NOVELL INFORMATION SERVICES AND TECHNOLOGY

ManageWise @ Novell

A Beigepaper

by Grettir Asmundarson (grettir@neticus.com)

Last Revised: January 24, 2000

A Service Of Novell's Information Services & Technology Global Technical Architecture Group

Patent pending. All sales final. Void where prohibited by law. No purchase necessary. Low in saturated fat. Do not read this document if the printed seal is broken or missing. Do not drive a vehicle or operate heavy machinery while reading this document. Call a physician if swelling persists. The author's wanton use of the "@" symbol does not necessarily reflect the sensibilities of the author himself, who is personally opposed to the gratuitous use of internet-related typographic symbols. :-(

About The “@ Novell” Series

Most documentation starts as hastily scrawled notes from sleep-deprived developers who weren’t necessarily hired for their keen communication skills. Those notes are then fleshed out by recently graduated English majors who have spent their last four years immersed in works of fiction. The results are then passed on to the marketing department whose job it is to make sure that no word or phrase, even if it’s true, will reflect unfavorably on the product (“I don't think that the word ‘Basic’ properly communicates the exciting nature of the product. Why don’t we call it ‘Visual Zesty!?!’”). It is then beset by lawyers who finish the job by making sure that they haven’t explicitly promised that the product will actually do anything.

By the time the documentation gets into your hands, it has been so sanitized for your protection and generalized beyond recognition that you usually have to go out and buy a 3rd-party manual (that was, more likely than not, written by the same non-technical technical writer who wrote the original documentation) in a vain attempt to get an unbiased, unexpurgated, and/or unfiltered view of just how you’re really supposed to use the stuff.

That’s where the “@ Novell” series comes in. Rather than the vague, generalized, and wholly fictional examples found in most documentation, we’re going to tell you exactly how we use our own products to run our own company. After all, we are not a small, tidy computing environment suitable for documentation. We are a big, sprawling, untidy environment made up of over 500 production servers and 20,000 workstations in 130 locations throughout the world. In other words, we’re probably an awful lot like you.

And it’s not that we’re necessarily any smarter than you are, we just have a distinct advantage. By the time you get your hands on one of our released products, we’ve already been using it to run our business for quite some time. For instance, a month before NetWare 5 shipped, well over half of our 500 production file servers had already been upgraded to NetWare 5. (Keep in mind that these were production servers. These were not test servers that we had safely tucked away in antiseptic labs. These were real-world servers in a real-world environment solving real-world problems.) And two months before NetWare 5 shipped, we’d already converted one of our buildings to IP Only. That means that we’ve probably gained some insights into implementing our products in a big, sprawling, untidy environment, and this paper is an attempt to share those big, sprawling, untidy insights with our customers.

But keep in mind that this document may be a little rough. It wasn’t conceived by a committee, written by a committee, or approved by a committee, so it hasn’t been edited, re-edited, tidied up, sanitized, and whitewashed. Don’t think of this as an official whitepaper. It’s more like a beigepaper.

The EUNUCH System

I have developed what I think is one of the most innovative management solutions in the industry. I call it the End-User Notification & Ubiquitous Complaint Hotline (EUNUCH)

System. It is a simple, efficient, effective, and inexpensive way to manage your network and services.

The End-User Notification & Ubiquitous Complaint Hotline System consists of two parts:

1. You sitting at your desk.
2. The end-user who calls you when something goes down.

No, really. Think about it. The advantages are obvious:

1. You are notified of any downtime in direct proportion to the importance of the service. If a service is very important, a large number of users will usually call and complain almost immediately. If the service isn't very important, you might get a call after a couple of hours or so…if at all. This allows you to instantly prioritize since it focuses your limited resources on service outages of the largest magnitude.

2. It is much less resource-intensive than active monitoring. There's no spending hours configuring SNMP traps, fine-tuning monitoring thresholds, and staring glassy-eyed at consoles. You can sit back, relax, and catch up on that stack of PC Weeks that has been collecting dust for the last three months, knowing that the EUNUCH system will kick in at the first sign of trouble.

It's brilliant. Now all I need is a couple of venture capitalists and a branding consultant. Watch for my upcoming IPO. I'll be trading on the NASDAQ under the symbol LAZY.

