4030

Managing NT in the Enterprise - A Primer

Mark J. Konwiczka
Hewlett-Packard Company
1718 Indianwood Circle
Maumee, Ohio 43537

Objectives of this Paper:

1) Identify common components of enterprise management as viewed in the context of traditional Information Technology (IT) focus areas

2) Identify a subset of core components necessary for establishment of a foundation for an enterprise management framework

3) Describe how Windows NT Server (NT) maps into this core enterprise management architecture

4) Use the OpenView suite of products as an example of how to begin building a framework for enterprise management with NT as a primary component.

I Background

A quantum shift has taken place in the way corporations process information. A business anomaly just 15 years ago, the network is a ubiquitous and integral part of how corporate America does business. Client/server applications deployed nationally and globally present new challenges regarding how these highly complex, high bandwidth, mission critical environments are administered, monitored and managed. Windows NT Server has assumed it's position as a serious contender for the title of "dominant network platform", a title highly coveted, long held and fiercely defended by UNIX, which will not be easily vanquished. The vast sprawling network referred to as the enterprise has grown increasingly complex. It is a tapestry of complex components both in and outside the glass house, scattered across the country and around the world. The complexity of networks has grown beyond its architectural components to include a variety of applications, both mission-critical and none, utilizing a variety of data types with varying bandwidth and time critical dependencies. Traffic volumes are soaring as intranets become the de facto business utility for information exchange within corporations. As corporations connect their internal intranets to the Internet they continue to struggle to control this portion of informational exchange. As informational exchange becomes more sophisticated so too does the need to control this evolving environment. The distributed computing model continues to flourish, fueled by the growing popularity of Windows NT.

Let's take a look at the implications of NT deployment in the enterprise and what will be necessary to manage it there.

II Trends

`

The most recent surveys attest to the fact that UNIX will retain the distributed networks high performance/high availability server position for the near future. Also, and almost unavoidably, heterogeneous networks will remain the norm for distributed networks. NT is the up and coming platform of choice. According to estimates from

International Data Corp. (IDC), the number of NT Server licenses sold surpassed UNIX licenses by about 70,000 in 1996. As corporations assess their computing needs, and if "cookie cutter" solutions need to be propagated to large numbers of sites throughout the enterprise, then NT is getting the nod for those distributed locations. Large corporations are deploying NT server by the thousands in order to standardize work environment at remote sites. There are a number of good reasons for NT's wide spread adoption. NT's ancestral roots (i.e. the PC) reflect a short but rich history, showing widespread acceptance in both corporations and households. Some reasons for this broad acceptance are as follows:

1) Familiarity -they know the GUI, the system is easy to setup, use and manipulate

2) Versatility - tens of thousands of applications to choose from

3) Affordability - will pass under the bean counters radar for small installations and compares very favorably to other traditional platform choices for large scale deployment

III Characteristics of NT

Aside from the typical description of NT as a powerful file, print and application server, here are some additional characteristics that make it an attractive choice.

1) Powerful feature set masked by it's association with the "blue collar" PC

2) Catalyst for homogenization of heterogeneous PC network environments

3) Continuing to mature with regards to high availability and horsepower

4) Ability to be managed on a par with legacy enterprise platforms

IV The challenges of widespread deployment of NT

In a large majority of the deployment scenarios NT will be an addition to an already well established network infrastructure. Although a new player in the enterprise arena, NT can be incorporated and managed as easily as other veteran platforms.

a) Building on a strong foundation - how healthy is your network?
As with every other major network change, the primary and most crucial ingredient should be sound planning. A good understanding of the existing network infrastructure is important in order to verify that the existing network topology is sound and can be used as is, or to identify areas where the existing network needs to be beefed. Once the current network condition is understood, then proper deployment of NT servers and other critical resources like software repository servers can be accomplished

b) NT as a full & equal member in a heterogeneous environment

As NT servers are deployed throughout the enterprise they must be monitored, managed and administered just as any other major network platform. Sophisticated problem management as well as performance and resource management needs to be done proactively
as on other enterprise wide platforms

Some challenges to address with regards to NT deployment;

1) software deployment, maintenance and tracking
2) backup and recovery of this distributed environment
3) virus protection of this susceptible environment
4) High availability for mission critical apps
5) Security of NT

V Where do you start?

