

NightWatch Release Notes

4.2.1 January 12, 2004

Fixed a variety of problems in the Out-of-Process Server Library component (OPSLib.exe) added in 4.2 release.

When running NightWatch in a remote VNC session, you must add the registry key shown here:

HKEY_CURRENT_USER\Software\ORL\VNCHooks\Application_Prefs\OPSLib.exe\use_Defferal to 0

This will prevent run time errors at startup.

Added new function to ScriptGlobals object available to scripts run by Task MOs. The match function will compare a string to pattern and will return TRUE if a match is found, false if not. Calling sequence is:

```
boolval = sg.match(string, pattern)
```

The format of the pattern string can be found in the on-line help under pattern matching in the topic index.

4.2 October 1, 2003

With this release of NightWatch, significant changes have occurred in the design of this product. Please read these notes carefully and consider the impact of the changes on your use of NightWatch before you proceed with this update.

Multi-Threading

Previous NightWatch releases used multi-threading to keep the user interface responsive during the time NightWatch is scanning monitored objects for alarm events. This was fine for the early releases but as the number of features has grown the multi-threading technology has become untenable.

In 4.2 the multi-threading design has been changed. The new form of MT is active at all times so the menu option to enable/disable MT has been removed. With this new design, a compromise has been found that has removed the increasing reliability problems of the old MT design and retained most of the scan speed and user interface responsiveness. This means (depending on your specific installation setup) the scan time and user interface may be slightly slower than with old MT turned on. However it will be much faster than running with old MT turned off, and will give vastly improved reliability.

For the most part, MOs remain unchanged. One area that does need your consideration is Task and Host Login MOs. One side effect of the new MT design is that scripts run slower than before. This will most likely mean that the timeout value on your Task and Host Login MOs will need to be increased. The exact impact of this varies with processor speed and load, so some users may see no problems and some may see timeouts if they don't increase the existing timeout values.

Service Operation

There are several major changes in Service Mode Operation. Prior to 4.2 if you paused NightWatch while running as a service the NightWatch main screen would appear and you could interact with that screen. Due to a variety of interconnected problems with service mode operation, this feature is no longer supported. With 4.2, if you pause the NightWatch service, the service will simply pause operation but no screen will appear. In this respect, NightWatch now functions the same as all other services. Services do not normally present any user interface and doing so was causing problems that could not be fixed.

During Service Mode Operation, NightWatch must impersonate some user account in order to have appropriate security credentials. Prior to 4.2 the service installed with Local System as the default service logon user account and then NightWatch would assume (impersonate) the identity of the user account that is entered on Options Tab 2, Service Install area. This after start-up impersonation scheme worked for the most part but more and more problems came up with this scheme failing to provide the security context needed for newer NightWatch features, like WMI and logging via Instant Messaging.

The solution in 4.2 drops impersonation after service start. Instead, it will install the service with the user account entered on Options Tab 2 as the default Logon user account for the service. By doing this, the security context of that user is successfully assumed by NightWatch for all functions when the service is started.

For updating users who run NightWatch in Service Mode, after update you will need to go to Options Tab 2 and UNINSTALL as a service. Then you must enter a user in the boxes on the tab with appropriate privilege to run the service and support the MOs and features you wish to use. Then click the Install as a Service button to install the NightWatch Service with that user as the default Service logon user. If you leave the user name blank and click Install as a Service, the Local System account will be used. Local System is adequate for some MOs but not others. Selecting an appropriate administrative user account is the better way to set up the NightWatch service. See the on-line help for more information on running NightWatch as a service.

Processing errors now include identification of the Monitored Object that caused the processing error.

Microsoft's forced upgrade of MSN Messenger users to version 5.0 or later, created major problems for our Messenger client logging feature. Our implementation of MSN Messenger logging was based on version 4.7 of Messenger. That implementation was not compatible with Messenger 5.0 and later. This required a rewrite of our Messenger support. This new implementation is contained in the OPSLib.exe file and is not dependant on any specific Messenger version. In fact, Messenger no longer needs to be installed on our host system. The file MessengerTool.exe is now obsolete and can be removed.

