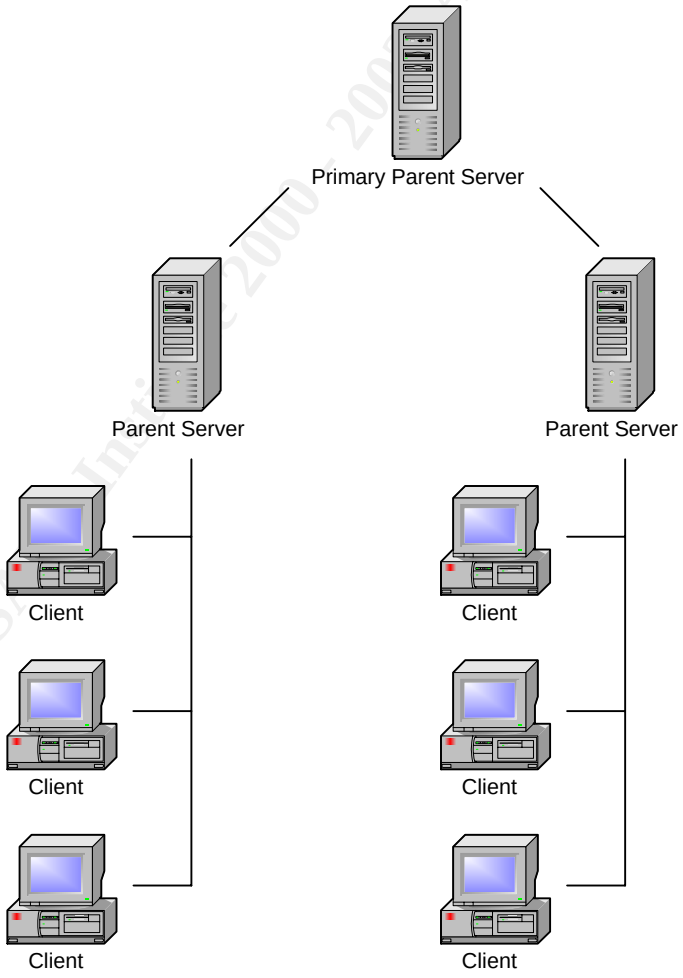
Millions of pages of documentation have been written on describing what danger lurks out there past your firewall. In fact, there are enough white papers on the internet to keep

you reading for years!! But, when the search is narrowed to only include practical, detailed steps for rolling out protection layers, the pages quickly dwindle.

Let's start with a brief overview of what this infrastructure will look like. Basically, each workstation and server will be "managed" by a Norton AntiVirus parent server. These parent servers can either be dedicated servers used exclusively as parent servers, or shared servers, used for other duties as well. It must be noted that they can manage more clients if they are not shared with any other functions. The parent servers are assigned to server groups and a server group can contain more than one parent server.

Each server group must have one parent server designated as the primary parent server. The primary parent server is responsible for updating definitions, configurations and all tasks for other servers in the server group. Configuration changes can be made at the server group level, which results in every parent server in that group receiving the changes.

Below is a basic diagram of how this infrastructure looks.



Now that we have a visual understanding of the infrastructure, let's go a little deeper and look at some of the significant considerations to keep in mind during the planning and deployment.

CONSIDERATION #1: Updating Definitions

"The need for up-to-date virus protection is greater than ever before, say security managers and analysts, because of the increasing importance of e-commerce and e-mail, which expose corporate systems to more hackers." (Computerworld, "Managing the Virus Threat")

The ability to keep definition files updated is the key to any virus protection. Without current virus definitions, antivirus software is practically useless. Keeping definitions current in a large enterprise is an ongoing challenge, but one worth fighting.

There are two native ways to update definitions in Norton Antivirus 7.6: LiveUpdate and the Virus Definition Transport Method (VDTM). Each way works differently and is tailored to different types of situations.