It all starts with a good plan. Methodology of approach is well beyond the scope of this paper but suffice it to say that an "all tools" approach, which is the main consideration of this paper, addresses only one third of a comprehensive enterprise solution. People and process are equally important and constitute the other two thirds of the solution pie.
As I stated earlier, from surveys published in the "trades" and data from the industry watchers, it appears that NT servers will continue to be

deployed, and in big numbers. Issues such as types of servers, deployed where and in what numbers are network topology issues that directly relate to NT domain design. Servers deployed away from a majority of their respective users inject performance and network bandwidth considerations, further complicating an already complex environment. Its traffic impact on the network must be understood for proper placement

and calculated impact. The plan must also take into consideration the specific business goals of the corporation as well as some pre-defined network goals..

Some goals of network management as define by Divakara K. Udupa in his book, Network Management System Essentials [1] are:

1) Higher network availability
2) Reduced network operational costs
3) Reduced network bottlenecks
4) Increased flexibility of operation and flexibility
5) Higher efficiency
6) Ease of use
7) Security

A good first step toward achieving these goals is the development of a network management strategy that focuses on a core set of management functions. I call these the "Strategic Six" IT management focus areas:

1) Node Management
2) Operations Management
3) System Administration
4) Backup & Recovery
5) Resource & Performance Management
6) Security & Virus Protection

First a distinction must be made between a "green field" or new network and an existing infrastructure. Although these six focus areas apply to both the approach will vary.

New Network

If you are at ground zero and building an new infrastructure, you start with, what I will call, the "Strategic Six". The "Strategic Six" are what I refer to as initial and essential building blocks of an enterprise Management Strategy. The "Strategic Six" consist of; **basic network management** which includes topology mapping and node discovery etc., day to day **operations management** which includes problem or fault recognition, **system administration** which includes user and group additions and modifications plus other administration housekeeping, **backup & recovery** or the ability to protect what you have and rebuild what you
lose/destroy and last but not least, **resource and performance management** to proactively monitor the health of enterprise servers (hardware, OS, databases, applications etc.) to mitigate troublesome surprises.

Existing Networks

The well established networks might require some fundamental baselining of their existing environment before NT deployment. The reason for this is that it is hard to determine destination if origin is seriously in question! Baselining gives you the current state of the network environment from which modifications, and presumably expansions, can be made.

VI Defining the Common IT Focus Areas

1) **Node Management** - Topology mapping and node discovery We have to know it is out there, what it is, its status and relative positioning

2) **Operations Management** - addresses any problems or errors which occur which need immediate attention or can affect short term performance

3) **System Administration** - inventory, configuration and change management

4) **Backup & Recovery** - monitor control & manage local backups with selective central file backup across the WAN

5) **Resource & Performance Management** - is the performance of the system being affected due to unusual bottlenecks or other anomalies

6) **Security & Virus Protection** - access to the physical hardware as well as access to network resources

These additional IT focus areas are also important and in most cases are touched on in the discussions of the "Essential Six":

7) Hardware & software inventory
8) Software distribution services
9) Print management
10) Network Infrastructure monitoring, tuning & simulation
11) Transaction Tracking
12) Service level agreement mediation & evaluation
13) Special monitoring of mission critical client/server environments (i.e. SAP)
14) Web enabled management
15) Event collaboration services

1) **Node Management** - This fundamental functionality of network and systems management provides for automatic node discovery and mapping of network devices as well as system nodes, the respective mapping of all network segments, receipt of status information from servers and client nodes as well as the network devices such as hubs, bridges and routers. In addition, automatic actions can be received based on predetermined thresholds. Hewlett-Packard's solution component for node management is Network Node Manager. This tool determines the general health of the network and all attached devices that are being monitored. The NT nodes will be discovered and mapped to their respective segments on the network. Node Management is both a fundamental and critical aspect of basic infrastructure management. This function has to be in place and functioning properly prior to any serious deployment of server platforms across the enterprise. The base level functionality required is:

1) Discovery and Mapping of network devices and systems
2) Identification and Monitoring of these devices
3) Ability to alarm on preset conditions
4) Flexibility to integrate with third party solutions

This is fundamental building block upon which all other network management functionality is built. It is the base into which all other network and systems management solutions are rooted and which provides the centralized, consolidated and sophisticated view necessary for today's complex enterprise environments.
Network Node Manager (NNM) is available on both UNIX and NT systems. The NT version of NNM is a full WIN32 implementation of the UNIX product

with the added functionality of being able to forward information to NNM for UNIX. The latest version of NNM 5.0 on NT is integrated with Microsoft System Management Server (SMS). NNM users can launch SMS from the NNM user interface and conversely SMS users can launch NNM from their user interface. An NNM operator can select a PC icon from the NNM map and automatically query the SMS database for hardware and software inventory information.