Added new toolbar button on the System View screen that will show only the defined MO groups and the MOs they contain.

It is now possible to customize the alarm cleared message text that is sent via email and paging with a registry key. If this is of interest, please contact tech support for details.

All MOs that use COM ports and the Paging Tab of the Options screen now display a drop down list of all COM ports that exist on the host system instead of a fixed list of COM1-COM4.

The ScriptGlobals object that supports Task MO scripts now exports a function called Shutdown. This function will shutdown the local or a remote system. A new script sample called Shutdown.txt is included in the Scripts\Samples directory.

A new Monitored Object has been added that supports the Room Alert 2 environment monitoring hardware device.

Paging can now be done over a network connection via the SNPP (Simple Network Paging Protocol) protocol to an SNPP capable paging provider. SNPP offers an alternative to paging via dial-up using the TAP paging protocol. TAP is being discontinued by some providers including ATT and in that case access to such paging providers is by email or SNPP only.

4.1.3 August 11, 2003

Fixed a bug in saving configuration to a disk file. On reload, any passwords read from the .cfg file were corrupted.

You may now set the SNMP query port on the SNMP Query MO. Previously it was fixed at the standard value of 161. Being able to change the port allows NightWatch to support agents using a non-standard port.

Fixed run time error when selecting paging groups on the Manual Paging screen.

Fixed email return address to be the return address entered on the Options screen Email tab. Previously, the return address was always 'NightWatch@systemname'.

Fixed run time error on the Service MO add/change screen.

4.1.2 June 2, 2003

Modify Verizon paging .msg files. Note that VerizonPager.msg works with Verizon Wireless Messaging PAGERS. Verizon.msg works with Verizon cell phones. Verizon paging and cell phone messaging are handled by two very separate divisions. The list of dial up numbers has been updated for the two Verizon services.

The FTP Get monitored object was extensively reworked to handle the IBM AS400 system correctly.

Fixed bug in Event Log monitored object that caused a run time error if an event record contained more than 25 message substitution strings.

4.1.1 April 21, 2003

Fix DNS Monitored Object. This MO is included in the DataCenter Edition of NW but was incorrectly set up to be in the Enterprise Edition.

Fix the System View screen to be rebuilt the next time it is opened after MOs have been added, deleted or modified.

The Microsoft part of the Network Scan function would fail if there was a Terminal Services server present on the network. This has been fixed.

4.1 March 24, 2003

Added a new Monitored Object, Bandwidth. This MO monitors the network interface(s) on a target system and generates an alarm if traffic on an interface exceeds a user defined threshold.

Added a new Monitored Object, Directory. This MO monitors a windows disk directory and can generate an alarm if the directory disk space or file count exceeds user-defined thresholds. It can also alarm on any change to directory size or file count. This MO can also monitor a specific file for size or size change.

Added a new Monitored Object, DialUp. This MO monitors a dialup modem line by dialing the line number and confirming that the modem connects and does so with a time limit. Also supports RAS via Windows Dial Up Networking.

Added a new Alarm Notification option, Instant Messaging. This feature allows activity logging and alarm notifications to be sent to Instant Messaging clients. This feature uses the Microsoft MSN Messenger client version 4.6 or 4.7 on the system where NightWatch is installed. A messaging user is established with the MSN Messaging Service (or Exchange Messaging Service) for NightWatch. Messaging users add the NightWatch user to their contact/buddy lists and will receive information from NightWatch when it is scanning. See the Help for more information.

Fixed bug that could cause a run time error if running multi-threaded and a scan was stopped while scanning a TCP or UDP Service Monitored Object.

The Log File MO has been modified to allow wild cards in the disk file name. When wild cards are present, the MO searches the target directory and opens the most recent file meeting the wild card spec. This file is examined and closed. This allows the MO to monitor a log file that may have ongoing iterations denoted by date/time or a sequence number in the file name. The MO selects that most recent interaction of the file on each scan. The processing of file names without wildcards remains unchanged.

The SNMP Query and Performance Counter Query MOs have been modified to allow individual Objects or Counters in the Query to be disabled. If an Object or Counter is disabled, its value is still retrieved from the target system (so the value is available to the option script) but the value is not automatically evaluated by the MO.