Just Kidding

Of course, such behavior is not only reprehensible, but also appallingly widespread. Some internal IS organizations, having what amounts to a monopoly on information services, start behaving like monopolists: overcharging, providing poor service, etc. But while you might be able to get away with such behavior when it comes to internal customers (unless your company has an internal Justice Department equivalent), it simply doesn't work with external customers.

Why? Because if something is down…

Customers don't call. Customers leave.

To expect a customer (internal or external) to act as your systems/network management/monitoring system is to invite that customer to look elsewhere for service. That's why, here @ Novell, we are making it a goal this year to not roll out a single service that cannot be actively monitored and managed. If a call from one of our internal customers is the first notification we receive about a particular outage, we've failed.

In order to meet this goal, we are relying on our management products even more than we have in the past. This beigepaper will explain the various components of ManageWise and how we are using those components to meet our goals. Then, we'll go through a step-by-step guide of how we configured the various components at our San Jose site.

Discovery

Here @ Novell, we've broken up discovery into three different "scopes." Our NetExplorer server in Provo handles discovery for our two Utah campuses, our Americas Field Offices, the Asia-Pacific region, and our WAN connections. We also have a NetExplorer server dedicated to our San Jose campus. And our Capelle, Netherlands office handles discovery for the entire EMEA region.

There is an issue with discovery in a Pure IP environment. Since the NetExplorer Manager is unable to rely on IPX routing tables and SAPs to discover NetWare servers, the only thing that it can do is find a local router to learn about other routers on the network. It then goes from router to router, dumping information from each router's routing tables. That means that the only things you're going to discover are the routers themselves and the various network segments. You won't discover any IP nodes.

We're getting around that limitation to a certain extent by deploying LANalyzer agents on most of our application servers. Since our application servers talk to the majority of the other production servers (in one way or another), and since almost every production client maintains an attachment to an application server, the LANalyzer agents on those application servers can take the information that it has gained about IP Only devices and provide that information to the NetExplorer server.

If you're flirting with the idea of reducing your workload by not using discovery on your DHCP-assigned IP address ranges, don't do it. Every time we try it, someone will call up and need a MAC address and we won't have it and we just have to turn around and start using discovery on those ranges again.

NetWare Monitoring Agents

Here @ Novell, we have the NetWare Monitoring Agents loaded on between 600-700 servers. We use these NMAs for "trending" (Is that *really* a verb?) on all of our production servers, and we use TrendComplete to generate daily health reports and monthly health/availability reports.

With that many NMAs out there, network traffic can be an issue. So, we've done a few things that help us reduce the amount of traffic generated by the NMAs. First, we turn off SAPping at the Console and unload FINDNMS.NLM on the NMAs. Why? Well, by default the Consoles send out a SAP identifying themselves and saying "Hey everyone, I'm here. If you generate a trap, send me one, too." FINDNMS.NLM sits on the NMAs looking for those SAPs from ManageWise Consoles and keeping a list of all of the Consoles that it has discovered. When the NMA generates a trap, it sends one to every Console that it knows about.

In our particular environment, where we have ManageWise developers, testers, and all sorts of Labs scattered hither and yon, Consoles are constantly brought up all over the place. If each of those Consoles is broadcasting SAPs and all of those NMAs are keeping track of all of those Consoles, a single trap can end up being sent to hundreds of Consoles. That particular problem is probably unique to our environment, but if you're trying to cut down on SAPs and miscellaneous noise (And who isn't?), you might want to consider doing the same thing.

Since we're not using SAPs to tell the NMAs where they should send traps, we have to manually configure the SYS:\ETC\TRAPTARG.CFG file on each of the servers, but that's not a big deal. We simply have a standard TRAPTARG.CFG for each region and copy that file to all of the servers in that region. Our standard TRAPTARG.CFG sends traps to two different Consoles. First, all traps are sent to the Console in our corporate-wide GNOC. Second, if the regional administrator wants us to (and they all do), we send a second trap to the regional Console.

Another thing that we've done to reduce traffic is "mask" the unimportant traps at the NMAs, so they only send traps that we really care about. You can filter traps at the Console, but by then they've already generated traffic. Why not just stop them before they're even sent?

NetWare LANalyzer Agents

Since most of our production servers are running in a switched environment, the NetWare LANalyzer Agents aren't as helpful as they might be if we had a non-switched environment, but they are still quite useful.