LiveUpdate is an incremental update, which means the client only downloads the definition files that are new since the last time they were updated. This results in less required network bandwidth. The average download size is around 250 kb, assuming the client is fairly up-to-date. One thing to note here is that if Symantec bundles a new scanning engine update in the definitions (which happens a few times a year), the size could be as much as 1.5 MB. LiveUpdate is triggered either manually by the end-user through the LiveUpdate button on the client software or by scheduling the client to automatically check for newer definitions.

One of the best ways to set up LiveUpdate is to install a LiveUpdate server internal to your company, which will serve the definition files to all your clients. The number of servers you would need and configuration of those servers will depend on your network topology and the physical location of your clients.

With NAV 7.6, there are three choices for connection types between the clients and the LiveUpdate servers:

- LAN
- HTTP
- FTP

The LAN method is not a preferred method because it must be configured with a username and password, which is stored in clear text in the registry. The HTTP method is a very popular method because of the universal availability of port 80. FTP is also a good method, assuming that every node in your company has port 21 enabled. (Harvel, Symantec)

INSIDE TIP: LiveUpdate can be configured to handle "missed events"—times when LiveUpdate is scheduled to run, but the computer is turned off. This forces LiveUpdate to run the next time the computer is booted if it missed its original scheduled time. But, if your company has mobile users, or those who take their laptops home on occasion, you need to realize one thing about missed events: If a laptop is on, but not connected to the network, either through the network card or modem, and LiveUpdate's schedule says to check for new definitions, this is not considered a missed event, even though the network was not reachable.

The definition files are not applied until the full set of files are downloaded. So, if there is a problem during the download process, it will not result in a corrupted set of files being used, possibly causing NAV to not work properly. A negative aspect of LiveUpdate is this: if a bad set of definition files is distributed using LiveUpdate, you cannot fix this by backdating the definitions; you must wait for a corrected set of definitions from Symantec and distribute those out.

With VDTM, definitions can be backdated, so that you can revert to a previous set of definitions that are proven good. But, unlike LiveUpdate, there is a possibility of corrupted definitions if a problem occurs during the download process.

Definition files distributed using VDTM are sent to the clients from the parent servers as soon as the parent server receives them. VTDM is a push operation which is initiated when a server receives new definitions. The file that is pushed to the clients is large in size, as it contains an entire set of definition files.

CONSIDERATION #2: Client Configurations

The first question you will face will be how much do I lock down this environment? I don't think anyone would argue with the fact that antivirus protection is needed on workstations and servers. In fact, the ICSA labs 2001 annual prevalence survey indicated that "respondents were clearly inclined to believe the problem of computer viruses in general was much worse than in 2000. Of the respondents, only 28 percent felt the problem was about the same or better. Conversely, almost three-quarters (72 percent) of them felt the problem was somewhat worse or much worse." (ICSA, p. 13)

"Experts state that the number of viruses and their severity reached an all-time high in 1999. Deploying antivirus software and developing antivirus policies and procedures should be high on the list of New Year's resolutions for any mid-sized IT department that doesn't have them yet." (Utopia Place, Virus Management)

The problem of computer viruses is not getting better. But, there are some considerations that must be addressed as you plan your protection.

Newer versions of antivirus software, like Norton AntiVirus Corporate Edition 7.6, provide administrators with easy ways to lock down options that end-users could potentially change. The most significant of these would be the ability to turn realtime protection on and off. Each time a user is allowed the choice whether or not to disable realtime protection, a potential hole is opened in your protection. A lot of viruses spread on the basis of end-user ignorance. Since the majority of emails are spread via email, more and more users are faced with decisions on whether to execute an attachment or not. Viruses and malicious code are disguised in appealing attachments that lure an end-user to satisfy their curiosity by opening it. In fact, a recent visible virus, W32.Alcarys.D@mm, comes disguised as an alphabet testing game. (Alcarys, SARC) An average user with average curiosity would find it hard not to open this attachment!

Experience has shown that users tend to blame antivirus software for everything from slow performance to Dr. Watson errors to their screen saver not working. Given the chance, they will disable antivirus as their first steps of troubleshooting. **Remember: your AV protection is only as strong as your weakest user** (and, for that matter, your weakest workstation or server).

