# Norton AntiVirus C.E 7.6

For Dos, Win3.1, Win95, Win98, NT, Win2000, ME, XP.
Other Modules included in package:
Nav for Notes, Nav for MSExchange, Nav For FireWalls (CVP), Nav for Palm, Nav for Mac, Nav for Gateways.

***By Andre Botelho***

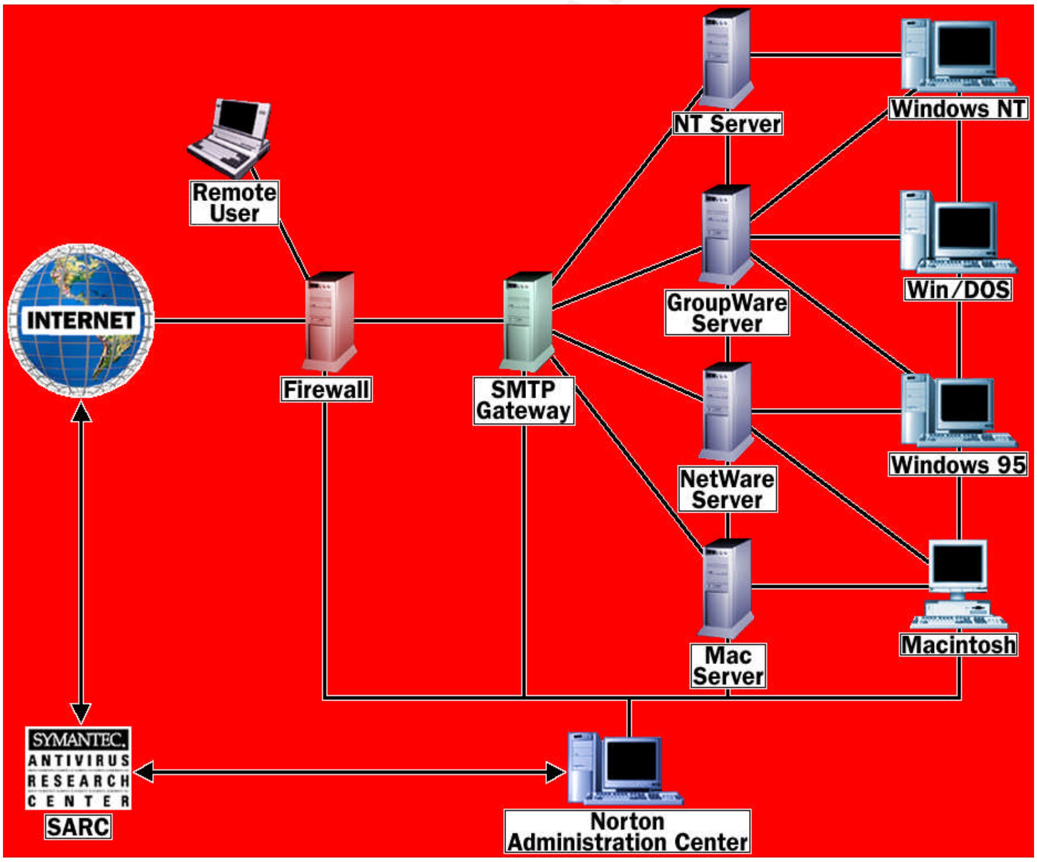
## Index:

## Introduction:

Since the Introduction of Norton Antivirus 7.x, Symantec have managed to created a truly remarkable product with full single point manageability, centralized quarantine, single engine (NavX), remote rollout (Push Based from Console), Web based installer (Pull) , single definition set for all flavors of Nav (Using MicroDefs), customizable Liveupdate technology (Centralized Microdefs) and something new called the Digital immune system ©. Just to mention a few of the new features. In this document I will cover most of the new fetchers of NavCE, I have also included some URL's at the end of the paper that you can feather research this product.

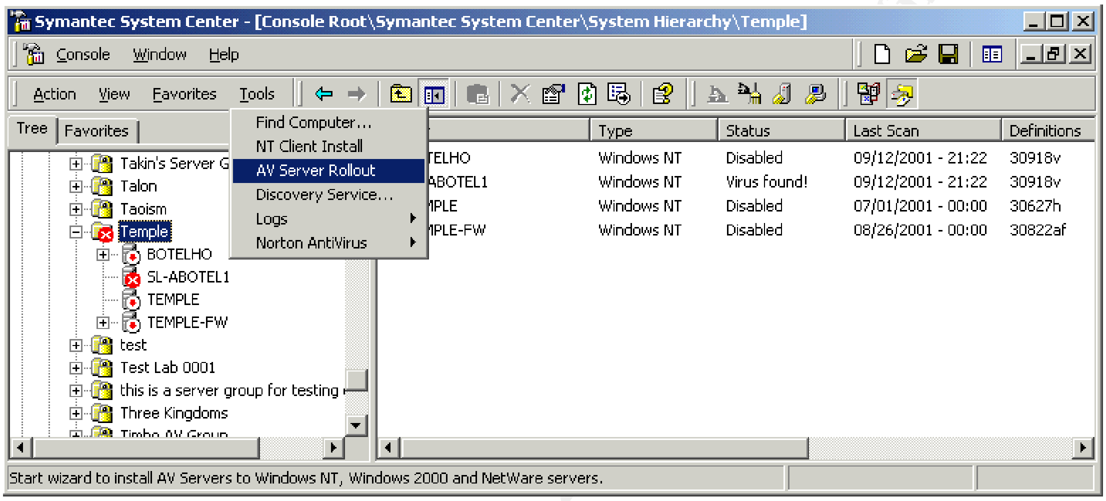
Now with Microsoft Terminal Servers as well as Microsoft Windows® XP support.

**NavCE basic Structure:**



## Rolling out the Product:

One of the new feature of NavCE is the ability to remotely push the product over the WAN, from a single point to Windows (Intel) based PC's, this can be easily achieved by either a push (From within the console, See Diagram bellow) or a pull via the Web based installer, there is also a packaging tool to assist other product like Tivoli or MSXXXX to be used.  This can also be achieved from CD2.



| | Type | Status | Last Scan | Definitions |
|---|---|---|---|---|
| TELHO | Windows NT | Disabled | 09/12/2001 - 21:22 | 30918v |
| ABOTEL1 | Windows NT | Virus found! | 09/12/2001 - 21:22 | 30918v |
| MPLE | Windows NT | Disabled | 07/01/2001 - 00:00 | 30627h |
| MPLE-FW | Windows NT | Disabled | 08/26/2001 - 00:00 | 30822af |

Start wizard to install AV Servers to Windows NT, Windows 2000 and NetWare servers.

