Interested in learning
more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

Using MOM 2000 to Secure Servers

The primary focus of this document is to show how MOM 2000 out of the box can address many security issues and act as your eyes and ears on every managed machine. Furthermore to address the NetIQ security Management Pack for MOM 2000 and its functions. As well as demonstrate functionality and capabilities of the two products together in an enterprise helping administrators make their servers more secure therefore reducing risk and increasing uptime. This will cover the history of MOM 2000, the architecture behind it, a...

Copyright SANS Institute
Author Retains Full Rights

AD
ONLY ONE INDEPENDENT TEST
MEASURES REAL-WORLD,
ENDPOINT MALWARE PROTECTION.
TREND MICRO SMART PROTECTION NETWORK

Using MOM 2000 to Secure Servers

SANS Security Essential (GSEC) Practical Assignment
Version 1.3
Wyatt Banks
June 5, 2002

1. Introduction

1.1 Microsoft Operations Manager 2000 delivers enterprise-class operations management by providing comprehensive event management, proactive monitoring and alerting, reporting, and trend analysis. It is commonly known that event logs are a vital part of security monitoring and management. MOM 2000 provides a robust backbone that has the ability to sort through all your events and take necessary action. Out of the box MOM 2000 comes with a vast amount of knowledge for performance and availability monitoring. It is a key component of Microsoft Operations Framework. The MOF initiative is a collection of out of the box best practices for IT professionals to help ensure that critical systems are operational and secure. Another key to this is the "Get secure and stay secure" theme. Constant badgering by industry experts and analysts has finally forced the big player to take the security space seriously. Microsoft has recently released tools that can address security holes and patch management. Some of these tools include hfnetchk.exe, Windows Update Corporate Edition, integration points with SMS and hfnetchk.exe for patch deployment, Microsoft Baseline Security Analyzer, and of course MOM. Additional components of the MOF are Application Center 2000, SMS 2.0, and of course the native technologies that are built into Windows 2000, some examples are group policy, WMI, Active Directory, and the Windows Installer.
(http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/prodtech/windows/windows2000/staysecure/secops01.asp)

1.2 The primary focus of this document is to show how MOM 2000 out of the box can address many security issues and act as your eyes and ears on every managed machine. Furthermore to address the NetIQ security Management Pack for MOM 2000 and its functions. As well as demonstrate functionality and capabilities of the two products together in an enterprise helping administrators make their servers more secure therefore reducing risk and increasing uptime. This will cover the history of MOM 2000, the architecture behind it, and why NetIQ is so interested in this Microsoft product. This will also show some features and functionality of a systems management product in the face of security.

1.3 History of MOM 2000

It is difficult to talk about this tool without mentioning where it came from and why Microsoft has such a heavy investment in it now. The technology that has become MOM 2000 was licensed from NetIQ Corporation. On October 12, 2000 Microsoft announced that it had joined NetIQ and formed the Microsoft

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Management Alliance partner program. Part of this alliance was the licensing of this technology. (http://www.microsoft.com/presspass/features/2000/oct00/10-12dotnet.asp)
Formerly this technology was sold by NetIQ in the form of a product called NetIQ Operations Manager. Now it gets really interesting. Before NetIQ and Mission Critical Software merged on February 8, 2000, (http://www.netiq.com/news/press_releases/2000/000228MCSMerger.asp) Operations Manager was marketed and sold by Mission Critical as OnePoint Operations Manager or OOM. The predecessor to OOM was a Mission Critical software product called seNTry. SeNTry was purchased by Mission Critical Software in mid 1997 from the UK based company Serverware. (www.serverware.com) Originally based on Microsoft Access, therefore scalability could be an issue. It was able to alert on events with limited functionality. It could also filter events out so they would never reach the database and detect missing events that were expected but never received. (Information gathered from personal interview please see references for details)

So now we know where MOM 2000 came from, what does it do and how can it help you secure your environment?

2. Event logs and why we care

2.1 There is no argument that event logs are crucial for security auditing. Furthermore the security event is the key to forensic analysis of intrusions and incidents. Still the common event log is so full of apparent pollution and junk how can we groom valuable information from it? Let's break this down a bit and examine a pretty common event. Taking a quick peek on my laptop I have some events with ID 592. In the details tab I see the following figure 2.2

2.2

Event Type: Success Audit
Event Source: Security
Event Category: Detailed Tracking
Event ID: 592
Date: 4/19/2002
Time: 5:27:11 PM
User: NT AUTHORITY\SYSTEM
Computer: *LAPTOP*
Description:
A new process has been created:
New Process ID: 2876
Image File Name: C:\WINNT\SYSTEM32\sol.exe
Creator Process ID: 480
User Name: *JIM.SHOE*
Domain: *DOMAIN*
Logon ID: (0x0,0x3F7)

For more information, see Help and Support Center at http://go.microsoft.com/fwlink/events.asp.

2.3 This event has some very good information in it. It tells me that it was a

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

successful audit of a process that was started on *LAPTOP* by the user *DOMAIN\JIM.SHOE.* The program that was started happens to be sol.exe. This is very useful indeed, if I were monitoring the use of solitaire on all servers in my environment. Because I have a lot of events I would need to filter out information from all of the events to narrow down what I want to see. Once I find the events I am looking for then what? If I cared about this process enough I would have to sit in front of the console and constantly watch the event log for this event to magically appear. Then if the event appears among the thousands of others I would have to go to that machine to do something about it or execute a bit of remote code to stop this process. Furthermore if auditing is not enabled I would have never seen this event or any like it. Sounds pretty easy right? This is just not possible, the sheer thought of combing through NT event logs can put even the biggest nerds to sleep. Even thought they contain the richest form of information available native to the WinNT family operating system. In the example above we get a cute little link to the Microsoft events knowledge base. There we can look through a vast database of information of what these event mean and why I may or may not be getting certain ones. This is great if you are researching incidents that have happened, or if you are the typical IT professional with all of the time in the world to invest in research. But it doesn't scale to the real world or to real time examination of your logs. Alternatitively we could pay a newly coined MCSE right out of the roadside certification school to look through all event logs all day long looking for something. Something that is not normal, something that is not good, something that is not expected? How would and NT administrator know the answer to any of these questions? How would our log-monitoring fellow keep up with millions of events in an enterprise of merely a few hundred servers? Using the native event viewer there is no way to generate reports on this data even if we were to comb them. With every possible numeric valued event a human would need to research the meaning and then do something about it. This becomes a daunting task. The solution is to have an automated process that will look at events in the event log and examine the contents, determine if it is important or if it needs to be ignored, take some action if necessary and notify the authorities of what it did and when. In addition having a database with possible causes, information and extended pre-researched knowledge specific to the application or bottom line of the problem would complete the circle. This sounds like a powerful piece of software. The solution that was just described it the function of Microsoft Operations Manager 2000.

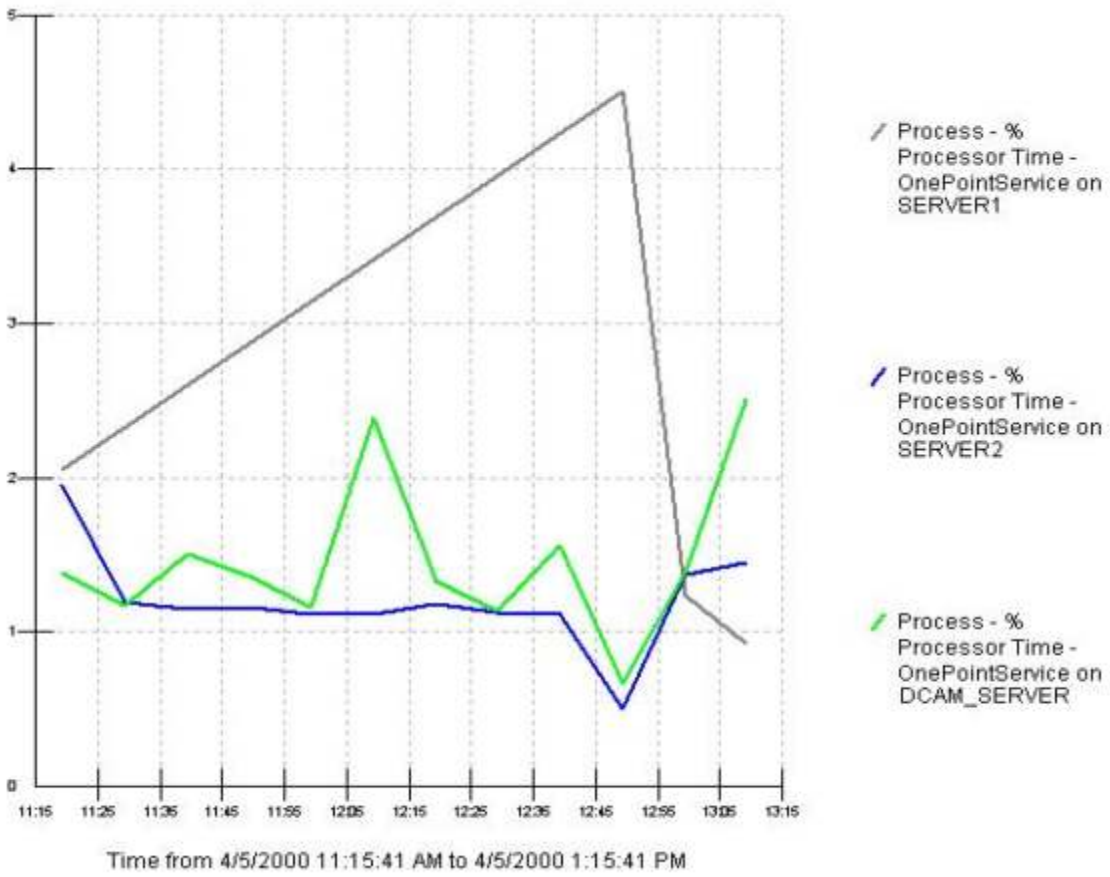
3. Performance and Availability

3.1 MOM 2000 is a performance monitoring tool. It has the ability to monitor event logs, performance counters, services and applications. MOM has two main components the base monitoring pack, and the application monitoring pack. With these packages you get the ability to gather specific information about the health and availability of not only your servers but also the critical applications that are running on them in your environment. In order to monitor performance you need to have normalization. After you know what is normal then you can

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

monitor the specific thresholds and know what is not normal. Is it normal to have 100% CPU utilization on an Active Directory domain controller, or should I be seeing 5% utilization? It would certainly depend on the environment that the server is running and the operating conditions. Maybe this is normal and maybe not. The real question is how do you know what normal is with out having a baseline. Creating the base line of what normal is and measuring the thresholds that may be crossed is a key function of the MOM 2000 infrastructure.