The Web Page MO has been enhanced to allow multi-level link checking. You can now specify on the MO how many levels of links will be checked. Level zero checks no links in the target page, which is the same as the MO has operated in the past. If the Link Level is set to 1, the page links (A html tag) in the target page are each retrieved. If set to 2, the Links on the Level 1 pages are each retrieved, and so on. Note that graphic file references and forms pages are always retrieved.

The Host Process and Host Volume Monitored Objects have been enhanced to use SNMP as well as Telnet to retrieve process and volume data from host systems. This allows access to hosts without Telnet support. New host types added to the Host Type drop down list include VMS via Telnet and NetWare via SNMP.

In the AlphaNumeric Script paging language, the W (write to log window) statement used to write text to the main Activity Log window if the Log Level was 2 or 3. The Log Level must now be 3 for W messages to appear in the Activity Log window.

Fixed bug in Manual Paging screen that caused a run time error if a paging Group was selected as the target of a Manual Page.

Added the ReBoot System and Delete Files pre-defined Task Monitored Objects. These Task MOs can be added from the New Monitored Object selection screen. The ReBoot System Task executes a script that will restart the target Windows system. The Delete Files Task will delete the specified file set from a Windows directory.

Added the NetWare Server Health check pre-defined SNMP Query Monitored Object.

Fixed bug in SNMP Mib Explorer that caused the SNMP objects retrieved from some MIBs to not have the correct data type.

Fixed a bug in the Disk Log File Viewer screen. Some users encountered run time errors and some cases where the Print button did not function.

Fixed a bug in the FTP GET Monitored Object that caused it to not work correctly with VMS systems.

The Licensing and copy protection mechanisms in NightWatch have been strengthened in this release. If you have problems with MOs that quit working, it may be because NightWatch was not correctly enforcing some of our licensing rules in the past and allowed use of MOs that are not part of the license you have purchased.

The Install process had a bug which caused a new entry to be added to the Windows Add/Remove Programs list for each new version, instead of just updating the existing entry. This is because the version number was included in the Add/Remove entry name. This caused an accumulation of out of date entries in the Add/Remove list. Now, the Installer will add a single entry for this product and update it with each subsequent install. To remove the redundant entries, use RegEdit and find the key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall Delete any subkeys with this product name and a version number.

4.0.3 January 14, 2003

Fixed bug in search string processing that would cause a match to be found if the search string file contained a trailing blank line and the target string contained any spaces.

Fixed Run Time Error in SNMP MIB Explorer. MIB Explorer would abort if the target MIB contained an object id value with a very large number in any of the object id component parts.

Fixed bug in HostVolume MO. Extraneous output lines on host disk volume display output were not correctly ignored and fouled up the reading of volume information for the legitimate volumes.

4.0.2 December 16, 2002

Fixed bug in Web Status. Display of activity log failed under some conditions.

Added Windows XP System Health pre-defined Performance Counter MO.

4.0.1 December 2, 2002

Fixed bug in Performance Counter MO that caused a Run Time Error.

Fixed bug in Host Volume MO that caused a Run Time Error.

Fixed bug in Manual Page screen that caused a Run Time Error.

Improved formatting of SNMP Trap messages when additional SNMP objects are sent as addendums to the trap message.

Fixed the Web Page MO to correctly handle the BASE html tag.

4.0.0 October 25, 2002

NightWatch for NT has been renamed NightWatch. A side effect of this name change can cause problems when updating a previous release. When updating, NightWatch will try to locate the existing install directory and update that directory. If you uninstall the previous release first or change the install directory path for the new (any) install, file names stored in your configuration may no longer be correct. Up to now, if you uninstalled and installed fresh, the path name stayed the same (NightWatch for NT) and there was no problem. Now, if you uninstall and install fresh, the path name will be just NightWatch. It is not necessary to uninstall before an update, so updating your existing installation is recommended. Be sure to watch the install process and see that the installer properly detects your existing install. If it does not, set the install directory manually to the existing directory.