One of the biggest struggles of a large, enterprise environment is to maintain current antivirus protection on desktops and servers. It's almost inevitable that in a virus infection situation, someone who has previously disabled realtime protection ends up being responsible for infecting other parts of the company with the virus.

One thing to remember is that, even though realtime protection may be locked down, a user with local administrator rights would be able to stop the Norton Antivirus client service, thereby turning off realtime protection.

Options are locked down primarily through the Parent Server with the Symantec System Center, which provides the centralized management console. When configurations are set, most options have a padlock button that allows the administrator to lock down that option so it cannot be changed by the end user. Another way to lock options is by manually editing the GRC.DAT file. This file, which also contains configuration settings that are made through Symantec System Center, provides the way these settings are merged into the registry.

> **INSIDE TIP: Want a fast way to lock down client settings? If you use Norton Antivirus 7.6 and make settings by manually editing the GRC.DAT file, you can lock down options by typing a exclamation point before the option in the GRC.DAT. This file can then be distributed to the clients with locked-down options.**

As the administrator makes configuration changes through the Symantec System Center, these settings are written to the GRC.DAT file on the parent server. Also, the settings are written to the registry on the parent server under the following path:

HKLM/Software/Intel/LANDesk/CurrentVersion/ClientConfig

When you click the OK buttons on the configuration screens, a value is changed under the **HKLM/Software/Intel/LANDesk/CurrentVersion/ProcessGRCNow** registry key. This indicates that there are new configurations available and a new GRC.DAT needs to be pushed out to clients. Then, the parent server feeds the new GRC.DAT file to all its clients. This allows all clients to receive updated settings, including any configurations that you choose to lock.

There are some things to keep in mind as you change and lock options. If you make a configuration change, but do not lock that option, the connected clients will not receive the change. The reason for this is because Norton Antivirus (NAV) assumes you don't want to enforce that configuration because it was not locked. However, any new workstations that connect to this parent server in the future **will** receive the new configurations. But, if you make configuration changes, then hit the Reset All button instead of the Ok button, all clients will receive the configurations, regardless of whether those configurations were locked or not.

Locking down the ability for a user to unload the NAV services and forcing a regular scheduled scan will help to ensure that users don't weaken your antivirus defenses.

> **INSIDE TIP: Norton Antivirus 7.6 relies heavily on the registry to hold all configurations. Be careful to allow plenty of size for the registry.**

CONSIDERATION #3: Reporting

If there is one major downfall of NAV 7.6, it is the lack of adequate centralized reporting. For large companies with many server groups, quickly running reports can be a cumbersome process. In order to collect data into one report, you would have to export the logs from each server group into an Excel spreadsheet or other delimited file format. Depending on how you connect to the parent servers for administration, gathering this information could take a long time.

Another option is the AMS or Alert Management System. AMS runs on each primary parent server and allows an administrator to customize the alerts that are generated during various events. Some of the events include configuration change, NAV startup/shutdown, virus definition file update and virus found. If an event occurs for which you have set an alert, it generates a thread. The NAV service (RTVSCAN) forwards a VIB (Virus Information Block) to the client's parent server. When the parent server receives this, it enters it into its AMS log. Then, the VIB is forwarded to the primary parent server, which gets entered into the AMS log there, and the action is executed. The actions that are associated with the different events include message boxes, pages, internet mail, broadcasts and a write to the event log.

For example, you can configure AMS to send a page to your support team each time a virus is detected on any client. This helps to centralize the alerts that you care about most.

But, back to the issue of reporting. Part of effectively managing secure antivirus protection is being able to know what is going on at any given time. Let's say a user introduces a virus into your network via their workstation that has outdated definition files. Wouldn't it be nice to be able to track the spread of the virus to see if it can be contained in a certain region of the country? Or a certain department in your company?

What if your management asked you for a report of yesterday's virus activity across your company? How fast could you get a report together?