As displayed in the illustration 3.2 graphing is easy and has a basic look.



3.2 Performance graph showing %processor time of the agent service on each managed computer

4. Security in the context of management

4.1 As mentioned earlier MOM 2000 comes with a built-in knowledge base. This knowledge base can not be edited by the user however provisions have been made to incorporate company learned knowledge. This can be inserted into each and every rule. This is very important when maintaining a large amount of servers in a mixed environment. The significance of this knowledge base is the key to the product. When speaking about applications and operating system data the source of this knowledge is the product groups within Microsoft. In the ideal world the product groups would be developing the management packs for their

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

applications. Who knows how to monitor IIS better than the people who wrote the code? The management packs consist of sets of predefined rules, views and knowledge. These management packs can also be customized and tailored to particular environments as well as expanded to fit custom applications.

4.2 Management packs are not just for applications. As part of the management strategy that Microsoft has developed, the MOM 2000 framework allows for third party Independent Software Vendors (ISV's) to produce management packs to meet the needs of customers. NetIQ Corporation was named as a premier ISV for management solutions. (http://www.netiq.com/products/xmp/default.asp) (http://www.microsoft.com/mom/partners/default.asp)

4.3 The new lines of products that NetIQ has produced since the release of MOM 2000 are called Extended Management Packs for MOM or simply XMP. The XMP's are designed to bring added value and bolt on knowledge to help complete a management system using MOM 2000. These add on knowledge packs help address issues such as hardware monitoring, third party non Microsoft applications, and expanded operating system support including UNIX and Linux. Some XMP's also allow connections to framework products like Micromuse Netcool and Tivoli. Another key to keep in mind is that MOM 2000 has limited support for Windows NT. NetIQ provides full support for Windows NT and expanded support for Windows 2000 and Microsoft .NET applications. This added management comes in the form of Active Analytics NetIQ's version of out of box knowledge, additional views and reporting.

4.4 So how does this pertain to security? NetIQ announced at Microsoft's Tech-ED in April 2002 that the company had developed a Security Management Pack for MOM 2000. (http://www.eweek.com/article/0,3658,s=1884&a=24876,00.asp) The Security Management Pack or SMP is a group of three Knowledge modules that add security functionality and the automated response associated with it to the MOM 2000 infrastructure. The security XMP for Windows includes rule sets and knowledge for monitoring Windows security logs, IIS security events, and host based intrusion detection. Security XMP for Anti-Virus brings three major anti-virus solutions into the MOM 2000 system for correlation and monitoring of virus outbreaks within the same console. Anti-Virus applications supported are Trend Micro, Symantec Corp. and Network Associates. The final piece to the SMP is a knowledge module for NetIQ's Security Analyzer. Security Analyzer is a vulnerability assessment tool supporting Windows 9x, Windows NT, Windows 2000, Sun Solaris, and Red Hat Linux. (http://www.netiq.com/products/sa)

4.5 What this means it that by using MOM 2000 you can not only have a comprehensive management system for monitoring operating systems, the applications on them, the hardware that they run on but securing the systems is another benefit. Using the Security Management Pack from NetIQ, administrators have the ability to see security information in the context of systems management.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

5. Rules and Knowledge

5.1 Your MOM 2000 system uses rules for monitoring. Rules are important because they are resident in memory on each monitored system looking and waiting fore something to happen or, taking a more proactive approach, by pulling information using scripting. There are several types of rules. When rules are created criteria is set to determine how the data that is gathered is dealt with. When an event or data that matches a rule is generated by the agent system MOM 2000 can act upon that data in many ways. The significance of the condition can also be defined as well as information that could possibly help resolve the condition.

5.2

- **Event rules** This is the type of rule that lies and waits for something to happen. It is looking for a particular event to appear in the event log. When that event comes to pass it will trigger this rule to take some action. This could be simply an alert to the console or send notification to a group of operators. Automated response can also be running a script or some kind of command line executable.
- **Default collection** – Rules that simply collect data. Most often this data is the raw event log entries to be stored in the database. Default event collection is not highly recommended simply because of the mass of data that a heavily used Windows NT or 2000 server can produce. This can cause extra unnecessary load on the database and the network. Collections do not take any action or generate alerts.
- **Timed event rules** – This type of rule runs as a timed interaction with the managed client. This can be very useful while gathering metrics or looking for specific things that the event logs do not contain. Scripting is a very powerful approach to managing and monitoring. A real creative scripter can even craft elaborate processes that check multiple settings including making direct API calls to applications or the operating system.
- **Event consolidations** group similar events into a single summary event that is stored in the database.
- **Filtering rules** can identify events that are insignificant. Filtering can come in three variants Pre-filter stops processing and does not continue to evaluate the event, Database filter evaluates the event but does not store in the database, and Conditional filter witch saves the events only if they match the conditions of another rule.
- **Missing event rules** will generate an alert and can send notification if a significant event is expected but does not happen.
- **Alert rule** allows a specified response for an alert or for a number of previously defined alerts within a processing rule group.
- **Performance processing rules** have two variations, measuring or sampling and threshold. Performance rule gather data from the Windows performance counters and WMI numeric data. Sampling gathers data the

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

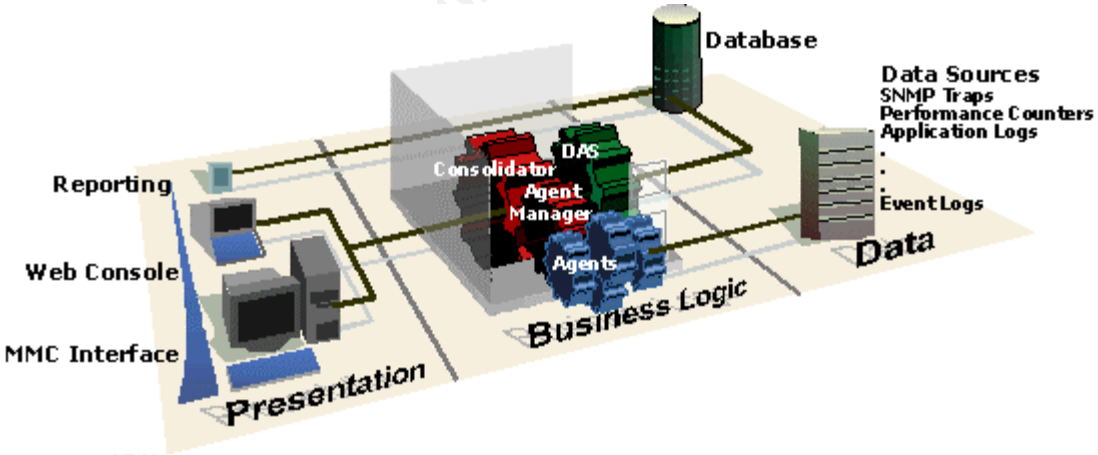
can be displayed in a graph form. Threshold measuring pulls data and compares it to specified thresholds. Alerts can be generated when the thresholds are met.

5.3 Rules are meant to gather data, and act upon it if necessary. Where that data comes from is defined within the rule. Each rule uses a source called a *Provider.* Providers that MOM 2000 can use somewhat match the type f rule that uses them.

- Windows NT Event logs, including the extended logs in Windows 2000.
- Windows performance counters
- Timed event providers
- Application logs including IIS logs, SQL trace logs, syslog files, and generic ASCI files.
- WMI events
- WMI numeric data
- Generic providers usually are in the form of internal events within MOM such as when an agent heartbeat fails.

6. Architecture

6.1 By nature MOM 2000 is focused on performance and availability management and monitoring. It uses an active agent technology that places code on every server that it is monitoring. Using the Microsoft DNA architecture it looks something like figure 6.2



6.2 *This image file was placed in the install directory on the MOM 2000 server at C:\inetpub\wwwroot\webconsole.*

6.3 The central computer or management server is called a D/CAM. This stands for DAS/Consolidator/Agent Manager. Each component can be installed on a single system or it can be broken out. Microsoft recommends leaving all components on one system.

The function of the DCAM can be broken down to each of its components.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

DAS is short for Database Access Service. Its function is to broker the data between the consolidator and the database. It runs as a COM+ object under Microsoft Transaction Server to accomplish this as well as provide dynamic load balancing.

6.3.1 Consolidator collects information and from the agents and passes the data to the DAS service for insertion into the database. It is associated with the Agent Manager and acts as an agent on the local machine.

6.3.2 Agent Manager tracks the agents and decides what systems need agents installed on them. It also assigns the agents to the proper computer groups and pushes out rules. It is associated with the Consolidator component.

6.3.3 Agents collect the data and apply rules. The agent stores all rules locally in memory. It is responsible for taking local action as a response to an event. As stated in architectural diagram the data sources the that agents can collect information from are Event Logs, Performance Counters, Application logs, and SNMP traps, Furthermore the agents also can pull data from the Windows Management Instrumentation service, as well as a built-in syslog data provider. Application logs can be any "single event per line" log file i.e. web server logs and ftp logs. This also provides a dynamic system when customizing monitoring for other applications. Any application that logs to the NT event log or even its own log can be monitored with MOM.

6.3.4 Database component uses Microsoft SQL server 2000. Everything goes in the database. This includes information about configuration, data that is collected and an exact copy of each event that is gathered. This is very important for forensic analysis.

7. System Requirements and Install

Minimum Requirements For Central Computer	
Processor	550-megahertz (MHz) or higher Pentium-compatible processor
Operating System	Microsoft Windows 2000 Server, Advanced Server, or Datacenter Server operating system with Service Pack 2 or later
Memory	512 megabytes (MB) of RAM
Hard Disk	1 gigabyte (GB) of available hard-disk space
CD-ROM Drive	Available for installation purposes
Monitor	Super VGA (800 x 600) or higher resolution
Pointing Device	Microsoft Mouse or compatible pointing device
Database	Microsoft SQL Server 2000 Standard or Enterprise Edition or later (recommended); Microsoft Access 2000 or later

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Minimum Requirements for Active Agents	
Processor	200-MHz or higher Pentium-compatible processor
Operating System	Microsoft Windows 2000 Server, Advanced Server, or Datacenter Server; or Windows NT Server 4.0 or Windows NT Server 4.0, Enterprise Edition, with Service Pack 4 or later
Memory	64 MB of RAM
Hard Disk	100 MB of available hard-disk space

7.1 System requirements taken from the *Microsoft Operations Manager 2000 Reviewers Guide* appendix A page 41

7.2 An additional requirement is that the MOM 2000 server must be installed into a Windows NT or Active Directory domain, NetBIOS must be enabled with full WINS support if using Windows NT or Active directory in mixed mode. Microsoft office Graph component is also required to view graphs. If the web console is desired, than an IIS server on Windows 2000 or IIS 4.0 with Internet Explorer 4.01 SP2 on Windows NT is needed. Of course the hardware recommendations are minimal requirements. Like any application the more resources that are thrown at it the better it will perform.

