



Harford Technology Corporation

HP Openview NNM Security Configuration Version 0.72

Abstract

As companies strive to become part of the e-Commerce industry, the Network and associated Systems are often the enabling technology for the business plan. Therefore, solid measures must be taken to protect the infrastructure from known (and unknown) threats present in the industry.

To aid in this endeavor, Harford Technology Corporation has assembled the attached security profile for Hewlett Packard's Openview NNM. This document is intended to provide the necessary information to secure the System, while balancing operational concerns and maintaining the necessary scalability.

As new threats and techniques evolve, this document will be updated to reflect the new information.



© 2003 Harford Technology Corporation. All right reserved.

The information contained in this document represents the current view of Harford Technology Corporation on the issues discussed as of the date of publication. Because of the dynamic nature of business computing environments, Harford Technology Corporation cannot guarantee the accuracy of any information presented after the date of publication and/or delivery.

Harford Technology Corporation makes no warranties, express or implied, in this document.

Harford Technology Corporation is a registered trademarks of Harford Technology Corporation. Other product or organizational names mentioned herein may be the trademarks of their respective owners.

Table of Contents

Abstract	1
<u>Table of Contents</u>	5
Distribution	7
Document Update Process	7
Contributors	7
Conventions	7
Installation	9
Post Install	9
Map Ownership	10
HP Openview Configuration and Application Security	11
Miscellaneous Issues	12
Event Configuration	13
Sudo (Superuser DO) Configuration	14
General Considerations	15
Audit -	15
Change Control -	15
References -	16
Appendix A – Rediscovery	17
Appendix B – newsyslog.HTC	18

Distribution

This document can be released to **SPECIFIC** clients with approval from the Account Manager and Operations Manager.

Document Update Process

The mechanics of an update process are TBD. However, this will require collaboration among many within the company. We will make certain that credit is given to the folks that help us keep the document up to date and aware of the latest issues

Contributors

-
-
-
-

Conventions

As we elaborate on the concepts and necessary commands to realize the concepts, we will present the information in the following manner

Bold is used to display commands and options.

Italic is used to display arguments and options. These should be replaced locally defined values.

[] used to surround optional elements in the description of syntax

| used to separate optional arguments when illustrating a list where only one alternative may be chosen at a time.

< > used to illustrate one or more required parameters

Installation

HP Openview NNM must be installed by 'root' as most applications in the Unix realm require. However, In a system that has been secured in accordance with the Harford Technology Corporation Security Practices (i.e.; Solaris) pay special attention to the 'umask' value as you may inadvertently install the application such that only 'root' can see and use the application.

In addition, make certain to document the following information, as it may be needed in the event of a support call.

- Host ID
- System Name
- TCP/IP Address

- HP 'Support Handle'
- HP License Key
- Any relevant information regarding non-standard issues

Post Install

There is generally a cumulative patch available for NNM from the Openview web site at <http://support.openview.hp.com/cpe/patches/>

Immediately following the install is probably the best time to apply any necessary patches to the system. In addition to the cumulative patch, there may also be security related patches that are deemed necessary. Pay special attention to any noted dependencies.

Map Ownership

By default when launching a session (ie; GUI) for NNM, the first session is launched with Read-Write access to the default map. Subsequent sessions are launched as Read-Only.

The Read-Write map, due to it's properties, can be modified by the current operator. This is generally undesirable as in terms of mission critical systems, not just anyone should have the ability to make changes.

To contain this issue, we strongly recommend the following actions

- Create the group oadmin
- Create the user oadmin (SUID Only)

```
ovwchown oadmin default
ovwchgrp -a oadmin
ovwchmod 775 default
```

The result changes the map ownership to the SUID account 'oadmin.' Also, the group ownership is changed to 'oadmin.' Finally, the mode is changed to 775 or -rwxrwxr-x. This controls access to the Read-Write map in that the user must be a member of the 'oadmin' group to have the authority to change the map.

Users who are not a member of the group 'oadmin' will still have the ability to use NNM, however, they will not be able change any characteristics of the map display.