## MSI Installer explained:

**http://service1.symantec.com/SUPPORT/nav.nsf/docid/2000101109523706**

***Behind the scenes:***

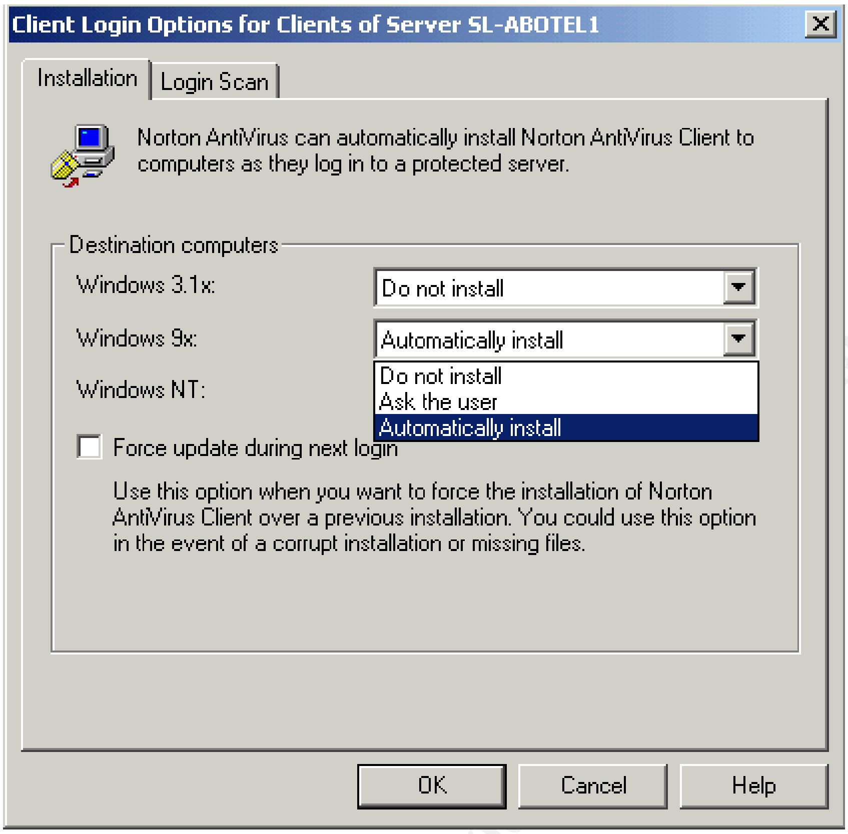
***Upon the install of NavCE (Server), Nav will create two shares on the NT/Win2000 server:***

***\\servername\VPHOME***
***<drive>:\Program Files\nav\***
***This is the root folder for NavCE on the server. NavCE installer files live in the 'clt-inst' sub folder.***

***\\servername\VPLOGON.***
***<drive>:\Program Files\nav\logon***
***This folder contains all batch files and tools to remote install NavCE.***
***'VPLOGON.BAT' is the file that NavCE uses to remotely install itself.***

*Ps. Before using this batch file, NavCE must be configured from the console to allow this function (See diagram bellow).*

*Under 'Client Login Scan and Installation' on the server from within the console.*



Client Login Options for Clients of Server SL-ABOTEL1

Norton AntiVirus can automatically install Norton AntiVirus Client to computers as they log in to a protected server.

Destination computers

Windows 3.1x: Do not install

Windows 9x: Automatically install

Windows NT:

□ Force update during next login

Use this option when you want to force the installation of Norton AntiVirus Client over a previous installation. You could use this option in the event of a corrupt installation or missing files.

*From this Menu, NavCE is able to enable what will happen when the 'VPLOGON.BAT' file is executed, this ranges from, 'Do Nothing' (Default) to 'Ask the user' (Prompt the user if he would like to install NOW!), to 'Automatically install' (Do a silent install NOW!). There is also a 'Force update during next login' tick box (This will force a full reinstall of the product on login).*

*Login Scan tab. This option enable the System admin to make NavCE do a command level scan of the users workstation every time he logs in to the network providing that 'VPLOGIN.BAT' is part of everyone's login script.*

*There is also a WEB Based installer that must be pre-configured prior to install. Please follow the link bellow for a detailed set of instructions:*

**http://service1.symantec.com/SUPPORT/ent-security.nsf/docid/2000091810135748**

**@ the CORE! – GRC.DAT – Symantec Ref.**

The Grc.dat file is a file in text format that functions as a repository of changes that were made to a group of clients.

There are several versions of the Grc.dat file on a parent server. One version appears in \Program Files\NAV (or for Windows 2000 systems in \Documents and Settings\All Users\Application Data\Symantec\Norton AntiVirus Corporate Edition\7.5). This version of the Grc.dat is copied to the client to initiate options changes at the client level. Another Grc.dat file appears in each of the \CLT-INST directories. Each of these is copied to the client during installation to the client. A third Grc.dat is in the rollout directory of Disk 2. It is a "bare bones" version, with some commented lines that allow you to turn on and off LiveUpdate, or to specify a parent server.

Any time you modify client options from the Symantec System Center console at the server group level or server level, this information is updated on the clients' parent server.

When you modify server options, no matter from which level you make the modifications, you are directly modifying the registries of the selected servers via the Transman communication method. Transman uses dynamic libraries that include CBA (Common Base Agent) and NTS (Network Transport System).

*Grc.dat for servers (Grcsrv.dat)*

The Grc.dat for servers is called Grcsrv.dat. This is currently only used to apply group settings to a server when it is moved into a new server group. The new server group must have a primary server. The Grcsrv.dat has the same format as a Grc.dat. This file is not propagated like a Grc.dat file. It is created only when synchronizing a server to a new server group's settings. This only works for NAV CE 7.5 servers. For older servers, the topology service will copy registry settings from the primary to the server being moved.