7.3 Install procedures are very well documented in the MOM 2000 installation guide. The installation guide contains a checklist to help the installer decide if it is acceptable to place all components on one server or if it would be more appropriate to separate the database server. According to the matrix, if the intent is to monitor more that 10 systems then the database server needs to be separate. Additionally an implementation check list can be found that will walk through the install process and post install to get the system up and running.

7.4 Delegation of permissions within the MOM 2000 console is done through Windows local groups. A total of five groups are created during the install procedure. A list of functionality and permissions of each group is found in detail within the MOM 2000 installation guide on page 41. Here is a basic list of functionality

OnePointOp Users

Monitor the information that is collected and resolve alerts but cannot modify MOM functionality. Members can also use reporting.

OnePointOp Operators

Modify the information that MOM collects and what the product does with the collected information. Can take advantage of the web console and modify rules.

OnePointOp ConfgAdms

Modify the list of computers that the MOM Agent Manager installs agents on. Members have full control of the system.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

OnePointOp Reporting

Run reporting and view reports

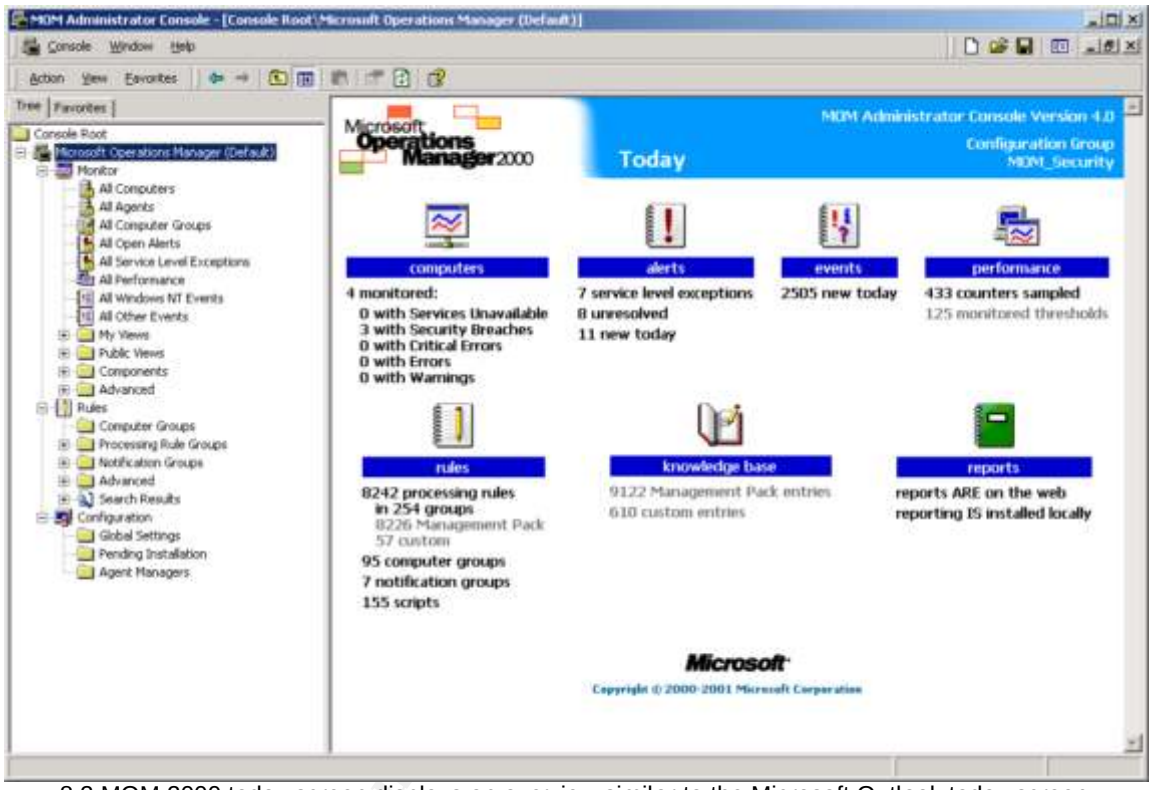
OnePointOp System

System group that service account is a member of. Has full control of the system

© SANS Institute 2002, Author retains full rights.

8. Let's take a look at MOM

8.1 The following screen shots are taken from a fresh install of Microsoft Operations Manager 2000 with the NetIQ XMP for SQL including Active Analytics, NetIQ XMP for Windows NT servers, NetIQ Security Management Pack for Windows, NetIQ XMP for Anti-Virus, and the Microsoft Management Pack for SQL servers.



8.2 MOM 2000 today screen displays an overview similar to the Microsoft Outlook today screen.

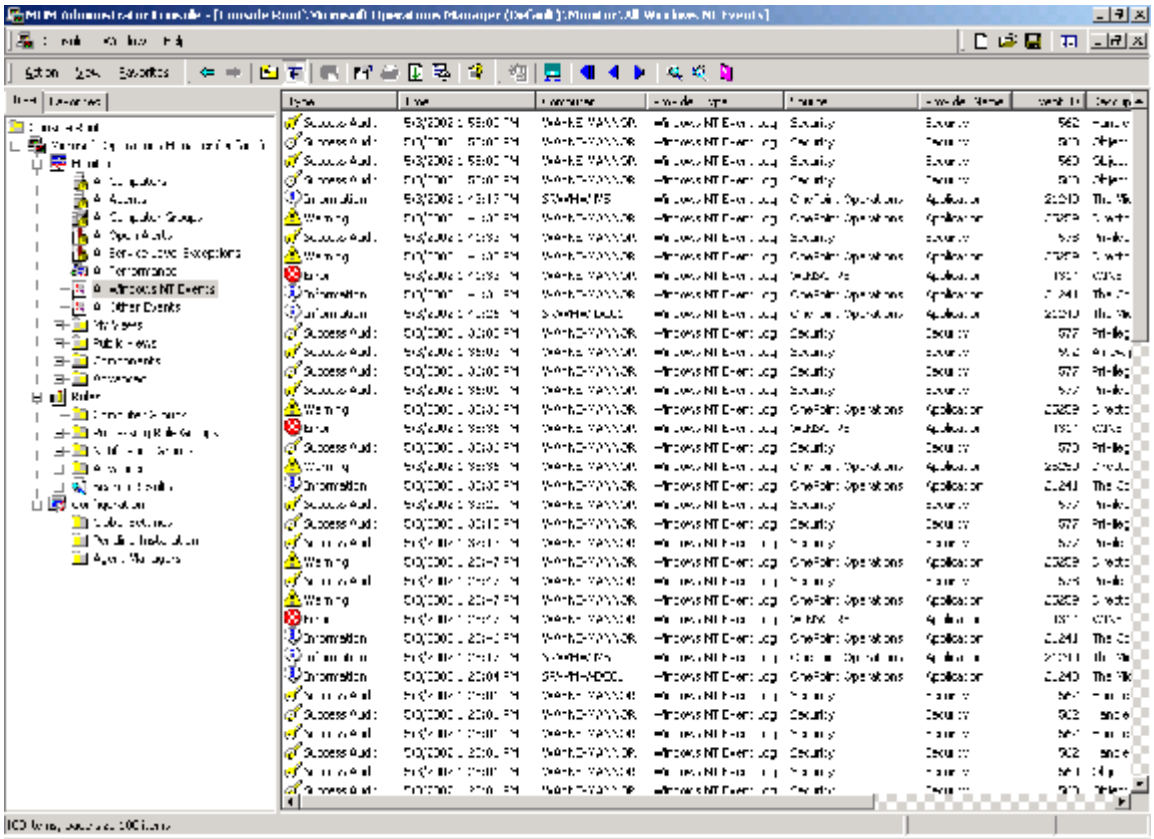
8.3 MOM 2000 uses the MMC for its primary configuration interface. There is also a Web interface that is used for displaying events and reporting information. On the left hand side of the MMC there is a tree view snap-in. The three main snap-in branches are Monitor, Rules, and Configuration. Monitor contains views that are a definition of what an administrator wants to see. Some views are "Public" meaning that any administrator can see them; other views are "My Views" that can be customized so that each administrator can create their own.

8.4 Creating an event view will allow the user to specify criteria for the types of events or content that the user wants to see. Several options are available to query on. This can be very handy when searching the entire database for a certain event. Narrowing the criteria can include the text in the event description. This is invaluable when looking across multiple machines. It is possible to search for an event caused by a specified user, event ID, time frame or even if the event generated an alert. It is even wild card friendly when creating the search. It is also possible to create views that for Alerts, Performance, attributes,

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

and reporting.

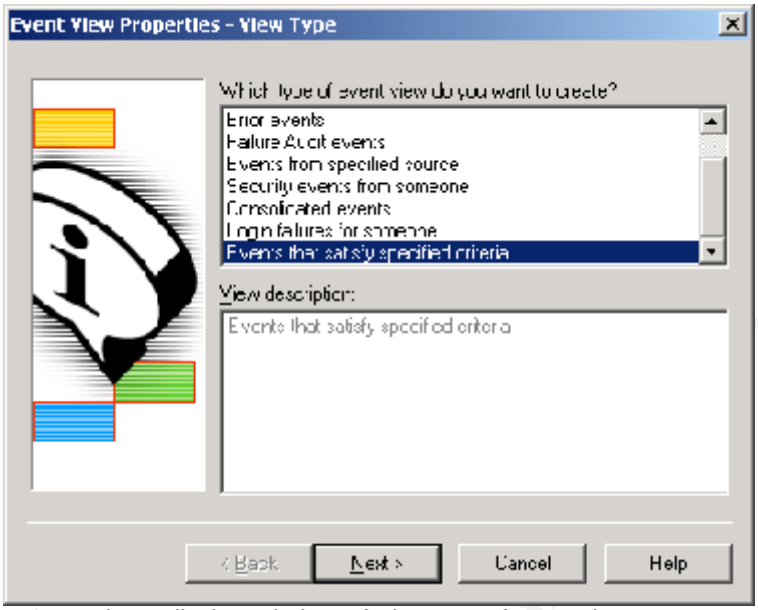
8.5 All events can be viewed through the *All Windows NT Events* view. This displays the events from the logs of all of the managed servers. This view only shows 100 events by default. When looking at an enterprise, 100 events certainly does not seem like very many. Listed in figure 8.6 below there are three servers all of witch are producing events of various types.