HP Openview Configuration and Application Security

The HP Openview NNM framework is very powerful in that it can be configured for nearly ANY environment. Also, NNM has many other tools such as the MIB application builder, threshold monitoring etc. These tools are extremely powerful, however, incorrectly configured, they may have an adverse effect on the system as well as the network. To control access to these tools, we strongly recommend controlling access to these facilities via the methods described below.

Assuming the user/group oadmin exists from the previous section, we will control access using the basic mechanics of Unix file permissions.

The files listed below control the following configuration characteristics and applications:

MIB Application Builder: SNMP
Data Collection & Thresholds: SNMP
Alarms
Load/Unload MIBs: SNMP
SNMP Configuration
Event Configuration
Network Polling Configuration: IP

```
chmod 440 $OV_REGISTRATION/c/ovsnmp/xnmbuilder
chgrp oadmin $OV_REGISTRATION/c/ovsnmp/xnmbuilder
```

```
chmod 440 $OV_REGISTRATION/c/ovsnmp/xnmcollect
chgrp oadmin $OV_REGISTRATION/c/ovsnmp/xnmcollect
```

```
chmod 440 $OV_REGISTRATION/c/ovsnmp/xnmevents
chgrp oadmin $OV_REGISTRATION/c/ovsnmp/xnmevents
```

```
chmod 440 $OV_REGISTRATION/c/ovsnmp/xnmloadmib
chgrp oadmin $OV_REGISTRATION/c/ovsnmp/xnmloadmib
```

```
chmod 440 $OV_REGISTRATION/c/ovsnmp/xnmmibappl
chgrp oadmin $OV_REGISTRATION/c/ovsnmp/xnmmibappl
```

```
chmod 440 $OV_REGISTRATION/c/ovsnmp/xnmsnmpconf
chgrp oadmin $OV_REGISTRATION/c/ovsnmp/xnmsnmpconf
```

```
chmod 440 $OV_REGISTRATION/c/ovsnmp/xnmtrap  
chgrp ovadmin $OV_REGISTRATION/c/ovsnmp/xnmtrap
```

This configuration will allow only those users whom are members of the ovadmin group access those configuration tools/applications.

Also, in the event that more granular control is desired, this technique can be expanded to accommodate nearly any organizational structure.

Miscellaneous Issues

NNM requires a variety of configuration files to achieve its goal. However, some of these files are installed such that any user has the ability to make changes. To prevent accidental or malicious modifications it is recommended that the following actions be performed.

```
chgrp ovadmin $OV_CONF/.license  
chmod 664 $OV_CONF/.license  
  
chgrp ovadmin $OV_CONF/collectProxyMap  
chmod 660 $OV_CONF/collectProxyMap  
  
chgrp ovadmin $OV_CONF/mib.coerce  
chmod 660 $OV_CONF/mib.coerce  
  
chgrp ovadmin $OV_CONF/mibExpr.conf  
chmod 660 $OV_CONF/mibExpr.conf  
  
chgrp ovadmin $OV_CONF/ovspmd.auth  
chmod 660 $OV_CONF/ovspmd.auth  
  
chgrp ovadmin $OV_CONF/ovuispmd.state  
chmod 660 $OV_CONF/ovuispmd.state  
  
chgrp ovadmin $OV_CONF/ovw.auth  
chmod 660 $OV_CONF/ovw.auth  
  
chgrp ovadmin $OV_CONF/ovwdb.auth  
chmod 660 $OV_CONF/ovwdb.auth  
  
chgrp ovadmin $OV_CONF/polling
```

```
chmod 660 $OV_CONF/polling

chgrp ovadmin . $OV_CONF/snmpCol.conf
chmod 660 $OV_CONF/snmpCol.conf

chgrp ovadmin $OV_CONF/snmpRep.conf
chmod 660 $OV_CONF/snmpRep.conf

chgrp ovadmin $OV_CONF/snmpmib
chmod 660 $OV_CONF/snmpmib

chgrp ovadmin $OV_CONF/snmpmib.bin
chmod 660 $OV_CONF/snmpmib.bin

chgrp ovadmin $OV_CONF/statTimeRanges.conf
chmod 660 $OV_CONF/statTimeRanges.conf

chgrp ovadmin $OV_CONF/C//trapd.conf
chmod 660 $OV_CONF/C//trapd.conf

chgrp ovadmin /etc/opt/OV/share/www/conf/session.conf
chmod 444 /etc/opt/OV/share/www/conf/session.conf
```