The Grcsrv.dat was implemented because it is slightly faster than copying registry settings directly. Also, it is a forward looking change since it puts grc processing code on the server, and it may assist in making future enhancements backwards compatible.

**A brief summary of how the Grcsrv.dat works**

Like Grc.dat, Grcsrv.dat is a file representation of a registry hive. Grcsrv.dat is created from the DomainData key, similar to the way Grc.dat is created from the ClientConfig key. This is done at the request of the topology service. The topology service copies the Grcsrv.dat file from the primary server to a secondary server. The topology service then instructs the secondary server to process the Grcsrv.dat. This processing is similar to the client processing. However, it is not automatic.

The Grcsrv.dat mechanism is backed up by the method of copying registry settings directly. It should therefore not currently need troubleshooting.

*The role of the primary server*

The primary server acts as the repository of all server options on a server group level. If you make modifications at the server group level, the changes are recorded in two places:

- In the registry of the primary server for that server group in the CurrentVersion\DomainData sub-key.
- In each of the other servers.

The CurrentVersion\DomainData key contains all the entries found under CurrentVersion, including the ClientConfig key. (See the section "The role of the ClientConfig key" for more information.)

*The role of the ClientConfig key*

The Client Config key on the CurrentVersion\ClientConfig level contains all the option changes for the clients of the server that is being selected for action.

The Client Config key under the CurrentVersion\DomainData\ClientConfig key (on the primary server) contains the client options for all the clients of all the servers in the server group. Note that the options are only recorded here if you have changed the options at the server group level.

If you make a client configuration change at the server group level, the ClientConfig key at the CurrentVersion level on the primary server will change so as to affect the options of its children. The ClientConfig key under CurrentVersion\DomainData will also change so as to affect the children of all the secondary servers in that group as they receive the registry changes from the Console.

*Where changes are recorded*

The process changes if you modify client options at the server level. The options changes are written to the registry of the server under CurrentVersion\ClientConfig. The options are then bundled into a Grc.dat file and sent to the clients. RTVSCAN on the client then converts the options to registry keys in the clients' registry, and then deletes the Grc.dat file.

If you modify client options at the server group level, all changes are written to the registry (CurrentVersion\ClientConfig) of the primary server for the benefit of the primary server's children. The options are written to the \Nav\Grc.dat file on the primary server and pushed to the primary server's children.

The changes are also written to the registry to the CurrentVersion\DomainData\ClientConfig sub-key. These changes are then written to the secondary servers' registries, and then a \Nav\Grc.dat file is written and pushed to the clients of each of the secondary servers.

*How the Grc.dat is written*

When you make a change to client options on a group level, the changes are recorded in the ClientConfig registry sub-key. The changes are next written to the \Nav\Grc.dat folder, and then pushed to the client, where the changes are incorporated into the client registry.

When you click OK from the Symantec System Center Console to changes on the server group level, the ProcessGRCNow sub-key under CurrentVersion\ProductControl on the affected server moves to 1 from 0. RTVScan on the server has a thread monitoring this key. When RTVScan sees the move from 0 to 1, it rebuilds the Grc.dat file in its \Nav directory, and resets the value to 0. Another thread then feeds the Grc.dat to all of its clients, locating it in the clients' \Nav directory, where the local RTVScan can find it. Every 60 seconds the local RTVScan runs a CheckGRC call (configurable in the registry). When the local RTVScan finds a Grc.dat file, RTVScan converts it to registry entries, and then deletes the Grc.dat.

**More than one change at a time**

When you click OK the first time to change options, the ProcessGRCNow value changes to 1. RTVScan begins to process the changes into the Grc.dat file, and then pushes the updated file to its clients. In the meantime, you may have made more changes and clicked OK again, or perhaps two or more times. Each time you click OK, the ProcessGRCNow value is checked. If the value is already set to 1, it stays there. If the value is set to 0, it is incremented to 1. RTVScan has then finished pushing out the Grc.dat file with the first OK change. Now RTVScan can return its attention to the ProcessGRCNow key. RTVScan sees that the value is again at 1, and starts the process over. Now, though, RTVScan has all the accumulated changes going into the new Grc.dat. The changes are processed per normal and pushed out to clients. RTVScan checks one more time for the value of ProcessGRCNow. If the value is still at 0, RTVScan goes back to sleep and watches for changes. If the value is at 1, RTVScan begins the process again until ProcessGRCNow returns to a 0 value.

*ProductControl\Debug*

To display a debugging window, open the CurrentVersion\ProductControl registry sub-key, and then change the Debug key to a value of "verbose." A DOS window appears where any action performed by RTVScan is recorded. For example, if you make a client option change at a server or server group level, the entire process described in the previous section is viewable on screen.

To capture the data in a file, add "logging" after the verbose setting. Note that both settings may slow a system considerably.

*Editing the Grc.dat file*

You can make changes by manually editing the Grc.dat file. See below for examples:

- !KEY!=$REGROOT$\AdministratorOnly means that a key called AdministratorOnly will be added to the registry under HKLM\Software\Intel\LANDesk\VirusProtect6\CurrentVersion