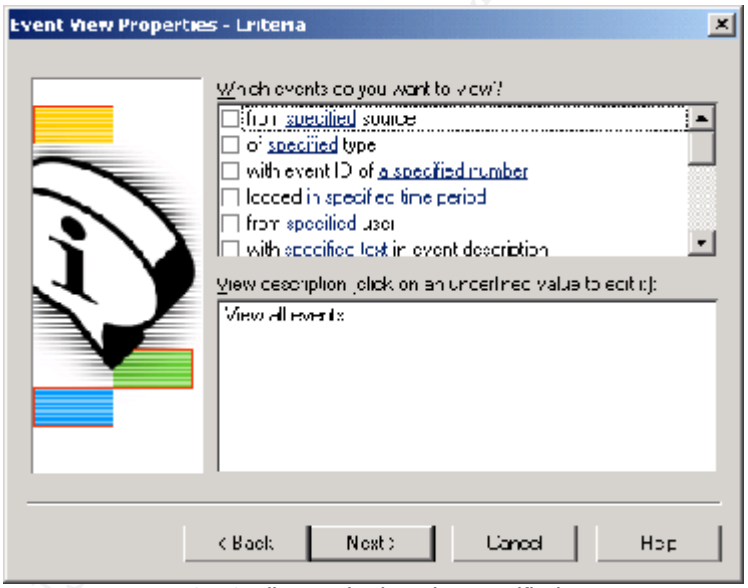
8.6 All Windows NT Events displays events across the enterprise.

8.7 What if an administrator actually has to go back and refer to the event logs? In an enterprise with any amount of servers, without some kind of consolidation this task is nearly impossible. Bringing all of the logs into view is one thing but having the ability to search for aspects of the logs is a true luxury. This will be useful when tracking down incidents to correlate events with them. The example below shows step by step how to create a custom view searching for particular events.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

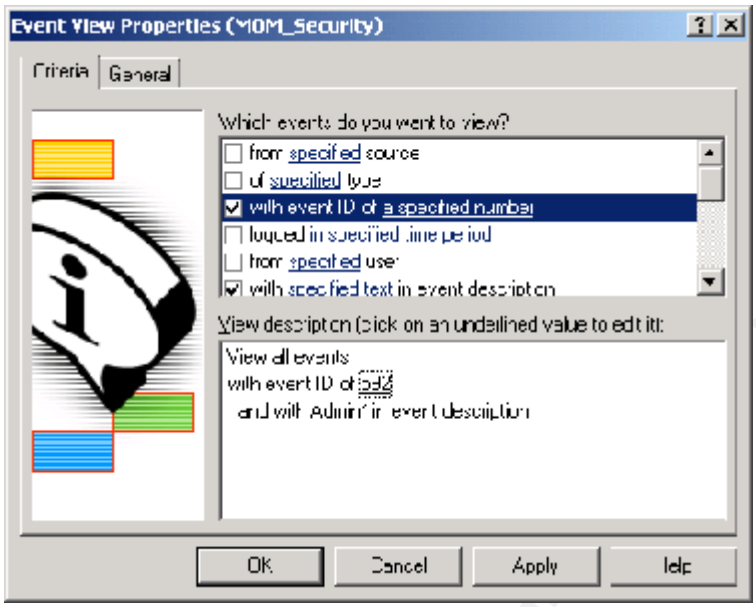


8.7.1 Figure displays choices of what type of event view to create

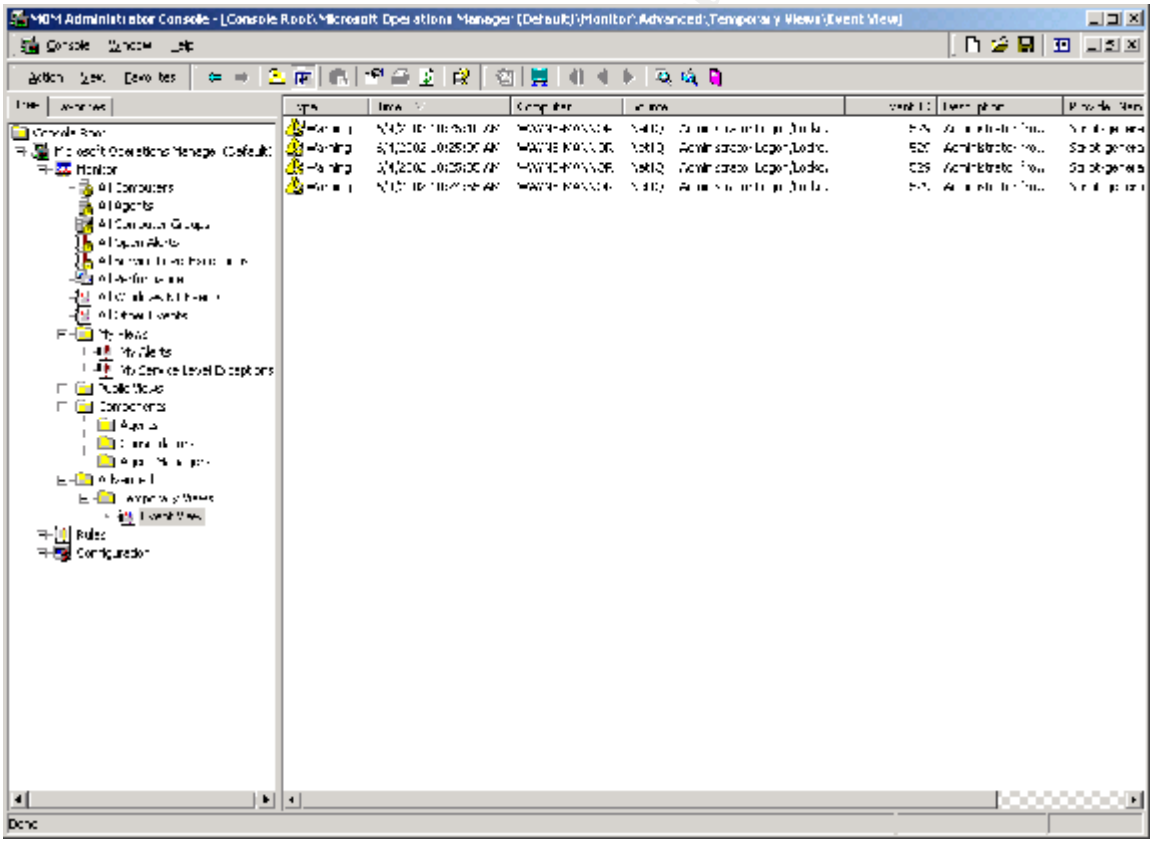


8.7.2 Allows criteria to be specified

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.



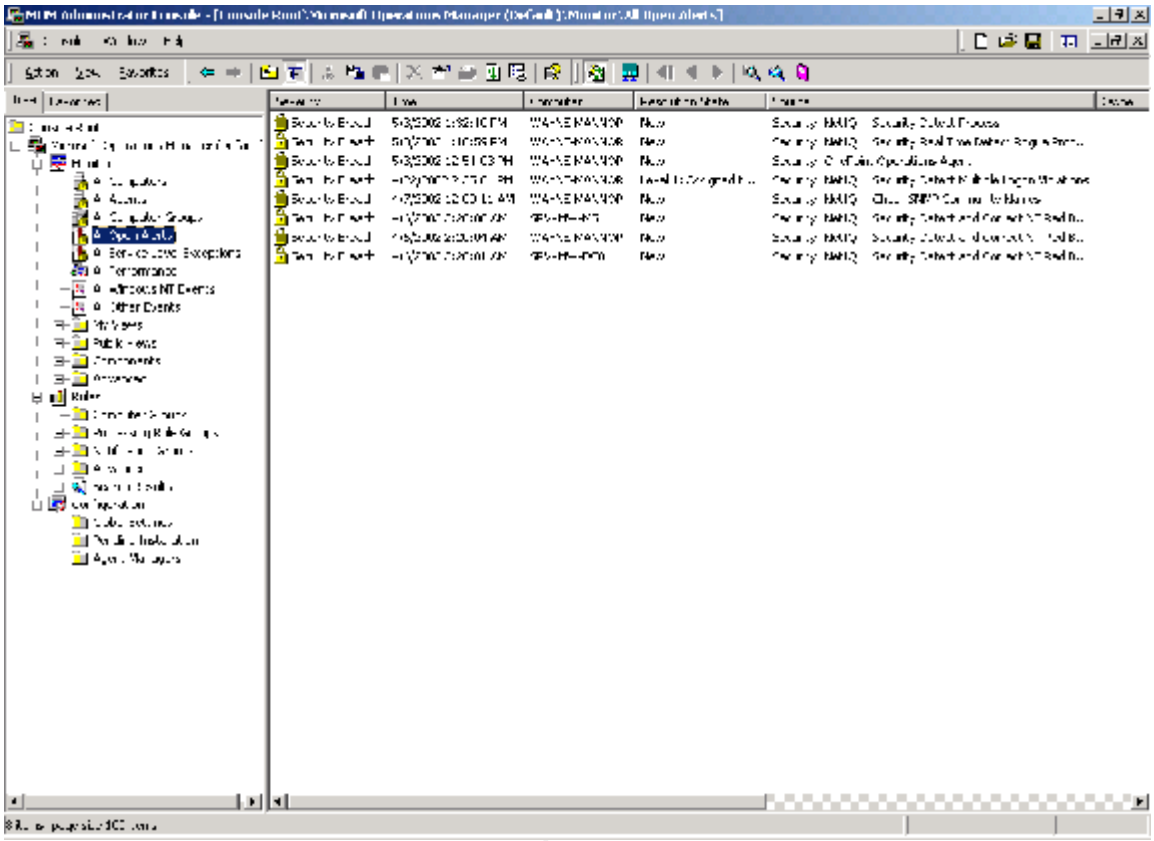
8.7.3 Check the boxes on the left to choose search requirement



8.7.4 Results of custom view creation

8.8 All open alerts will display the current alerts and their status. Views are self updating therefore when new alerts are generated views will automatically be updated displaying the new alerts. Alerts are interactive and respond to double click by opening the alert and right click bringing up an options menu.