One of the biggest needs in antivirus protection is the ability to centrally manage and report on what is happening in your company.

One of the best ways to get around NAV's shortcomings is to set up a way to get virus detections back to a central repository. There are a few software packages that can do this and one of the best is from Aelita. Aelita can be configured to grab events from the event log of a Windows NT or Windows 2000 machine. Since AMS can be configured to enter NAV events into the event log of the Primary parent server, Aelita can then be used to pull these events back to a central reporting server. Setting up a SQL server to collect these events allows a lot of flexibility in the programming and set up of a reporting instrument that meets the needs of your company. In fact, Aelita has over 20 built in reports specifically for Norton AntiVirus.

CONSIDERATION #4: Network Traffic

Another consideration in setting up a managed antivirus infrastructure is network traffic. If all your nodes are contained in one physical location, this won't be an issue. But, if there are workstations and/or servers scattered across many physical locations, especially if they are located throughout the country, network traffic should be a concern. There are plenty of "network traffic generators" in NAV 7.6. Obviously, when you think of this being a "managed" environment, with clients checking in with a parent server, you must assume that there is some network traffic. But, when you begin to examine exactly what causes network traffic, how often that traffic is caused and the sizes of the traffic, you begin to realize that this environment could be a network bandwidth eater if not properly planned.

Server groups should be set up so they don't span WAN links. NAV uses IP, UDP and RCP protocols to communicate in various situations, so keep this in mind as you plan your infrastructure.

There are roughly five major categories of items that generate network traffic under NAV 7.6, which I will explain in more detail:

- Events (virus detections, scan information, etc.)
- Keep-alive packets
- Configuration downloads
- Definition file updates
- Other miscellaneous traffic

Events

There are certain events that are automatically forwarded from the clients to their parent server. These events include a scan start, scan stop, scan abort and virus found. After the parent server receives these alerts from its clients, it forwards these alerts on to the primary parent server. Each of these events is approximately 250 bytes, so this can result in significant network traffic, depending on how many virus alerts are received and how often scheduled scans are run.

Keep-alive packets

A keep-alive packet is sent from the client to its parent server. This packet contains client information such as machine name, user that is logged on, date of the definition files, last date a scheduled scan was run and IP address along with other miscellaneous information. This is a UDP packet that is generated once every 60 minutes by default. Its approximate size is 50 bytes.

Configuration downloads

Configuration settings for the clients are made through the Symantec System Center on the parent servers. If only some configurations are changed, resulting in a "partial" GRC.DAT file being pushed to clients, the size would be around 300 bytes. If the "Reset All" button is pushed on the configuration screens, this results in a full GRC.DAT file being generated, and the size can be anywhere from 6 kb to 30 kb.

Definition file updates

We have already mentioned the two ways get updated definitions files to clients: LiveUpdate and VDTM. Both methods have advantages and should be investigated in light of your current network and what would work best for your topology. We have discussed these in detail, but for the sake of this discussion, let's now look specifically at the network traffic generated for each type.

The update process for LiveUpdate is:

- Source files are downloaded from Symantec (approx. 16 MB)
- Client, based on its schedule, checks with LiveUpdate server for new defs (approx. 5 bytes)
- A file, livetri.zip, is downloaded to the client. This is the catalog file that NAV uses to see if it has the newest definition files (approx. 6 kb)
- If newer definitions are available, the clients downloads the needed files from the LiveUpdate server (approx. 250 kb)

LiveUpdate can be scheduled, so there is some flexibility on how you distribute the load. "When setting options for scheduled LiveUpdate sessions for servers and clients, you can specify advanced settings…Randomize LiveUpdate schedules for multiple computers to minimize the impact on network traffic." (Implementation Guide, p. 195) In this way, you can stagger the updating and minimize the impact to the network.