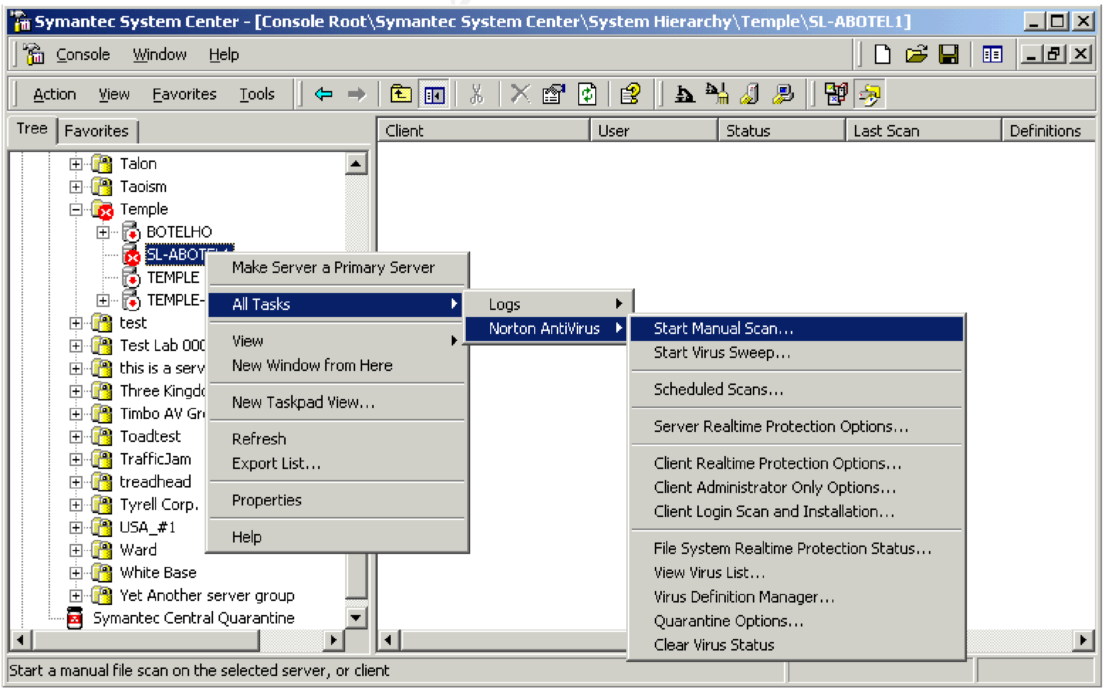
  Any additional lines of text up to the next instance of !KEY! are key values.
- !KEY!=$REGROOT$\AddressCache\GUESTROOM

  Below this line, you could add a line such as "test=D1."

If you then copy this modified Grc.dat file into the Program Files\Norton AntiVirus folder on the client (or for Windows 2000 clients into \Documents and Settings\All Users\Application Data\Symantec\Norton AntiVirus Corporate Edition\7.5), in less than a minute the Grc.dat will convert to a registry entry. The key and value you defined will be created.

## The Console:

NavCE is managed from within MMC (Microsoft Management Console), from within the console you can fully manage NavCE, ranging from a simple check of an overall company Virus stat to selecting a remote directory on a PC for a scan. This can be achieved very easily by a simple right mouse clicking on the relevant level that you would like to command. E.g. if you would like to do a manual scan on a folder on a remote workstation (On the right window) under its master server (On the left window). In fact most commands can be achieved this easily, you just have to right click on the relevant level to execute the command you wish.. (See Diagram bellow).

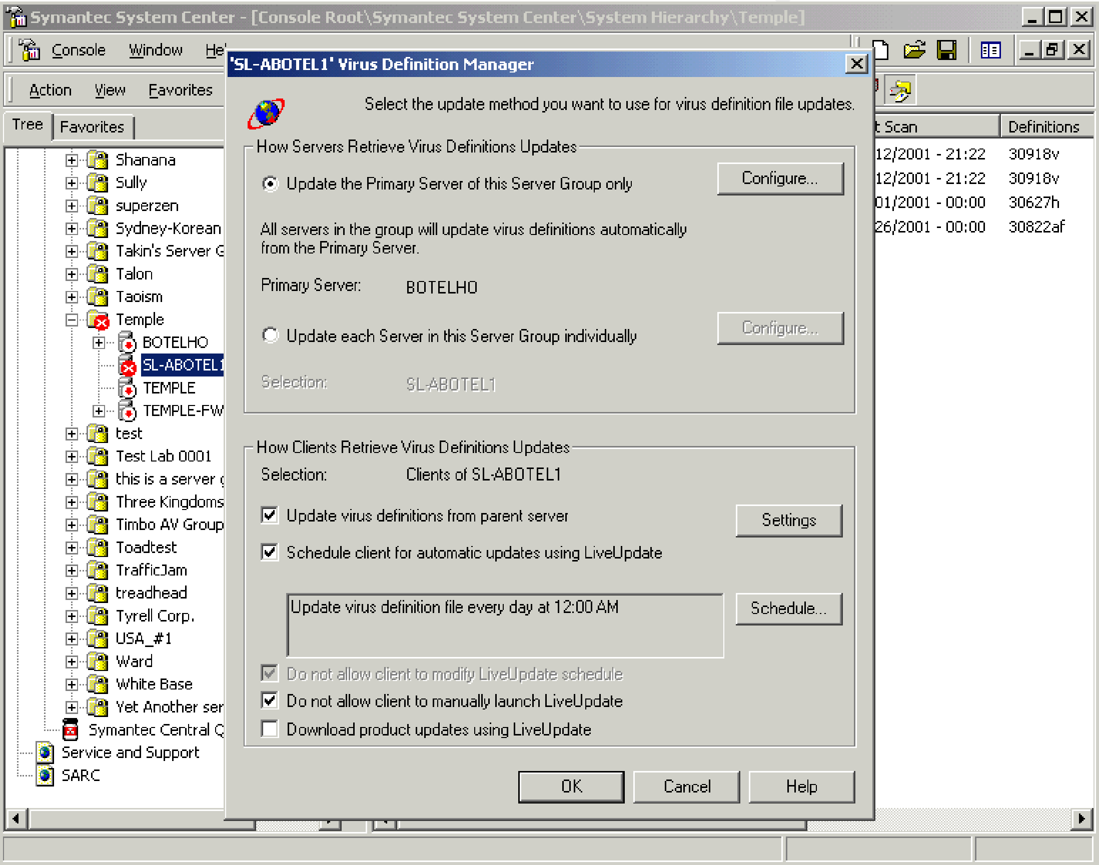


Start a manual file scan on the selected server, or client

## Keeping NavCE up-to-date:

NavCE Incorporate a great and easy technology call Liveupdate that uses MicroDefs, Liveupdate is the ability to do a single click to update NavCE via the internet to the latest Definition, MicroDefs is the ability to download only what's new (The deference) from your current definition to the new definition.

To setup NavCE to automatically just right click on the master server in your group and select 'Virus Definition Manager…" from here you will have full control of how, when, and where NavCE will do its updating… See Diagram bellow.