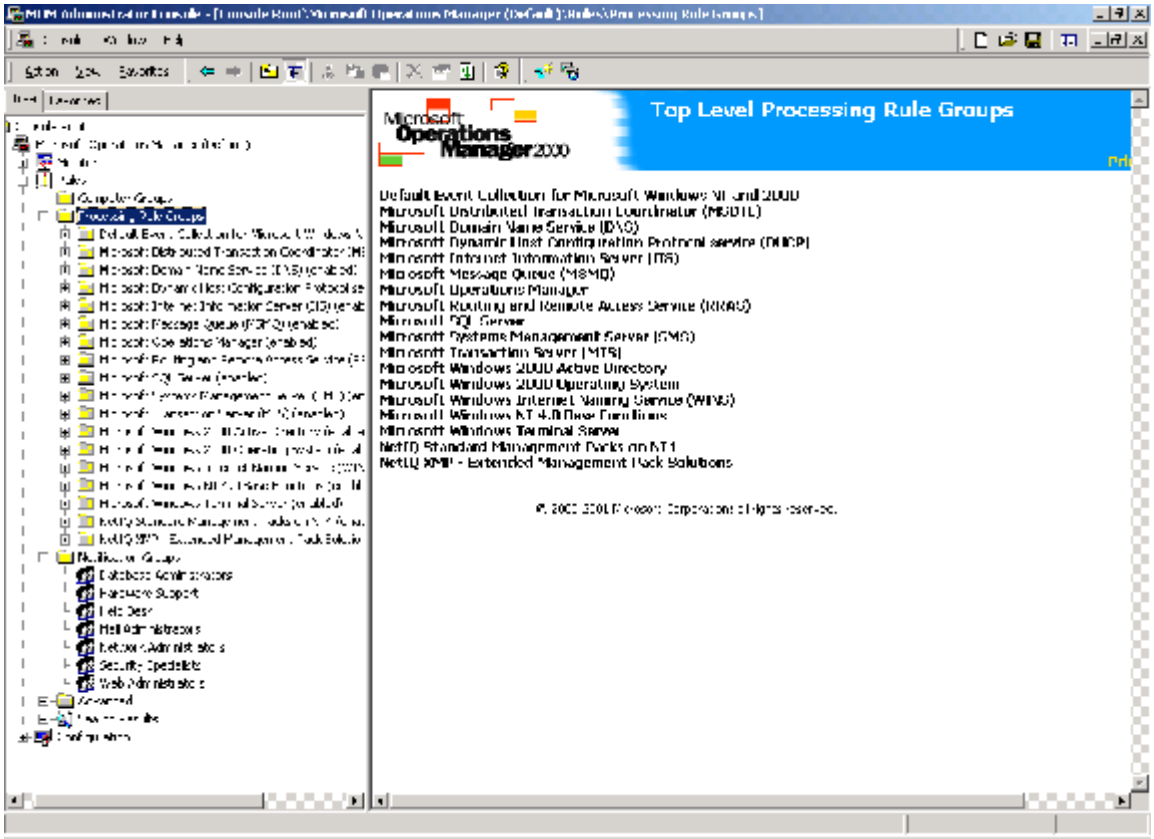
© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.



8.8.1 All open alerts displays alerts, the status, source and owner for a quick view.

8.9 The rules snap-in contains a folder called Processing Rule Groups or PRG. The PRG contains rules and knowledge base for each rule in the management pack. Each PRG contains nested child rule groups. Clicking to highlight the knowledge pack displays the overview knowledge base stating the purpose of the group and each child rule group within. *Rules* is also where computer groups are defined, as well as notification groups. Notification groups specify how administrators are notified when an alert is generated.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

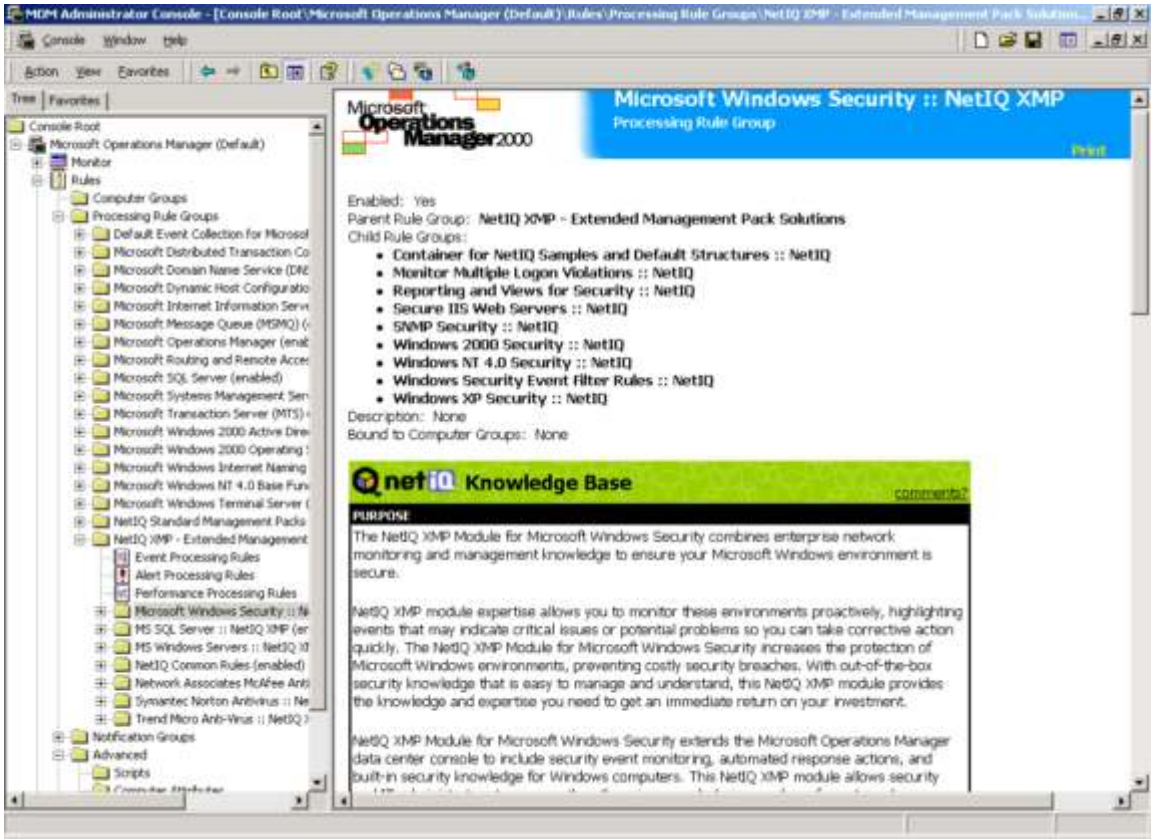


8.9.1 Processing Rule Groups are nested within folders

9. The Security Management Pack

9.1 The NetIQ SMP installs a number of rules into a Processing Rule Group named *NetIQ XMP – Extended Management Pack Solutions.* Note in Figure 9.1.1 the right hand pane the knowledge base shows a brief description of the rule set and in some cases configuration instructions.

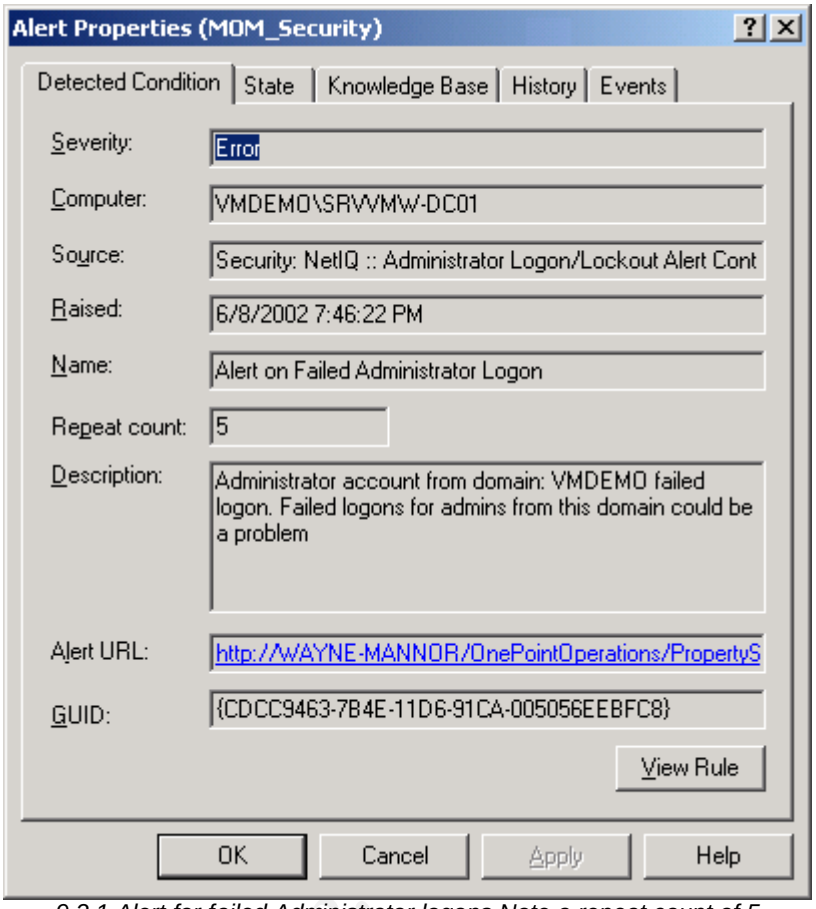
© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.



9.1.1 Figure displaying the PRG that contains security knowledge and rules

9.2 Now that we know how MOM 2000 works we can pull the security functions together. One of the key rule sets that the SMP contains is the ability to correlate failed logon attempts across the enterprise. One simple rule displays when an administrator fails to logon using a bad password. According to the knowledge base for this *alert failed administrator logons could be an indication of an intruder attack*. (SMP Knowledge base for rule located in a default install: NetIQ XMP - Extended Management Pack Solutions\Microsoft Windows Security :: NetIQ XMP\Windows NT 4.0 Security :: NetIQ\Windows Security :: NetIQ (Shared)\Windows Security Events :: NetIQ\) This is accomplished by tracking the event numbered 529 that is of warning severity along with other specific criteria for this event.

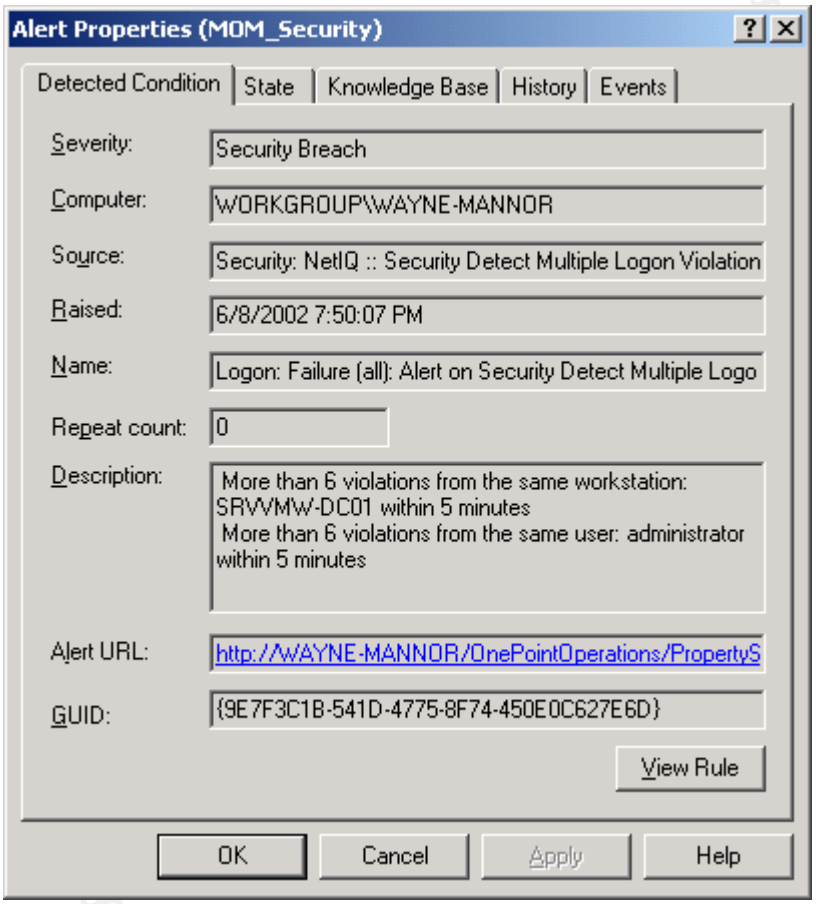
© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.