First, as I mentioned before, they can be invaluable when trying to use discovery in a Pure IP environment. Second, they are quite useful in our remote field offices. Running the LANalyzer Agent on at least one server per office allows us to troubleshoot LAN issues at each site. This is nice because we are then able to pull down the trace locally to look for the problem.

The ManageWise Console

As I mentioned before, we have one central ManageWise Console located in our GNOC in Utah. We also have regional Consoles in our major sites around the world.

We use the central ManageWise Console as our clearinghouse for all of the information coming in from every other management utility and service in the company. It receives traps from our NetWare Monitoring Agents, Compaq Insight Management Agents, and our backup and anti-virus software. It receives traps from AlertPage (formerly from Geneva Software before it was purchased by Platinum Technology which was then acquired by Computer Associates which always seems to be at the top of that particular food chain) which actively monitors our NetWare/NT servers and some of our other vital services. It receives traps from GroupWise Monitor, which we use to keep an eye on our e-mail system. And even though Cisco's

CiscoWorks and Bay Network's Optivity require us to use HP OpenView, we still relay all of the traps from our routers and switches to the ManageWise Console.

From there, we use Atlantis Software's PageManager Pro (a third-party product that plugs in to the ManageWise Console) to alert the appropriate people when a server or service is having problems. Our ManageWise Guru has also hacked together a nifty little script that can automatically generate a Help Desk trouble ticket when a trap is received and route it through Vantive's Web interface.

Step-By-Step In San Jose

The folks at our San Jose office were kind enough to provide me with this step-by-step guide of how they configure things at their site. I'm printing it here in its entirety since I think it does a good job of showing how the pieces fit together and provides some ideas that can be used in almost any environment.

1. If strict security is enforced on your campus routers, amend security on the routers to accept SNMP requests from the NetExplorer server and the ManageWise consoles. ManageWise queries the routers to gather information on the various segments.

2. Install tuned LANalyzer agents on one NetWare server on each production segment to be discovered and monitored. Within the segments, the LANalyzer agent gathers information on devices on that segment. It can also monitor the segment for duplicate IP numbers and general health.

3. Configure SNMP on all manageable devices to send alerts to the ManageWise console. SNMP is widely supported by vendors and allows SNMP consoles to query/manage the supported devices from a single location.

4. Install tuned NMA agents on all NetWare 5 and NT servers. NMA agents will provide extended monitoring.

5. Install a NetExplorer server on the main Data Center segment for discovery.

6. Tune the NetExplorer server to discover at certain times, scope the discovery, and configure segment monitoring.

7. Install a ManageWise console on the same segment as above. This is not a requirement, but it helps.

8. Introduce the MIBs into the ManageWise console.

9. Tune the alert disposition settings on the ManageWise console. It is easier to change the settings here to suit your notification needs.

10. Create connectivity test windows for services. You can create one for servers/LAN devices and one for printers.

11. Install AlertPage and configure alerting by pager, e-mail, cell phone, and call ticket. AlertPage should obtain SNMP alerts from ManageWise. One thing, ManageWise does not currently provide the ability to test connections to a specific port number for a given IP number. This function can be handed over to AlertPage (i.e. HTTP ports, FTP ports, GroupWise WebAccess port, etc.).

12. Backup the ManageWise and AlertPage databases. A utility is provided to zip up the existing ManageWise database. AlertPage database directories should be copied to another location on a regular basis. Database corruption has been known to occur with AlertPage, and this can be fatal if you have to remember what to notify on and where to send the notifications, especially if all eyes are on you to get it up and running immediately.

13. Amend device names and icons on the intranet and segments if necessary. (Can also build custom maps). ManageWise allows you to customize the maps. This is where you can get creative.

14. Introduce devices if necessary. Sometimes, you may find you need to introduce a device to the database manually.

15. Tune Alerts and notifications as necessary. As time goes on, you will find yourself tuning, chopping and changing configurations on the console in order to get one step closer to covering all you wanted to cover and being notified of all that you wanted to be notified of.

Misc. Recommendations

- Allow proactive (*Ouch*, there's that word again!) notification by alerting selective local staff on all services that affect the local customers (this will include some local and maybe some remote services).
- Place the management console and notification service at each major site and at the GNOC. Notify from each major site, and from the GNOC for the smaller sites.
- Work with local staff to baseline alert dispositions and notifications. Local customization will naturally follow.
- Provide guidelines through ISO documentation for standardizing, performing regular backups, configuration, and preventative maintenance.
- Maintain remote consoles by using remote control software.
- Backup the console regularly.
- Notify individuals on services that affect the customer for that area, not just local devices.
- Focus first on alerting on end-to-end services, then on standardizing (as each environment is different).