Symantec System Center - [Console Root\Symantec System Center\System Hierarchy\Temple]

'SL-ABOTEL1' Virus Definition Manager

Select the update method you want to use for virus definition file updates.

How Servers Retrieve Virus Definitions Updates

● Update the Primary Server of this Server Group only [Configure...]

All servers in the group will update virus definitions automatically from the Primary Server.

Primary Server: BOTELHO

○ Update each Server in this Server Group individually [Configure...]

Selection: SL-ABOTEL1

How Clients Retrieve Virus Definitions Updates

Selection: Clients of SL-ABOTEL1

☑ Update virus definitions from parent server [Settings]

☑ Schedule client for automatic updates using LiveUpdate

Update virus definition file every day at 12:00 AM [Schedule...]

☑ Do not allow client to modify LiveUpdate schedule

☑ Do not allow client to manually launch LiveUpdate

☐ Download product updates using LiveUpdate

By selecting the 'Configure' you can easily Schedule when to download, where, and how.

From here you can also customize how and when the clients will download the definitions from there muster server.

***Some Background:***

***NavCE out of the box is setup to automatically download the latest definitions to the master server on Fridays. Following a successful download, all sub servers in the group will request the latest definition from there master server, once all servers have been updated, all workstations will be updated from there local servers automatically!***

**The Digital Immune System:**

**Bloodhound discovers new virus**

Symantec's Bloodhound heuristics engine scans files to seek activity that may be viral in nature. Immediately when a suspicious file is identified, it is securely quarantined to prevent the user from inadvertently activating the virus and spreading the infection. In addition, a copy of the infected file is forwarded to the Central Quarantine Server where it can, if necessary, be sent to the network of Symantec AntiVirus Research Labs (SARC) around the world for analysis, after the system has stripped out any confidential or sensitive data if required.

**Central Quarantine**

Whether the customer updates on a weekly or monthly schedule, Central Quarantine can be configured to download and use the latest certified definitions from Symantec. As a result, Central Quarantine will scan all in-coming submissions forwarded by the Local Quarantine to check if the most current Symantec update will solve the customer's problem upfront, without having to submit the file to SARC for analysis. If the infection is a previously unknown virus, the file is submitted automatically or manually by the administrator to SARC for further investigation using a technology called Scan & Deliver.

**Scan & Deliver**

Scan & Deliver is essentially a secure communications link between the customer and Symantec's backend response infrastructure via Central Quarantine. Until the Digital Immune System, anti-virus vendors' primary method of communication was e-mail. However, because today's viruses threaten the very existence of e-mail itself—either because the customer shuts down mail systems as a precautionary measure during an outbreak, or the mail server crashes due to the sheer overload of email traffic—email is no longer a reliable transport mechanism in emergency situations. Furthermore, email is based on store-and-forward technology and loses some of the real-time benefits that a web link can provide. As a result, Symantec has augmented the communications link by adding a secure web link (HTTP using SSL).

**Immune System Gateways**

When the customer submits a file to Symantec from the Central Quarantine console, the meta-information for the file is first sent to an Immune System Gateway. At this Gateway, the file's 'fingerprint' or checksum is checked against a database of known clean files, known new viruses, false positives, and previous submissions. This not only ensures that the customer receives the quickest possible response for submissions that are not virus-related, it also means that Symantec is not flooded by redundant or unnecessary submissions. When a submission is deemed to be 'new', i.e., it potentially contains a previously unknown virus, then and only then is the actual file transmitted to the Gateway and forwarded to Symantec's back-end virus response infrastructure. For redundant submissions, the Gateway queues the submission and awaits a response from SARC.

**P's and Queues of Rapid Response:**
Once a file lands in the queue at SARC, it is again processed using the latest 'uncertified' cures generated either by a SARC researcher or by automated systems. If the file is believed to contain a previously unknown virus, the first stage is for it to be processed by SARA (Symantec AntiVirus Research Automation), a unique automated system designed and built together with IBM to handle definition creation for the majority of new viruses. SARA is to the anti-virus world, what Big Blue is to the chess world, in that it has built-in logic to analyze and generate cures for viruses. Essentially, SARA attempts to coax the virus into replicating, analyzes its behaviour, identifies a signature or fingerprint, generates a detection and repair routine, and tests the fix against all replicated variants of the virus. If SARA is 100% successful in generating and testing a fix, the fix is made available to those customers with infected files. If not, the file is passed to human hands for further analysis.

Although many viruses still require human expertise, the vast majority (over 80%) of boot, macro, and DOS executable viruses can be cured using automated techniques such as SARA. Both SARA and human researchers in SARC and Technical Support are tied to the same control and backend management systems to ensure that there is no overlap and that cures are available to anyone who requires them. In addition, customers can check the real time status of the submission via the Central Quarantine console.

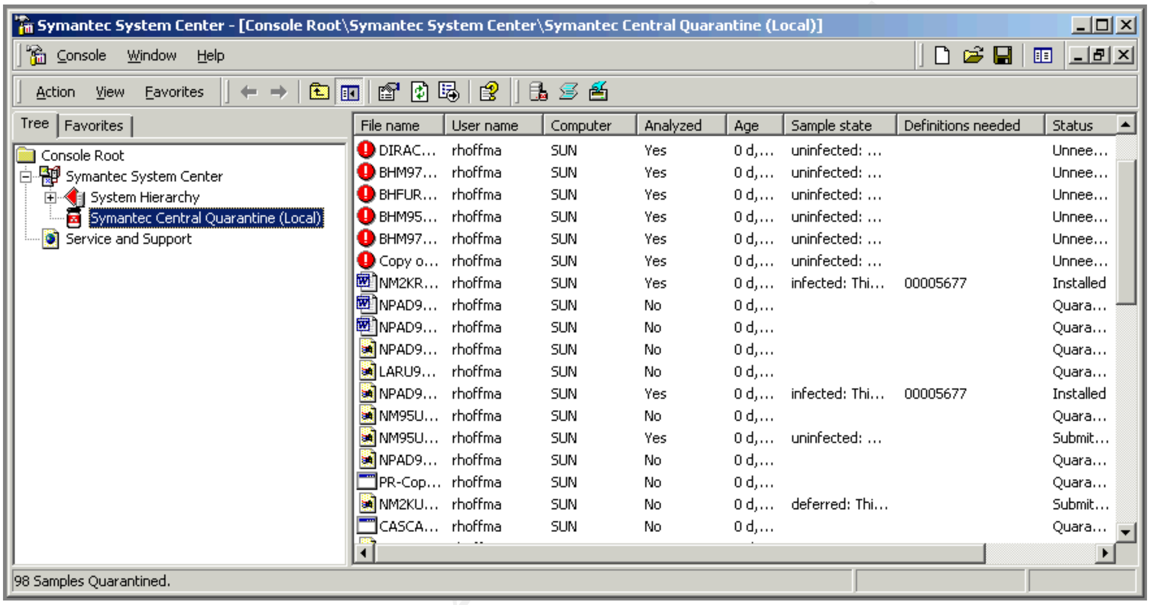
**Sending the cure downstream:**
Once the cure is available, the SARC submission queue is again checked to ensure that all submitted files that have the same virus receive the cure automatically at the same time. The cure is then forwarded downstream to the reporting Immune System Gateway(s) and back to the customer site via a secure Internet connection to the Quarantine Console. At the same time, the cure is replicated across all Gateways to ensure that the next customer submitting the same sample gets the cure in real-time.