9.2.1 Alert for failed Administrator logons Note a repeat count of 5

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

9.2.2 Simply tracking a failed Administrator logon is one thing be correlating multiple failed logon attempts across servers regardless of the account is really the power of this functionality. The script that does the correlations pulls the failed logons and generates an event when the maximum number within a given time period is met. Another rule lies in wait for the event that may be generated. It also has the ability to do advanced analysis, which will gather the information about the computers or user that is generating the failures. The advanced analysis can also be set so that it is suppressed within script.

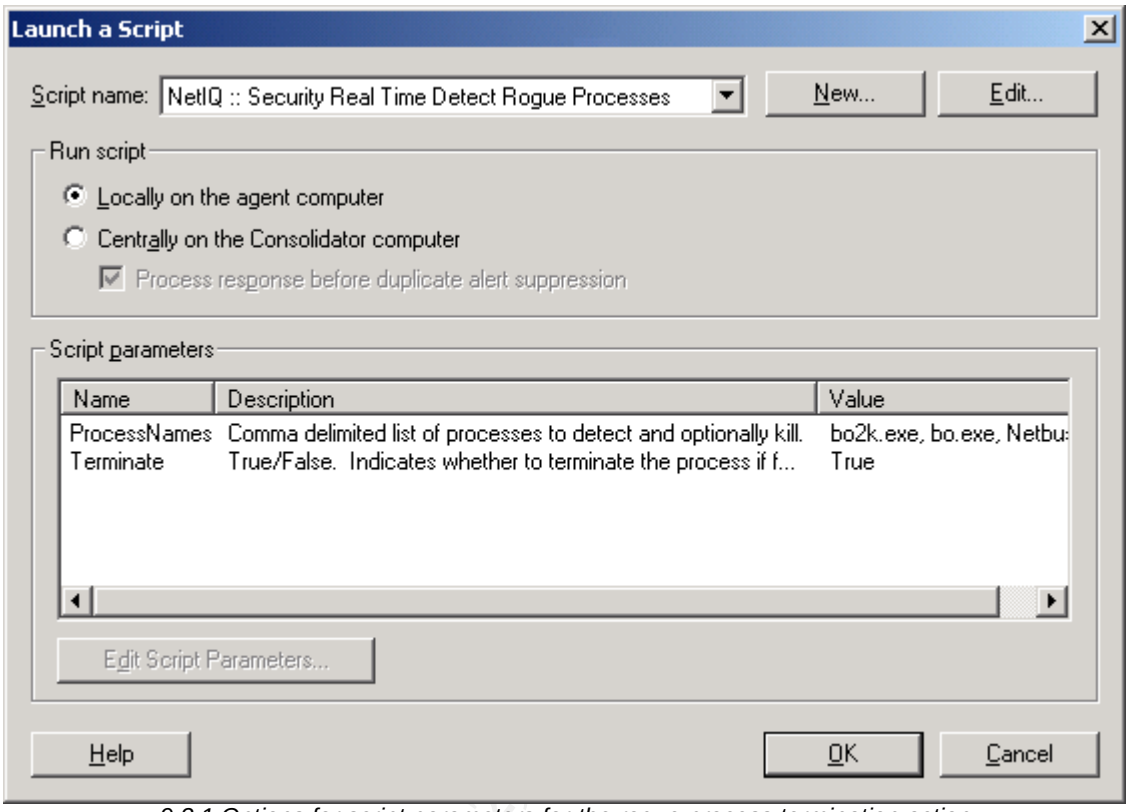


9.2.3 Alert for Multiple failed logon attempts, Note the detailed data in the description

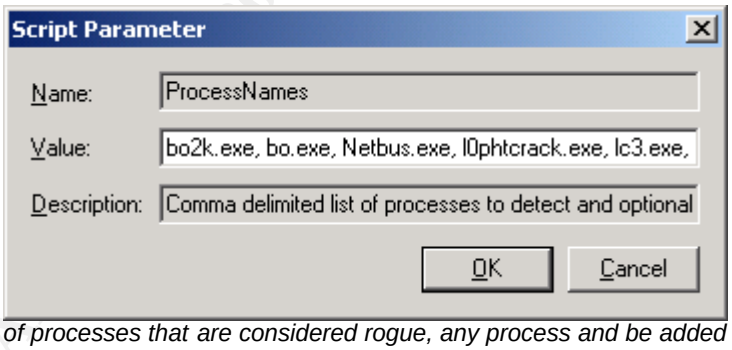
9.3 Another feature of the SMP for MOM 2000 is the ability to automatically detect and optionally terminate a rogue process or application. Any application or malicious code can be defined as rogue. The rule set that handles this operation requires some customization to work properly. The figure below displays the option for the script NetIQ:: Security Real Time Detect Rogue Process. This script is triggered as a response to any application or process launch. Administrators can take the default list of processes or specify additional malicious applications based on local business policy or as new exploits are discovered. Included in the default list are: bo2k, bo.exe, Netbus.exe, PCAnywhere, l0phtcrack.exe, lc3.exe, NetXray, SnifferPro, netmon, tftp.exe, root.exe. Another rule that works similar runs this script on a timed basis looking

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

for rogue applications.



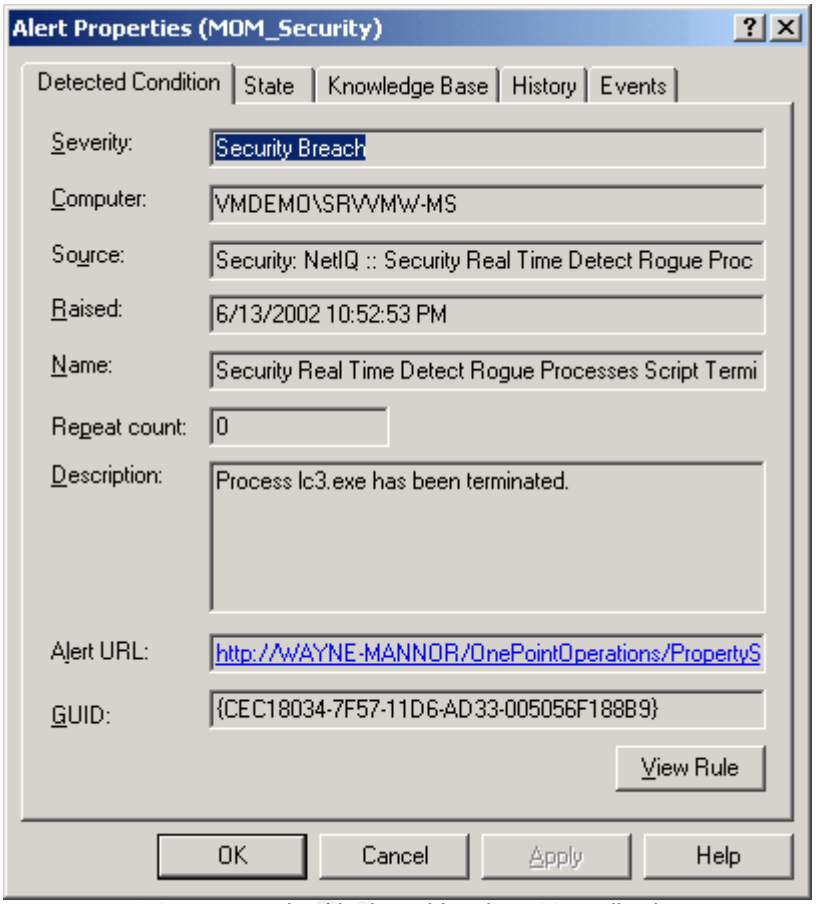
9.3.1 Options for script parameters for the rogue process termination action



9.3.2 List of processes that are considered rogue, any process and be added to this list

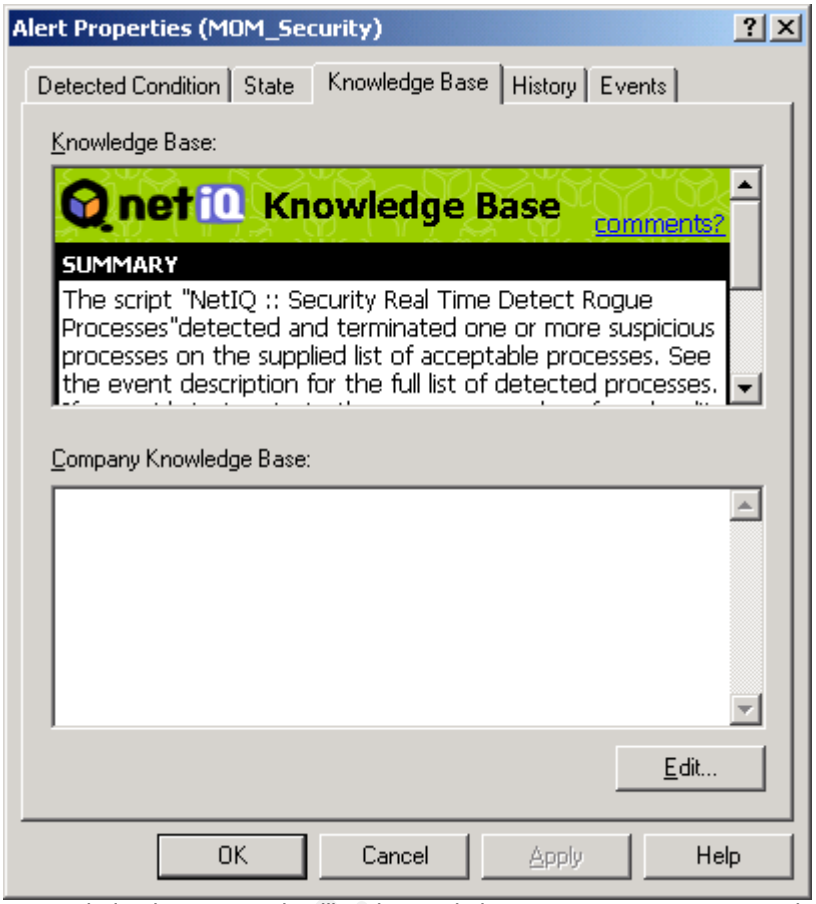
9.3.3 Running lc3.exe on a MOM 2000 agent produced the event in Figure 9.3.4. The detection and termination of the application was “real time”, nearly instantaneous with barely a glimpse of the GUI interface showing.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.