Event Configuration

Although there is no one correct answer in the realm of event configuration, in the event that any custom programming and/or scripting is utilized be cognizant of the following issues:

- Ownership
- Group Ownership
- Crontabs
- SMTP Configuration
- Fault Tolerance

Sudo (Superuser DO) Configuration

Sudo will undoubtedly require discussion, as all clients/installs are different. A first cut would suggest leveraging sudo as a tool of 'last resort' in that senior engineers may feel that it is necessary to disable NNM temporarily in the event of large scale changes or large scale outages.

This can help 'bridge the gap' that may be created based on the necessary control of the root password by not making it impossible to manage the system in the absence of the root password. As with any configuration, Sudo can and will grow and evolve to meet the necessary objectives in a balanced fashion with regard to security and operations.

Sudo is available from the following sites

<http://sunfreeware.com>
<http://www.courtesan.com/sudo/index.html>

The documentation that is present on the courtesan web site and that accompanies sudo has extensive documentation regarding the installation and operation of the package. Also, bundled with the package are extensive man pages relating to its deployment and operation. In addition, Courtesan supports a variety of mailing lists relating the use and development of sudo.

General Considerations

The information and policies listed above are merely a starting point. No amount of policy and/or procedures can substitute for due diligence.

For instance, HP typically releases known security problems with work-arounds between Versions. It is the administrator's duty to determine the need for these patches. This may be a balance between Operational Issues as well as security Needs.

Also, there are MANY mailing lists such as SAFER, and SANS, that distribute a great deal of information for Openview NNM and the related threats, new attacks, and new methods of security.

Audit -

Standard reports should be created to list the Device's characteristics such as OS revision, Interfaces, etc. It is likely that 3rd party tools will be required to construct the appropriate information.

Change Control -

A logbook should be kept of all changes made to the system. This is not only related to security, but to 'General Operations Best Practices' as well. Each host will have a record book, that begins with the install, installer and date right through to a reformat.

References -

Solaris Security, v 1.0, Sans Institute, <http://www.sans.org>

Solaris Operating Environment Network Setting for Security, Alex Noordergraaf & Keith Watson, Sun Microsystems, December 1999

Solaris Operating Environment Security, Alex Noordergraaf & Keith Watson, Sun Microsystems, January 2000

Sudo in a Nutshell, <http://www.courtesan.com/sudo/intro.html>

Appendix A – Rediscovery

The following steps will delete the current Openview Database and restart the network discovery process.

```
$OV_BIN/ovstop -c  
  
rm -rf $OV_DB/openview/*/*  
rm -rf $OV_DB/eventdb/*/*  
  
xnmsnmpconf -clearCache  
  
$OV_BIN/ovstart owdb  
  
$OV_BIN/ovw -fields  
  
$OV_BIN/ovstart
```

As the discovery begins, be certain to apply the map ownership defined earlier in the document.

```
ovwchown ovadmin default  
ovwchgrp -a ovadmin  
ovwchmod 775 default
```

Appendix B – newsyslog.HTC

Below you will find the source for the script newsyslog.HTC. This replacement for newsyslog orients the designated logs and their archival along a calendar date. Also, to add some flexibility to the process, we have created a configuration file called newsyslog.conf. The file will contain the log entries that we will rotate based on the date and time. We recommend the newsyslog.HTC script be run at Midnight via cron.