**Immunizing the network:**
Both the cure for the submitted virus-infected file and the certified definitions can be automatically and securely delivered to the customer's Central Quarantine console—the customer's 'emergency control center' for combating the spread of virus infection. From here, the administrator can target individual computers, subnets, or LAN segments for emergency updating. This forced or pushed update ensures that the administrator can fight the spread of viruses in real-time and not depend on the same fixed schedule that is used for the weekly updates. Updates are pushed down from the Central Quarantine to the respective 'parent servers' and from there, using a fast, multi-threaded technique, are sent to the individual workstation and server nodes.

**Summary:**

Through a rapid, automated response infrastructure like the Digital Immune System, Symantec can leverage the network effect inherent in its large and growing customer base to provide its customers with rapid, 'Internet time' response to the latest threats. In addition, high levels of automation means that more than 10,000 submissions per hour can be handled, and Symantec's backend infrastructure is protected from being overloaded in the event of a LoveLetter or Melissa-like global virus outbreak. Regardless of where a new virus appears, in the Philippines, in Hong Kong or in Anchorage, Alaska, the cure can be disseminated as rapidly, perhaps even more rapidly, than the virus can spread.

## Centralized Quarantine console



Symantec System Center - [Console Root\Symantec System Center\Symantec Central Quarantine (Local)]

Console Root
- Symantec System Center
  - System Hierarchy
  - Symantec Central Quarantine (Local)
- Service and Support

| File name | User name | Computer | Analyzed | Age | Sample state | Definitions needed | Status |
|---|---|---|---|---|---|---|---|
| DIRAC... | rhoffma | SUN | Yes | 0 d,... | uninfected: ... | | Unnee... |
| BHM97... | rhoffma | SUN | Yes | 0 d,... | uninfected: ... | | Unnee... |
| BHFUR... | rhoffma | SUN | Yes | 0 d,... | uninfected: ... | | Unnee... |
| BHM95... | rhoffma | SUN | Yes | 0 d,... | uninfected: ... | | Unnee... |
| BHM97... | rhoffma | SUN | Yes | 0 d,... | uninfected: ... | | Unnee... |
| Copy o... | rhoffma | SUN | Yes | 0 d,... | uninfected: ... | | Unnee... |
| NM2KR... | rhoffma | SUN | Yes | 0 d,... | infected: Thi... | 00005677 | Installed |
| NPAD9... | rhoffma | SUN | No | 0 d,... | | | Quara... |
| NPAD9... | rhoffma | SUN | No | 0 d,... | | | Quara... |
| NPAD9... | rhoffma | SUN | No | 0 d,... | | | Quara... |
| LARU9... | rhoffma | SUN | No | 0 d,... | | | Quara... |
| NPAD9... | rhoffma | SUN | Yes | 0 d,... | infected: Thi... | 00005677 | Installed |
| NM95U... | rhoffma | SUN | No | 0 d,... | | | Quara... |
| NM95U... | rhoffma | SUN | Yes | 0 d,... | uninfected: ... | | Submit... |
| NPAD9... | rhoffma | SUN | No | 0 d,... | | | Quara... |
| PR-Cop... | rhoffma | SUN | No | 0 d,... | | | Quara... |
| NM2KU... | rhoffma | SUN | No | 0 d,... | deferred: Thi... | | Submit... |
| CASCA... | rhoffma | SUN | No | 0 d,... | | | Quara... |

98 Samples Quarantined.

From this console, NavCE has the ability to quickly centralize all files that it does not know what to do with. E.g. Possibly infected files, viruses that cannot be cleaned (possibly a new variant). Here the system admin. is able to make a few decisions on how to process the file, NavCE can request a new set of definitions from SARC (Symantec Antivirus Research Center) then re-scan or he can manually examine the file prior to sending it back to the user. Another new fetcher of NavCE is the ability to package and submit the possibly infected component of the file to SARC.

## Web Based Installer

NavCE has a full web base installer that lives in the sub folder:
<drive>:\Program Files\nav\clt-inst\WEBINST

Here NavCE has a subset of files that can be put up on a web server to make a HTML base install very easy, just by executing the file 'DEFAULT.HTM' from a web browser, you will be prompted to install NavCE.

***Background:***
*There is some basic editing of 'DEFAULT.HTM' that must be done prior to a successful implementation of this system.* ***Please follow the link bellow…***

**http://service1.symantec.com/SUPPORT/ent-security.nsf/docid/2000091810135748**

### Notes 5 & Outlook plugin

Norton AntiVirus client-based email protection for the Lotus Notes and Microsoft Exchange systems runs constantly, and is capable of catching and repairing virus-infected attachments before the user accesses them.

### MSI installer support

Currently Norton AntiVirus Corporate Edition (NAVCORP) 7.5 utilizes only a few of the new technologies of the Windows installer, e.g. rollback capability. If NavCE installation fails, It safely roll the machine back to its previous state, which is a considerable action for an installation as complex as NavCE. The installation of NavCE uses several Microsoft merge modules that allow us to update critical system files while not breaking Windows 2000 certification rules. Through the use of merge modules NavCE can update system DLLs. NavCE is also in the process of converting its email snap-ins to features, which will allow for installation on-demand. NavCE also make use of public properties, which allow modification of the installation from the command line, even during silent installs. NavCE can also take advantage of command line switches.