The process for VDTM is as follows:

- Source file is downloaded from Symantec (approx. 5 MB)
- A .vdb file is created that is approx. 3 MB in size
- This .vdb file is sent down from the Primary parent to all the other servers in the server group
- The file is then pushed from the servers to their connected clients

Other Miscellaneous Traffic

The Discovery Service, Find feature and Refresh feature are other ways that network traffic can be generated. When a local Discovery is initiated, the Symantec System Center broadcasts to the entire subnet, looking for other parent servers. If there are other servers out there, they respond with information about themselves, including the clients that are reporting to them.

If an intense Discovery is initiated, every server in the Network Neighborhood is pinged. Obviously, in a large network, this can take a while to complete and generate a large amount of network ping traffic.

Instead of ping discoveries, you can also use the Find feature to ping a certain server. There is little traffic generated from this type of activity.

If the Symantec System Center console view is refreshed at the server group level, a ping is sent out to all members of the server group. If it is refreshed at the server level, every client that reports to that server is sent a ping. Depending on the number of clients assigned to a particular parent server, this could generate a large amount of traffic.

To get a better idea of the network traffic generated, let's look at an example of an average workday in a typical, large environment. For example, if there are 100,000

workstations that have scans scheduled for execution on Thursdays, each workstation would generate two events: one for the start of the scan and one for the stop (or abort) of the scan. So, a scheduled scan running on Thursday would result in approximately 50 MB of network traffic from clients to parent servers. Not too bad? Don't forget that those same events are also forwarded to the primary parent server. Now the total size is up around 100 MB. Add in the keep-alive packets that are sent once every 60 minutes. That's another 5 MB per hour, which equals 120 MB per day. So, we're up to 220 MB from 100,000 clients running a scan and generating keep-alive packets.. If clients are set to LiveUpdate once a day (which is recommended by Symantec) (Harvel, Symantec), you will have that additional download traffic.

As you can see, if you don't take time to plan this infrastructure, getting a handle on network traffic can be a challenge.

In recent months, it seems like firewalls, email gateways and HTTP scanning devices have become the popular instruments against virus detection. While these additional layers of protection definitely enhance the total security picture, workstation and server protection are still crucial parts. "Efficient procedures combined with the right security tools can provide the best insurance against computer viruses and subsequent data loss. For large companies this means the same level of protection needs to be available for all the operating systems that are included in their networks." (Norman, 2/23/2000) Being able to centrally manage this protection has allowed administrators to provide better protection in a timelier manner.

In today's world of viruses being released almost on a daily basis, virus protection has become a daily challenge. But, with antivirus vendors finally releasing virus protection software with the large company in mind, there is a much better chance that we can go home on time at the end of the day!

References

1. Bridwell, Lawrence M. and Tippett, Peter. **ICSA Labs 7th Annual Computer Virus Prevalence Survey 2001**. URL: **http://www.truesecure.com/html/tspub/whitepapers/icsasurvey.pdf**

2. Lesniak, Tim. Utopia Place, **Survey Says …**, Virus Management. URL: **http://utopiaplace.com/research/surveys/survey_says.html**

3. **Norton Antivirus Corporate Edition Implementation Guide**. URL: **ftp://ftp.symantec.com/public/english_us_canada/products/norton_antivirus/navcorp/manuals/navce75i.pdf**

4. Scheier, Robert L. **"Managing the Virus Threat,"** Computerworld. May 7, 2001. URL: **http://www.computerworld.com/cwi/story/0,1199,NAV47_STO60208,00.html**

5. Harvel, David. **Symantec Corporation Consulting Services**. Personal Interview. October, 2001.

6. Alcarys Virus. **Symantec AntiVirus Research Center**. URL: **http://www.sarc.com/avcenter/venc/data/w32.alcarys.d@mm.html**

7. Press Release, **Norman Data Defense Systems**, "Big Business for Norman Virus Control." February 23, 2000. URL: **http://www.norman.no/uk/news/pr000223.shtml**

8. Delio, Michelle. **Find the Cost of (Virus) Freedom**, Wired News. January 14, 2002. URL: **http://www.wired.com/news/print/0,1294,49681,00.html**