2) **Operations Management** - Provides fault and problem management for heterogeneous systems throughout the enterprise. Hewlett-Packard's IT/Operations product monitors the use of systems and their respective resources and provides functionality in two areas of operational responsibility, which are, performing daily operational tasks and providing for fault/problem management. Proactive monitoring of all servers provides for up front planning of necessary memory disk, CPU or network upgrades to maintain network functionality at the required high levels. IT/O intelligent agents are provided for the Windows NT servers and workstations. The IT/O intelligent agent comes pre-configured to monitor some traditional bottleneck areas namely; CPU, Memory and Disk. Once a predetermined threshold is exceeded for either of these resources, the intelligent agent sends an alert to the central management station. IT/O also monitors, via default functionality, the application, system and security event logs on the Windows NT system and alarms on critical messages. In addition, IT/O also provides an "NT Toolbox" on the cental management station that allows network or operations personnel the capability of doing "ad hoc" status checks on over two dozen NT system functions. Some of the functions in this tool box are scripts which display the CPU, Disk and Memory status of the managed NT system on the central management console as well as the processes running on the NT node, number of processes, resource shares, etc. One of the more useful features is the ability of a network administrator to open a windows on the management station with the console prompt of the managed node. This can be used for more in depth probing of the system "real-time" and to take immediate corrective action via the "c:\" prompt.
This NT management product is customizable to provide the proper level of depth or granularity of management sophistication. Under the present product structure NNM is tightly integrated and bundled with the IT/O product. Native IT/O functionality for NT will be available in fourth quarter '97.

3) **System Administration** - is the third critical component of basic integrated network and systems management in the enterprise. It should integrates tightly with the Node and Operations management components. The administrative component generally provides centralized system administration functionality in areas dealing with:

1) Software distribution
2) Hardware and software inventory
3) OS parameter Management
4) Printer management
5) User and Account management

The HP product that provides this functionality is OpenView IT/Administration (ITA). Software can be tracked and distributed from the central management station. Software can also be distributed from the central management station to distributed NT repositories throughout the enterprise for further downstream distribution. HP's ITA product is also tightly integrated with Microsoft's Systems Management Server. This ITA-SMS integration provides for the following features:

a) Display the SMS Hierarchy in the ITA GUI

b) SMS collected Hardware and Software Inventory is integrated into ITA's repository to provide a single view of the inventory, enterprise-wide.

c) Initiate a SMS software distribution job from the ITA GUI.

Note: As per an agreement with Microsoft the ITO and ITA intelligent agents for NT will ship with the next major release of Systems Management Server. One other key component, user and account management, will be added in the near future to round out the administration of NT systems.

4) **Backup & Recovery** - as NT servers proliferate throughout the enterprise, the need to tightly control the backup process becomes more critical. Protecting proprietary corporate data is both necessary and tricky in a distributed systems environment. The necessary backup functionality needs to be evaluated with regards to :

a) Backup type - full, partial, incremental
b) Backup frequency
c) possible backup scenarios
    1) All files backed up to a device local to the server system
    2) All files backed up to a central system across the net
    3) Some combination of 1 and 2

Hewlett-Packard provides the OmniBack II product for sophisticated backup functionality for the NT platforms in the enterprise. OmniBack II is HP's centralized backup solution for heterogeneous platforms in the enterprise. (In addition to NT, OmniBack also provides a backup agent for Windows 95) Through the use of OmniBack II a operator may choose to backup critical files across the network to the centralized backup server or trigger a local backup on the NT system if a backup device is directly attached to it. So, from a central location an operator can control the backup process on all NT systems that have the backup agent installed. In, addition a backup interface exists on the NT system that allows the NT user to request a "pull" of a file or files from the central backup system. Backups can be performed manually or scheduled. If your objective is to centrally initiate and control backups of all systems, including NT, across the enterprise than OmniBack II should be in your management toolbox.