### How NavCE Communicates & TCP/IP – Ports

### The Primary Server

When you bring up the primary server of a server group, Ping Discovery Service (PDS) loads as a service. It always listens at UDP port 38293 for pings from other computers and responds to them with a pong data packet for registered applications. More on registered applications later.

If PDS load successfully, then RTVSCAN loads. TRANSMAN, which is a part of RTVSCAN, requests a port on which to listen. With NAV CE 7.5, a specific, or static, port is requested first. It requests this static port so that, on subsequent reboots of the server computer, RTVSCAN will listen on the same port. This makes communication more stable between computers, as other computers (Consoles, as well as Servers / Clients) will not have to resolve the correct port each time through PDS to find out where RTVSCAN is listening on that computer.

The static ports are specified in the registry and are written by the installation process. RTVSCAN uses the following registry key and values to determine the port on which to listen:

HKEY_LOCAL_MACHINE\SOFTWARE\INTEL\LANDesk\VirusProtect6\Current Version

AgentIPPort - (DWORD) 2967

AgentIPXPort - (DWORD) 33345

Prior to NAV CE 7.5, and as a fallback in the event of the static port failing, RTVSCAN will use a dynamic port. This port will be assigned by WINSOCK on that server and can be different every time you request a port.

As part of TRANSMAN's initialization process, RTVSCAN, using TRANSMAN, registers itself with PDS as "an application named x" where x is a hard-coded number for that application. This registration process is what provides the pong data packet, which PDS provides to applications pinging it from across the network.

RTVSCAN then tells PDS to listen for pings asking about it. If PDS hears a ping asking about that application number, then it is supposed to send back the pong packet as a reply. This communication is done through a memory mapped file, rather than APIs or other means.

So now we have RTVSCAN listening on a port assigned to it by Winsock. It told PDS that it is named X, staying in room #N, and asked PDS to listen for anyone coming to calling for it. It has given PDS a message to deliver to anyone calling for it: "Hi. I'm staying in room #N. This is my full address, room number, and some other information you might want to know about me later."

PDS continues to listen on port 38293 for pings coming from the network and passes the pong data packet to anyone who asks about the status of "an application named x."

### The Secondary Servers

Secondary servers do exactly what the primary servers do. The secondary servers determine the identity of the primary servers during installation, however, they do not know their location. They learn where to find their parent in one of two ways:

- If the parent has been contacted and has not moved, then he simplest way is to look in the AddressCache registry key. This key contains everything necessary to find their parent.
- If the parent has moved, then it must be rediscovered. The secondary server looks up the server's address using Win32 APIs (pings the server name). Once it obtains the IP address, it pings that address at port 38293, since that is the port where PDS listens. PDS replies with the pong packet of the parent. The secondary server reads the pong packet, finds out the port on which RTVSCAN is

listening, and tries to connect with it. It tries to connect on both IP and IPX. If both of these methods fail, then the secondary server gives up.

**How does a client make contact with the parent server?**

When a client is installed and local RTVSCAN is first loaded, the client initializes TRANSMAN, which then makes a call to WINSOCK requesting a static port first and then any free port as a fallback, the same as the servers do.

The port information is stored in a keep-alive packet, which looks remarkably similar to a pong packet. It cannot be a true pong packet because there is no PDS service that loads on a client, not even an NT client. Internally, it uses a pong data packet, the same as in server discoveries. It gathers the same information through the same functions, but reports it through a "COM_ALIVE" communication directly to its parent server, which then writes this information to its own "CLIENTS" registry key.

Local RTVSCAN then processes the contents of the Grc.dat file if it finds one in its program directory. This would be placed there as part of the installation process. It will contain configuration information and also the parent server's name. The contents of the Grc.dat file are parsed into the registry on the 32-bit clients and the Vpccc16.ini file on Win3x clients.

The parent server's name is now resolved to an IP or IPX address, the same as for servers using OS-level calls.

Now that it knows the address of its parent server, it can ping the server to get the port number that Server's RTVSCAN is listening on. (It pings at port 38293, and PDS running on that port replies with a pong packet that tells which port to find RTVSCAN listening on.) The client RTVSCAN (or its equivalent RTVSCN95) can now send its keep-alive packet to the parent server's RTVSCAN, and communication can begin. This keep-alive packet contains the client name, GUID, server group, parent server, and so forth.

When RTVSCAN on the server receives the keep-alive packet, it registers that client as its child and adds it to its Clients key. At this point, any discovery from the console will now elicit a response from the server that includes this client.

**The Symantec System Center Console and Discovery**

When NSCTOP starts, it initiates a quick discovery, which is essentially a broadcast ping to the entire subnet. It asks that any application listening on port 38293 please respond with a pong packet. Any computers running PDS will respond to the ping with a pong packet.

NOTE: NSCTOP always performs a quick discovery. If you configure it to do intense discovery, it will always perform a quick discovery first.

Any PDS running on any Norton AntiVirus server that hears this ping will respond with a pong datagram, which contains information including the server name, server group, and the port on which RTVSCAN is listening.

The console for that group then stores this address and port information in its address cache.

When the administrator clicks on a server to reveal its clients, the console queries that server's registry for a list of its client computers. These are stored in the Clients key of the server.

All communication between RTVSCAN is performed by the Intel communication method: TRANSMAN and NTS working together. If the console is talking to a server, then all calls go through NSCTOP and use Transman.dll.

### Ping/pong

When discussing how the discovery service works, it is imperative that we understand what is meant by the idea of *ping/pong*.

### Ping packet

A *ping packet* is a network packet that is sent out by a console, or any computer needing to find an application on a remote computer that is running the Intel Ping Discovery Service (PDS). Many different portions of the product send ping requests to locate products through PDS.