Notification

The objective here is to send the right notification to the right person in a timely manner. One way to do this is to amend the severity of the alarm in the "Alarm Dispositions" on the ManageWise console. Change severity to critical when paging is required. Arrange notification groups so that notification targets can easily be added/deleted/changed.

- Use SMTP email for 24-hour non-critical notifications.
- Use SMTP paging for daily technician priority notifications.
- Use modem paging for on-call staff only, since modems can get overwhelmed at times.
- Use SMTP Cell Message when no pager exists.
- Use Vantive work order generation when a work order needs to be generated.

Alerts received from services, segment monitors and regular connectivity checks are forwarded to pagers, email accounts, cell phones and our helpdesk database according to the following main groups. Selective alerts will generate a work order in Vantive. Here are some examples.

Group	Time	Type	Description	Who
24-Hour Paging	24x7	SMTP E-Mail	"Major" and "Critical" alerts from all services.	Key IS Personnel
24-Hour Paging	24x7	Modem Paging	"Critical" alerts from all services	Key IS Personnel
7am-5pm E-Mail	7-5 M-F	SMTP E-Mail	"Critical" alerts from all services.	Misc. IS Personnel
Backup Services	24x7	SMTP E-Mail	"Informational," "Minor," and "Major" alerts generated by Backup Exec.	Backup Administrators
7am-5pm Technician E-Mail	7-5 M-F	SMTP E-Mail	"Critical" alerts on services affecting their area of support.	Building Technicians
Volume / Cache Bufers	24x7	Vantive Work Order	Low Volume / Cache Buffers	Help Desk

Discovery

The network is discovered by a discovery server and the data is appended to a database on the management console. Information is gathered from conversations on the segments, servers and routers.

Discovery Process	When
Server queries the network.	Saturday, 5am-10am

Console appends to the database locally.	Daily, 2am-6am

Most segments have a module running on one server on that segment that collects data about that segment and watches that segment continuously. The agent has been configured so that it stops if processor utilization on that server gets too high and traps are only sent to the consoles specified in the SYS:\ETC\TRAPTARG.CFG file

Continuous Monitoring

Service	Check Every…	Alarm After…
NetWare/NT/UNIX Servers	60 seconds	5 retries
HTTP/FTP Ports	60 seconds	5 retries
Hubs, Switches, Routers, & RAS Interafaces	60 seconds	5 retries
Off-Site Services	60 seconds	5 retries
Network Printers	300 seconds	3 retries

- Watching for performance/change alerts from the above devices using SNMP over IP.
- Device inactive checking using SNMP over IP.
- Network segment performance checking using SNMP over IP.

Server and Segment Health and Predictions

Data is collected twice daily between 8:00pm and 6:00am, and a report is generated at 7:00pm. This report can be viewed on the Web.

Some Benefits Of A Local Console

- Allows local staff to turn off notification quickly when necessary (i.e. device change, segment down, troubleshooting).
- Console can be utilized for troubleshooting and managing devices.
- Device additions/deletions/changes on the consoles can be done quickly.
- Prevents a breakdown in the monitoring/notification service during WAN link failures, this can also stop unnecessary notifications.
- As each environment is different, only local support staff understands local needs. Also, customization is an ongoing process, which is easily managed locally.
- Maintenance of the console can be achieved locally and remotely (by using remote control software).

Misc. Facts

- 1500 devices discovered on the network in San Jose.
- 269 devices are being monitored and have notification services enabled.
- 918 different alarms: 11 are classified as “Critical” and 240 are classified as “Major.”
- 2 alarms prepares a Vantive work order automatically.

Acknowledgments

Nothing in this beigepaper represents original thought on my part. I couldn’t have written a word without the generous help and input from everyone in Novell’s IS&T Global Technical Architecture group. (I’d name them all individually but they’d probably get spammed.)

Send all comments, questions, corrections, and/or complaints to:

grettir@neticus.com

Tasty baked goods can be sent to:

Grettir Asmundarson
PRV-C-122
122 E. 1700 S.
Provo, UT 84606

And please note that Grettir Asmundarson is just a ridiculous pseudonym, so don’t bother trying to call. You’ll only confuse our receptionist.