5) **Resource and Performance Management** -
The PerfView/MeasureWare product is HP's powerful measurement tool used to monitor critical system resources and also serves as a central repository for service level measurements throughout the enterprise. In general, the MeasureWare agent for Windows NT provides the same functionality as MeasureWare UNIX agents. This flexible tool when used to monitor the NT systems provides;

1) Data on over 200 different Windows NT resource management metrics and includes collection management on three levels of granularity:

Global level - overall system health
Application - user defined groupings of processes
Processes - individual processes running on the system

2) Ability to acquire end-to-end applications transaction response time measurement using Application Response Measurement which is HP's Transaction Tracking technology.

3) The Data Source Integration feature of PerfView/MeasureWare provides for the ability to collect, log and alarm on resource and performance data from external sources. Almost any PC resident application in the enterprise that generates ASCII data can be centrally monitored using this flexible feature.

4) Powerful turnkey monitoring of:
   a) OS
   b) Database
   c) Networking
   d) Application metrics

5) Sophisticated collaborative analysis of the information captured on a variety of enterprise events is possible from a centralized management console. This feature brings together all network, system and application events for a comprehensive graphical view of what took place in the enterprise in a particular "slice" of time.

There is a growing emphasis in business today on service level management. Their ability to verify that the business needs of the end user are being met from a technology point of view is becoming increasingly more important. One way to accomplish this is through the establishment of service level objectives. These are then translated into Service Level Agreements or SLA's with the end users. The transaction tracker can provide this end-to-end transaction response time tracking capability for NT clients.

The PerfView/MeasureWare product delivers the "big picture" view of what events took place in the enterprise at what point in time and allows for a systematic analysis of these events. A variety of data can be displayed in graphical form on the management station and, one by one, variables can be eliminated from the graph to highlight the offending component. So through this collaborative display of time related items we can determine where it is NT, the network, the database or application that is at fault.

6) **Security & Virus Protection -** Security is a paradoxical characteristic in that it is much easier to prove the negative, that something is not secure, then the positive. In general, the topic of security becomes much more acute with the advent of distributed computing. Not only are there more systems to secure but they are scattered throughout the corporate infrastructure. The aspect of physical access to critical network components as well as access to network services takes on a whole new dimension when viewed from an enterprise perspective.

Windows NT has a variety of security features built in and was designed with the U.S. Department of Defense C2-level security in mind. Through the use of standard features of NT such as NTFS with accompanying ACL capability, comprehensive password policies, uniform system policy control and security audit capability a well fortified NT environment can be constructed. As secure as this NT environment appears to be, it is still subject to the common peccadilloes of the individual users. In addition, homogeneous environments will remain the exception rather than the rule so a truly comprehensive and centrally administrated security solution is necessary with a view to the enterprise. Ideally, a network security strategy needs to be implemented that takes password and security responsibility out of the hands of the users and the elimination of "clear text" as the preferred method of data transmission.. Even for intranet transmissions "clear text' is as confidential as a hallway conversation. A serious security strategy needs to consider the following characteristics and implement them enterprise wide for all platforms;

1) Authentication
2) Authorization
3) Data Integrity
4) Non-repudiation

HP's security strategy is designed to take the worry out of enterprise security management by providing end-to-end security for corporate intranets as well as the Internet. HP's Praesidium/Single Sign-On strategy is designed to provide users with a secure single point of entry to access distributed and heterogeneous resources, including databases, and applications on PC's, UNIX servers and legacy systems. This powerful security strategy can be used to shield distributed systems, including Windows NT, from unauthorized access in that it can provides an enterprise-wide single login solution. Administration of security enterprise wide can be a genuine nightmare, with heterogeneous systems each having their own security rules and implementation strategy. Do to modification or omission, security holes could easily develop and not be noticed immediately or until an outside intruder brings the omission to your attention. Praesidium Single-Signon provides a centralized security management environment from which security, enterprise-wide can be maintained, monitored and controlled in a consistent and uniform fashion. As the complexion of distributed solutions continues to evolve, with new applications, client/server solutions and platforms one thing above all should remain constant and that is security.