9.3.4 Event raised by launching the LC3 application

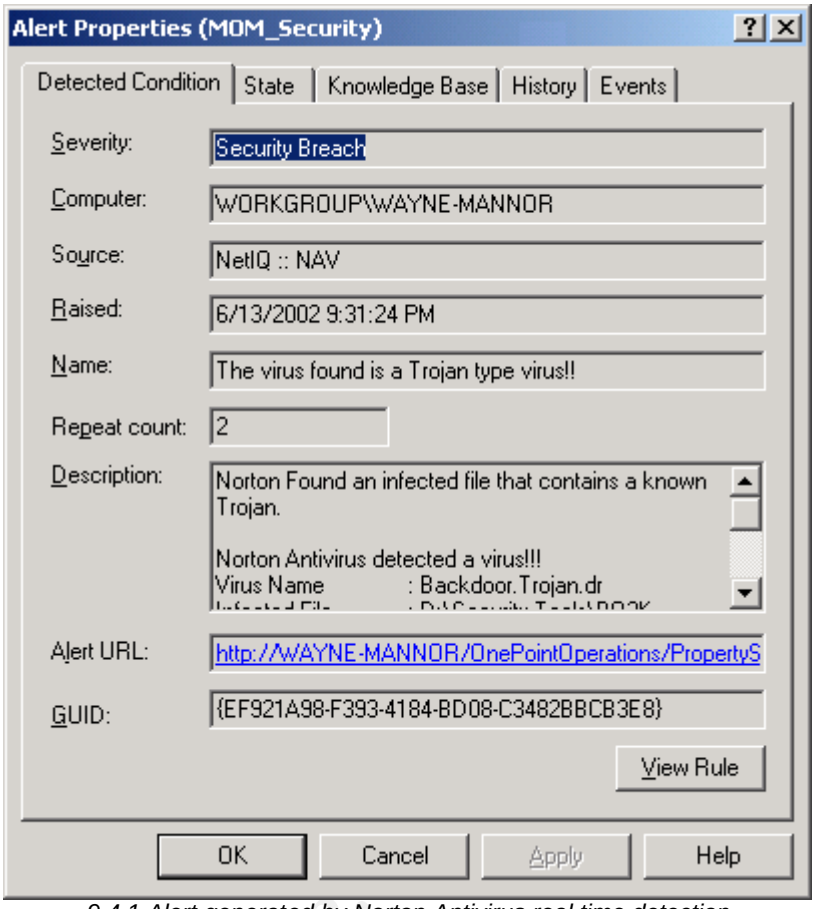
© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.



9.3.5 Knowledge base entry detailing the Real Time Detect Rogue Process rule set
Note the Company Knowledge Base field

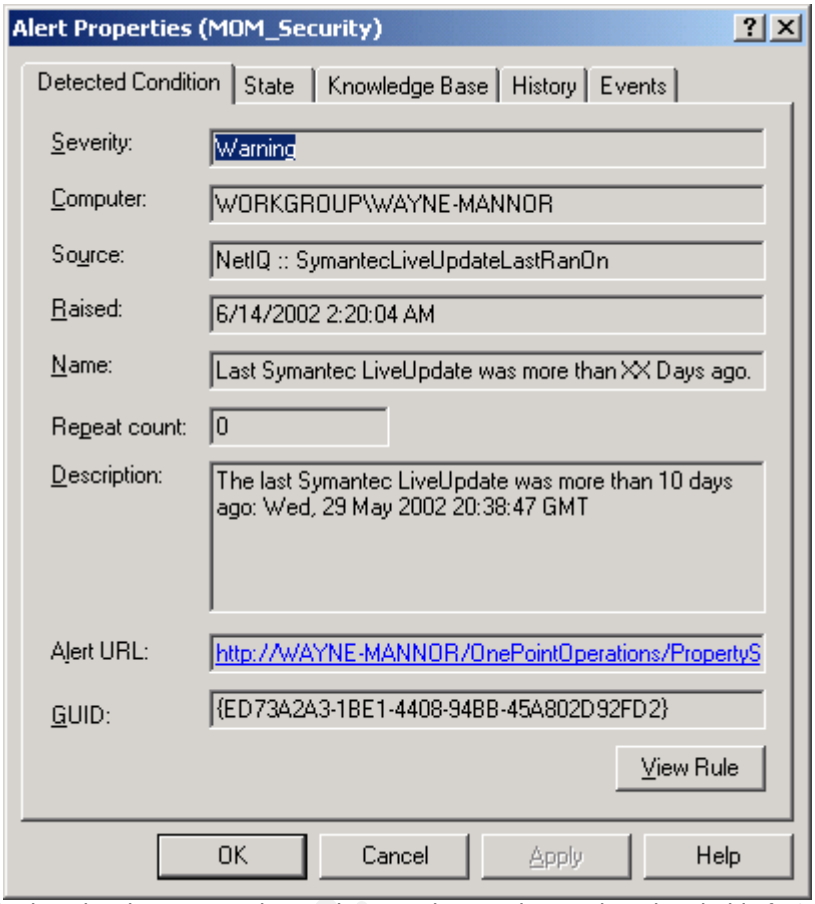
9.4 Monitoring Anti-virus alerts and bringing information about virus outbreaks is the function of the SMP for Anti-Virus. The Anti-virus knowledge module reads events and data provided by Trend Micro Anti Virus, Network Associates McAfee Anti Virus, and Symantec Norton Anti Virus. The knowledge pack also has the ability to monitor the last time signature files were updated or in the case of Norton the last time that Live Update was ran.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.



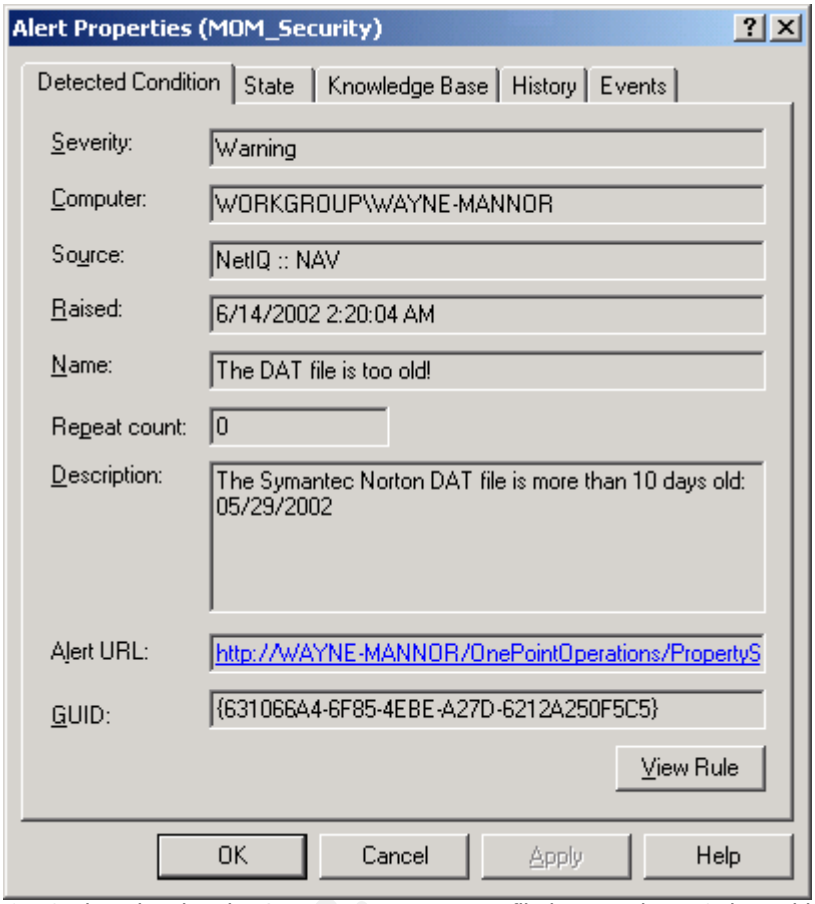
9.4.1 Alert generated by Norton Antivirus real time detection

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.



9.4.2 Alert showing Norton Live Update was last ran longer than threshold of 10 days

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.



9.4.3 Alert showing the Symantec Norton DAT file is more than 10 days old

9.5 Additional functionality of the SMP includes:

- Monitoring interactive logons using a service account and forcing a logoff if necessary
- Alerting when accounts are created and permissions have been elevated
- Alerting on IPSec failures and agent issues
- Administrator password changes
- Adding of trusted domains
- Audit log failures
- Notification of Audit log changes or clearing
- SAM database issues and failures
- Windows file protection and critical file access
- Local policy changes along with Group Policy failures
- Local and global group membership additions
- User rights assigned and modifications
- Reporting and security specific views
- Over 40 VBScripts out of the box for automated response and monitoring
- Supports both VBScript and Jscript
- Built-in knowledge base for all rules
- Flexible rules based architecture allows for custom rule to be created