In order for a console, or any other portion of the product to locate RTVSCAN, RTVSCAN must first register a *pong packet* (described in the next section) with PDS. To do this, during startup RTVSCAN acquires a port on which to listen, and then gathers all of its AV information together into a packet to submit to PDS. When the packet is complete, it registers with PDS under its Application ID. NAV CE 6 and earlier use a new APP ID from previous versions. The APP IDs for the old and the new versions of NAVCE are:

Old ID - CBA_ID_LDVP  0x5056444CUL  /*LANDesk Virus Protect 6 and earlier*/
New ID - CBA_ID_LDVP2 0x4D436948UL  /*NAV CE 7 and later*/

Pings are sent from the console on both the old and new APP IDs in order to locate all AV Servers running on a network.

All pings are sent to the Intel PDS running on a static port. The static ports for PDS are:

| | |
|---|---|
| IP - | 0x9595 (38293) |
| IPX - | 0x8857 (34903) |

This port must remain static in order for this service to function. This is the single point of entry to locate any product that is registered with PDS. This provides one static point of entry, which can then turn around and provide the location (port) and additional information about any number of products that can register with PDS.

This is very similar to many other services, such as the Remote Procedure Call service, which provides endpoint mapping for RPC functions running on a machine. Instead of having every remote function listen on a different port, an RPC service runs on a static port, and resolves the endpoint of an RPC call.

A ping packet contains 16 bytes of our data (total network size of 60 bytes).

### Pong packet

A *pong* packet is returned from the Intel PDS service to the requesting application on behalf of the registered application.

A NAV Server, or RTVSCAN, pong packet contains information about how to contact RTVSCAN (port information), and lets the pinging party know about AV information such as its current definition set, time of last virus infection, and so forth.

A pong packet contains 458 bytes of our data (total network size of 500 bytes).

Only AV servers are discovered using this ping/pong mechanism. Client information is found by querying the server for its client information.

### AMS - Alert Management System

Alert Management System (AMS$^2$) provides sophisticated emergency management capabilities. AMS$^2$ supports alerts on NetWare 3.12, 3.2, 4.1x, and 5.x servers, Windows NT servers and workstations, and Windows 95 and 98 workstations.

AMS$^2$ is a robust and fault-tolerant alert system with no single point of failure. While other alert handling mechanisms require a functioning network in order to send and receive alerts, AMS$^2$ can send and receive alerts when the network has failed or is only partly functional. AMS$^2$ can generate alerts through these the following methods:

- Message Box
- Broadcast
- Send Internet Mail
- Send Page
- Run Program
- Write to Windows NT Event Log
- Send SNMP Trap
- Load an NLM

### How AMS alerts are transferred from Norton AntiVirus into AMS$^2$

RTVSCAN on a client machine waits for an event thread that requires an alert. These threads can be generated by the following events:

- Configuration change

- Default Alert
- Norton AntiVirus Startup/Shutdown
- Scan Start/Stop
- Virus Behavior Detected
- Virus Definition File Update
- Virus Found

If you have configured an alert for any of these events, when the event occurs it will generate a thread. This prompts RTVSCAN to create a “Virus Information Block,” which it forwards to the client’s parent server. When the parent receives the virus information block, it enters it into its AMS log. The virus information is then once more forwarded, this time from the parent server to the primary server, which makes an API call to AMS, which enters the information into the AMS log – a database named AMSDB – and acts on it, depending on how you have this particular alert configured.

Communication in AMS is carried out via CBA, which is part of the Intel Communication Method.

| Service name | Binary name | Description |
|---|---|---|
| Console | | |
| Symantec System Center Discovery Service | Nsctop.exe | Discovery service used to find AV servers on the network. |
| AMS | | |
| Intel Alert Handler | Hndlrsvc.exe | AMS2 Alert handler service. Provides alerting actions such as message boxes, pages, emails, etc. |
| Intel Alert Originator | Iao.exe | AMS2 Alert Originator service. Allows for alerts to be received on this machine. Alerts can be received from either the local machine (in the case of a primary server) or a remote machine (in the case of unmanaged AV clients using a centralized AMS server). |
| Intel File Transfer | Xfr.exe | Intel file transfer service. Provides file transfer capabilities to AMS. |
| Intel PDS | Pds.exe | Intel Ping Discovery Service. This service allows for discovery of products on this machine. Applications register with this service, along with an APP ID (Such as LDVP) and a packet to return in response to ping requests (pong packet). |

| | | |
|---|---|---|
| NAV CE Server | | |
| Norton AntiVirus Server | Rtvscan.exe | Main Norton AntiVirus service. The brains of the AntiVirus server are contained in this service. Most AV server-related tasks are performed in this service. |
| Defwatch | Defwatch.exe | When new definitions arrive, RTVScan notifies the Defwatch service. Defwatch then picks up the new definitions and scans quarantined items. |
| Intel PDS | Pds.exe | Intel Ping Discovery Service. This service allows for discovery of products on this machine. Applications register with this service, along with an APP ID (Such as LDVP) and a packet to return in response to ping requests (pong packet). |
| NAV CE Client | | |
| Norton AntiVirus Client | Rtvscan.exe | Main Norton AntiVirus service. The brains of the AntiVirus client are contained in this service. Most AV client-related tasks are performed in this service. |
| Defwatch | Defwatch.exe | When new definitions arrive, RTVScan notifies the Defwatch service. Defwatch then picks up the new definitions and scans quarantined items. |
| Quarantine Server | | |
| Symantec Central Quarantine | Qserver.exe | Accepts infected files from servers and clients and communicates with Quarantine Console. |
| Symantec Quarantine Agent | Icepack.exe | Handles communications between Quarantine Server and the AV gateway. |
| Symantec Quarantine Scanner | Scanexplicit.exe | Scans submitted files using Quarantine Server's personal set of definitions. |

**References:**

**Company Web Site:**
**http://www.symantec.com**

**Product Page:**
http://enterprisesecurity.symantec.com/products/products.cfm?ProductID=23&PID=5928044

**SARC – Symantec Antivirus Research Center:**
http://www.sarc.com

**Knowledge base:**
http://www.symantec.com/techsupp/bizsolutions/nav/main_nav-75-ce.html

**Advanced Technology Review:**
http://www.technologyreview.com/magazine/sep00/benchmark7.asp

**IBM Research Center:**
http://www.research.ibm.com/antivirus/