HP's Praesidium strategy allows customers to detach security from otherwise proprietary dependencies such as platform and application. This detachment can provide the uniformity of coverage and consistency of security that enterprise environments require.

Although virus protection is a sub-topic in the discussion of network security, it's implications are dramatic in distributed environments. Virus protection is much more important for distributed environments because so much more is at stake. Consider this statement by virus protection software manufacturer Symantec, "Once a virus infects a single network computer, the average time required to infect another workstation is from 10 to 20 minutes, meaning that a virus can paralyze a network in a few hours."

On stand alone systems if a virus trashes a system it is a real inconvenience and a productivity killer. If a virus trashes hundreds or thousands of computers on a network it places the entire corporation in jeopardy, could cost hundreds of thousands or even millions of dollars in downtime to say nothing of the tremendous cost of exorcising this demon from the networking environment. You might say it can't or won't happen to you but a recent survey (1996) conducted by the National Computer Security Association of Carlisle, Pa. reported that about 98% of 300 mid-to-large-sized companies reported that they had discovered a virus on a PC.

An enterprise-wide virus protection strategy should be developed and deployed to protect NT or any other PC based environments from falling prey to unintentional virus introduction or sabotage. A number of third party products exist that provide generic and macro virus protection on NT and these should be used in conjunction with an enterprise wide virus protection strategy. (see Appendix A for a list of virus protection software suppliers)

Security needs to be addressed in the same planning breadth as network, system and application management in the framework. If treated in the same fashion as disaster recovery, corporations will risk more than just damage, they will risk extinction. As corporations move forward and deploy intranets and connect them to the Internet for E-commerce, security must be the critical linchpin in the planning process.

To use an analogy we can all relate to, "Just as our dentist admonishes us to not ignore our teeth or they will go away, if corporations ignore security issues, they risk waking up one morning to find that their business "has gone away", been destroyed".

VII Summary

Corporate intranets are no longer just an extension of the "glass house": The correct compute paradigm today is a variety of complex solutions that integrate in the enterprise. Customer are demanding that management vendors provide a comprehensive solution that deals with this complexity and addresses all three tiers, applications, systems and network simultaneously, hence the term framework. I believe that this solution falls short and is incomplete if security is not an integral part of the enterprise solution. Security should both envelop and permeate the framework. .

I have emphasized the "Essential Six" areas that I believe are critical for success if the objective is enterprise management, and have identified how NT fits into each of these areas. As Windows NT continues to play an ever increasing role in distributed network environments, a consistent set of management tools is needed to manage the enterprise as a whole. NT should be treated as an equal player in the enterprise, and the tools should reflect that status by providing the same level of support as the other member platforms. The OpenView suite of products provides that consistent, clear view of all systems in the enterprise, including NT.

Glossary of Terms

Agent - a process running on a system which allows it to communicate with the management server

Enterprise - vast expanse of interconnecting WANs and LANs geographically dispersed

Framework - encompasses the three integral enterprise management components which are the network(s), systems and applications

Intranet - a private corporate network using the same technologies as the Internet

Internet - worldwide collection of networks using the TCP/IP protocol

Managed node - A system that is able to exchange management information with the management server

Management server - a central system where a relational database and management processes are running. The system where the managed nodes sent information to be consolidated processed and archived.

Appendix A

List of Virus Protection Solutions for NT

Norton Anti-Virus www.symantec.com
(800-441-7234)

InocuLAN for Windows NT www.cheyenne.com
(800-243-9832)

Dr. Solomon's Anti-Virus Toolkit for Windows NT www.drsolomon.com
(800-701-9648)

VirusScan www.mcafee.com
(408-988-3832)

PC-cillin II NT www.touchstone.sc.com
(714-969-7746)

References

(1) "Network Management System Essentials", McGraw-Hill, Divakara K. Udupa

"HP to Become the Leading Framework Manager within 12-18 Months", Giga Information Group, December 30,1996

"The NCSA Guide to PC and LAN Security", McGraw-Hill, Stephen Cobb

"We've got trouble", Elizabeth Horwitt, Network World, April 14, 1997

Hewlett-Packard Praesidium Single Sign-On Security data sheet

Hewlett-Packard Technical Evaluation Guides & Field Training Manuals for:
OpenView Network Node Manager
OpenView IT/Operations
OpenView IT/Administration