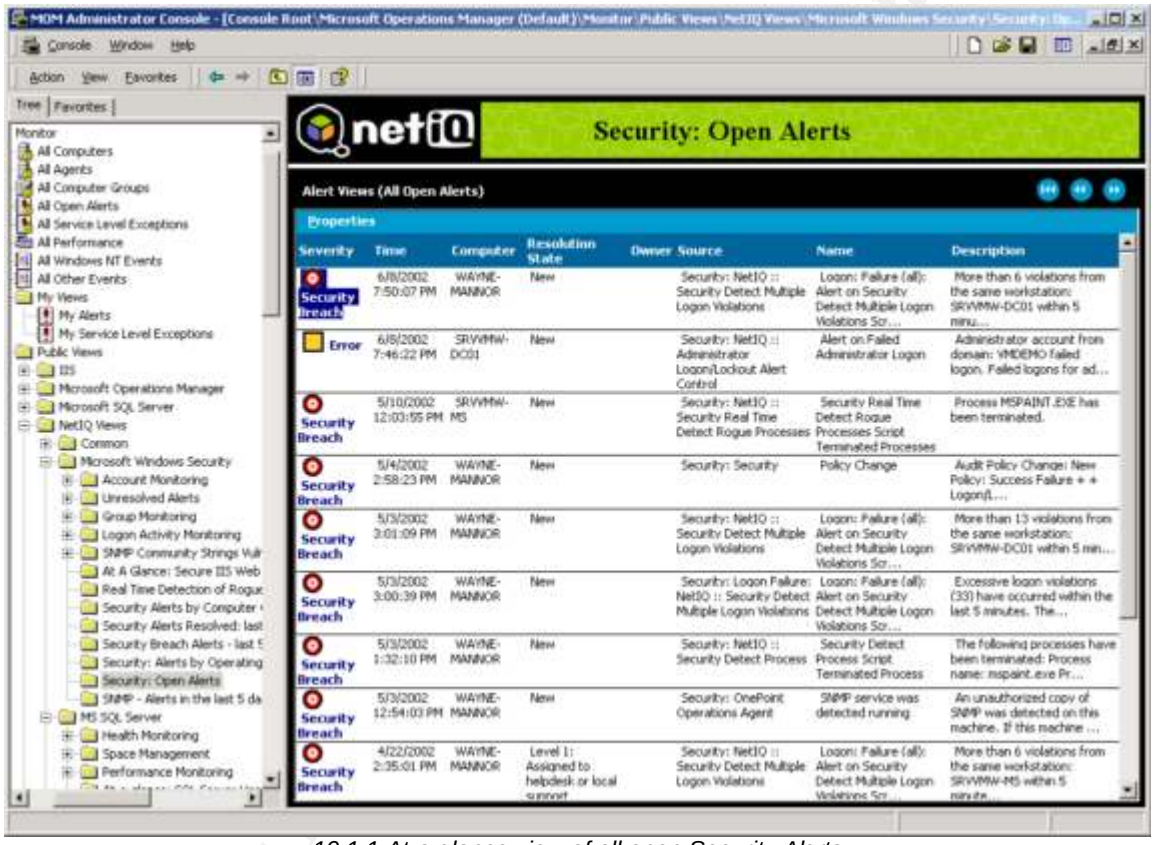
© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

using wizards

Note: This information was gathered by looking through the rule set provided by the SMP. This was a manual process.

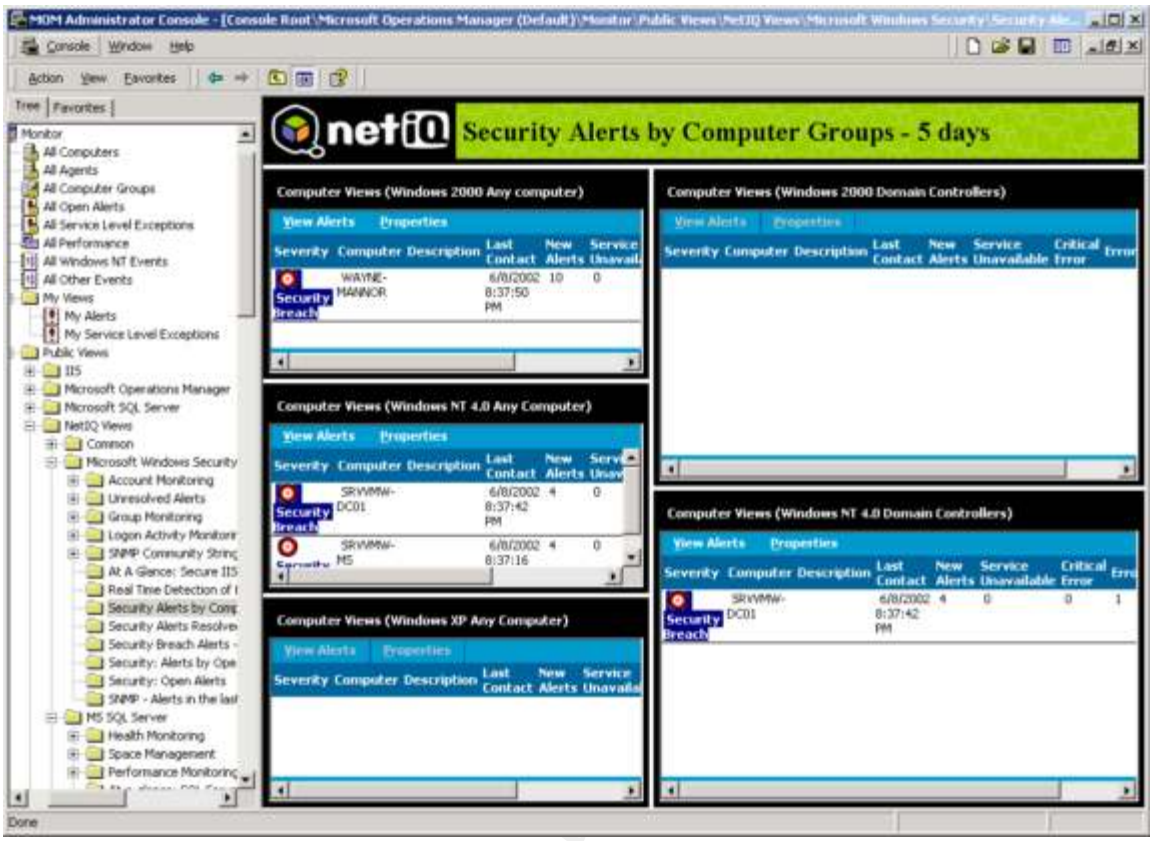
10. At a glance views

10.1 The SMP comes with public views that provide “At A Glance” information about the health and wellness of the monitored systems. This is considered part of NetIQ’s *Active Analytics* for MOM 2000.



10.1.1 At a glance view of all open Security Alerts

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.



10.1.2 Public views by computer group displaying open Security alerts for Windows 2000, Windows NT and Windows XP

11. Conclusion

In the world of Intrusion detection there are many products to choose from. Narrowing the choices to host based IDS there are certain key functionalities that different products have. Some products wrap around the Kernel for protection, some software products protect file systems, others look at network traffic on the host and some look at logs and applications. MOM 2000 with the NetIQ Security Management Pack is the type of IDS that looks at logs and applications. Systems management plays a key role if an overall security strategy. Consequently security is also very important when dealing with systems management. Traditionally these functions have been separate in some large enterprises. While in smaller deployments the administrators can wear many hats crossing the boundaries of security professional and network administrator. This paper has demonstrated some of the functionality that this powerful management tool can provide to both silos. Using the combination of MOM 2000 and the additional add-ons that are provided by independent software vendors can increase overall security, decrease down time and help administrators and security professionals' sleep better at night.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Sources
Internet Sources

Security Operations Guide for Windows 2000 Server
http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/prodtech/windows/windows2000/staysecure/secops01.asp

Microsoft Press release October 12, 2000
http://www.microsoft.com/presspass/features/2000/oct00/10-12dotnet.asp)

NetIQ Press Release February 28, 2000
http://www.netiq.com/news/press_releases/2000/000228MCSMerger.asp

NetIQ XMP Modules for MOM 2000
http://www.netiq.com/products/xmp/default.asp

Microsoft Operations Manager 2000 Partners Site
http://www.microsoft.com/mom/partners/default.asp

Microsoft Operations Manager 2000 Partners Site
http://www.microsoft.com/mom/partners/default.asp

Musich, Paula. "NetIQ Gives MOM Security Extension"
eWeek April 2, 2002
http://www.eweek.com/article/0,3658,s=1884&a=24876,00.asp

Serverware Corporate Website
www.serverware.com

Books
Microsoft Operations Manager 2000 Reviewers Guide Appendix A Page 41

Microsoft Operations Manager Installation Guide Page 41

NetIQ XMP for Security Users Guide was used but not referenced

Personal Interview
Jones, Mark NetIQ Corporation Product Manager XMP for MOM 2000

Seldon, Peter CEO Serverware Group plc

Supplemental
Microsoft, Microsoft Operations Manager, MOM 2000, Microsoft SQL, Microsoft Office and all other references to Microsoft Corporation are registered trade marks of the Microsoft Corporation. See the following URL for details:

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

http://www.microsoft.com/info/cpyright.htm

NetIQ, NetIQ XMP, Active Analytics and all other references to NetIQ Corporation are registered trade marks to NetIQ or its subsidiaries. See the following URL for details: http://www.netiq.com/About_NetIQ/LegalNotices.asp

Any other software product mentioned in this article may be a trademark of their respective companies or owners.

© SANS Institute 2002, Author retains full rights.

Last Updated: June 19th, 2013

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

Digital Forensics & Incident Response Summit 2013	**Austin, TXUS**	**Jul 09, 2013 - Jul 16, 2013**	**Live Event**
SANS London Summer 2013	**London, GB**	**Jul 09, 2013 - Jul 16, 2013**	**Live Event**
SANS Rocky Mountain 2013	**Denver, COUS**	**Jul 14, 2013 - Jul 20, 2013**	**Live Event**
SEC528 SANS Training Program for the CompTIA® New Advanced Security Practitioner (CASP) Certification	**Washington, DCUS**	**Jul 22, 2013 - Jul 26, 2013**	**Live Event**
SANS Mumbai 2013	**Mumbai, IN**	**Jul 22, 2013 - Jul 27, 2013**	**Live Event**
SANS San Francisco 2013	**San Francisco, CAUS**	**Jul 29, 2013 - Aug 03, 2013**	**Live Event**
SANS Boston 2013	**Boston, MAUS**	**Aug 05, 2013 - Aug 10, 2013**	**Live Event**
SANS SEC 560: Network Penetration Testing @ Bangalore 2013	**Bangalore, IN**	**Aug 05, 2013 - Aug 10, 2013**	**Live Event**
Critical Security Controls Summit	**Washington, DCUS**	**Aug 12, 2013 - Aug 18, 2013**	**Live Event**
Industrial Control Systems Security Training - DC	**Washington, DCUS**	**Aug 12, 2013 - Aug 16, 2013**	**Live Event**
SANS Virginia Beach 2013	**Virginia Beach, VAUS**	**Aug 19, 2013 - Aug 30, 2013**	**Live Event**
SANS Thailand 2013	**Bangkok, TH**	**Aug 19, 2013 - Aug 31, 2013**	**Live Event**
SANS Melbourne 2013	**Melbourne, AU**	**Sep 02, 2013 - Sep 07, 2013**	**Live Event**
SANS Capital City 2013	**Washington, DCUS**	**Sep 03, 2013 - Sep 08, 2013**	**Live Event**
Network Security 2013	**Las Vegas, NVUS**	**Sep 14, 2013 - Sep 23, 2013**	**Live Event**
SANS Canberra 2013	**OnlineAU**	**Jul 01, 2013 - Jul 13, 2013**	**Live Event**
SANS OnDemand	**Books & MP3s OnlyUS**	**Anytime**	**Self Paced**