--- start newsyslog.HTC ---

```
#!/bin/ksh
#
# newsyslog.HTC
#
# Usage:
#
# newsyslog.HTC
#
# There are no command line parameters at this time
#
# Dependencies:
#
# Uses the configuration file /usr/lib/newsyslog.conf to determine what files will be
# rotated in relation to the calendar date. If this file is not present, the Script
# will abend and email the designated administrator.
#
# The syntax of the configuration file is as follows ...
#
# # Comments are permitted under the standard notation with a '#' at the start
# # of the designated line.
# # Blank lines are not permitted at this time
# /var/adm/messages
#
# Notes:
#
# Several actions exist with the script but are commented out as there is no generally
# recognized default value. Otherwise the command is complete with the exception of the
# designated values noted with < value >.
#
# Created on May 19, 2003 by Mark Leighty ( mleighty@harfordtechnology.com )
#
# Copyright (2003) Harford Technology Corporation. With the exception of
# commercial resale, lease, license or other commercial transactions, permission
# is granted to use, copy, modify, and distribute this software. By exercising this
# permission you agree, that this Notice will accompany this software at all times.
#
# Harford Technology Corporation. MAKES NO REPRESENTATIONS OR WARRANTIES
# OF ANY KIND CONCERNING THIS SOFTWARE OR USE THEREOF.
```

```

#
# ----- #
# Revision Log #
# ----- #
VERSION=o.86 # mleighty@harfordtechnology.com
# Still some rough edges but good enough to begin testing at a 'beta'
# level. Will deploy as possible seeking feedback from pilot customers.
# ----- #
# Revision Log #
# ----- #
# Try to open /usr/lib/newsyslog.conf ... if it exists we're OK. If not we'll
# send an email to root and abort.
if [[ -f /usr/lib/newsyslog.conf ]]; then
#
# This may be extreme, however, for the truly paranoid where their processing
# schedule allows, we can down the hosts Interfaces if deemed necessary.
#
# ifconfig hmex down
# Loop through the files in newsyslog.conf one at a time. Note that the grep
# function shown eliminates the standard comment line
for FILE in $( cat /usr/lib/newsyslog.conf | grep "^[^#]" )
do
#
# At midnight we'll move the logfile to logfile.date ( ie; yesterday's date )
#
mv $FILE $FILE.`TZ=EST+24 date +%d%b%Y`
#
# Standard Mechanics to create the new log file, permissions, owner, etc.
#
touch $FILE
chown root:root $FILE
chmod 600 $FILE
#
# Look for any entries older than 30 days ( default ) and move to an archive
# location. This should be fast as we are limiting it to a particular directory
# and filename. Note the patters for the directory and filename. The default
# assumes that the directory structure is 2 levels deep. In the event the directory
# structure moves beyond 2 levels the pattern ${FILE%/*} will require modification.
/usr/bin/find ${FILE%/*} -name ${FILE##*/} -mtime +30 -exec mv {} /var/Archive \;
done
#
# Reset the syslog daemon as we have disrupted the filehandles for the logs

```

```
#
kill -HUP `cat /etc/syslog.pid`

#
# Now that the syslog daemon is 'fully functional' we can restart the interfaces
#
# ifconfig hmex up
else
#
# Something is amiss. As a default we'll notify root.
#
echo "Subject:Log Archival Aborted!!\n\nLog Archival `date +%d%b%Y` - Aborted ... \
/usr/lib/newsyslog.conf not found" | /usr/lib/sendmail root
fi

#
# Manage the disk space efficiently. Remove log entries older than 1yr. Or ... greater
# based on local policy
#
#/usr/bin/find /var/Archive -mtime +365 -exec rm {} \;

--- end newsyslog.HTC ---

--- start newsyslog.conf ---

#!/bin/ksh
#
# newsyslog.conf
#
# List of files to rotate on a calendar basis. Used as the configuration
# for the updated newsyslog.HTC script.
#
# To add a file to the newsyslog.HTC rotation, add the full path and name
# of the log file as displayed below.
#
# Syntax:
#
#   Comments are permitted with the traditional '#' at the start of a line
#
#   The filenames and path are entered in the following manner
#
#       /var/adm/messages
#
#   We'll handle the rest
#
# Copyright (2003) Harford Technology Corporation, With the exception of commercial
# resale, lease, license or other commercial transactions, permission is granted to use,
# copy, modify, and distribute this software. By exercising this permission you
```



```
# agree that this Notice will accompany this software at all times.  
#  
# Harford Technology Corpration. MAKES NO REPRESENTATIONS OR WARRANTIES  
# OF ANY KIND CONCERNING THIS SOFTWARE OR USE THEREOF.  
#  
/var/adm/messages  
/var/log/syslog  
  
--- end newsyslog.conf ---
```