When installing 4.0.0, you may be prompted to insert the Microsoft Office CD. This is caused by a bug in a Microsoft component that is shared by NightWatch and MS Office. Insert the Office CD and continue.

Added new Monitored Object, Host Process, which monitors processes on host systems, such as Unix, Linux, VMS, AS400, HP3000. This MO uses Telnet to connect to specified host systems and obtain a process list. This list is compared to a list of expected processes and an alarm is generated for any missing processes. This MO works in a manner similar to the Host Login MO, but is simpler to configure.

Added new Monitored Object, Host Volume, which monitors disk volume free space on host systems, such as Unix, Linux, VMS. This MO uses Telnet to connect to specified host systems and obtain a disk volume list. Disk volume free space is extracted from this list and compared to preset thresholds. An alarm is generated when a disk's free space falls below it's threshold. This MO works in a manner similar to the Host Login MO, but is simpler to configure.

Added new Monitored Objects, Win 2000 System and Win XP System. These MOs monitor Windows 2000 and XP systems to see if they are up in the same manner as the existing Windows NT System MO.

Added new Monitored Object, UDP Services. This MO monitors UPD network services such as SNMP and generates an alarm if the services are not active. Note that TCP and UDP services are very similar in nature but use different protocols. Note: the UDP Services MO only works when NightWatch is running on Windows 2000 or XP.

Added new Monitored Object, DNS Check. This MO monitors a Domain Name Service server to make sure the server is functioning and returning correct name to address mappings.

Added a new Monitored Object, ePage. This MO monitors an email mailbox and processes each mail message as a Page request. Contact names are put in the message subject separated by semi-colons. The first 80 bytes of the message body is sent as the page text. This allows you to send pages by sending email to the mailbox that is being monitored.

Added a new Monitored Object, Heart Beat. This MO generates an alarm on every scan, subject to Interval and Schedule settings. It can be connected to an appropriate Alarm object to perform notification that NightWatch is still up and running.

Added a new Options Tab called Auto Add. This tab displays the list of known network objects as detected by the Ping, SNMP and Windows auto discovery scans (also known as Network Scans). From this list of network objects, you can select a group of objects and automatically create new Ping Monitored Objects for them.

Added a new feature to aid in displaying large configurations. You can now organize monitored objects into Groups. You can then select these Groups for display on the Status screen and Web Status. On the new MO Groups tab of the Options screen, you can create arbitrary Groups and added MOs to these Groups. The Groups are then listed in the MO subset dropdown lists on the Status and Web Status displays.

The Status Screen now has grid lines drawn to separate the rows and columns to make this screen easier to read.

The Status Screen now displays the Monitored Object Type icons along with the object type text label.

The Web Status display's list of Monitored Objects will now allow you to toggle between display of the MO Identifier and MO Description. You can click on the small white box next to the Identifier column header to switch between Identifier and Description.

The Monitored Object Selection screen displayed when adding a new MO has been enlarged so more MO types can be seen without scrolling. You can also see the available MO types as a list.

Scan time and alarm time for MOs is now tracked and allows for a new display of percent alarm time (down time) for each MO on the Status screen and Web Status display. This new display shows the percent of time an MO spends in alarm state versus the total time the MO has been monitored. This data will help identify problem network objects by highlighting those objects that spend excessive time in alarm state.

The Scan Logging function now includes the information collected for the computation of the percent alarm time. There are new fields for total scan time and total alarm time. The log file also includes a new record for alarm end events with the elapsed time of the event. Users who employ the Scanlog log files should generate sample files with the column labels included to see the new format.

The Web Status pages used to display 'N/A' in blank fields. Now, blank fields are just that, blank.

The maximum message length for TAP paging protocol now defaults to 100 characters. This limit can be changed in a .msg script file with the T statement or you can change the default with a registry key.

The Web Page MO now will insert http:// into the page URL if it is missing. The Web Page MO add/change screen has been updated to better display the mini web browser that allows you to verify the URL to be monitored.

Fixed Disk Volume MO to handle 32-character volume labels correctly.

Fixed Web Page MO to correct handle HTML tags with redundant attributes specified in the tag.

Fixed Web Status internal web server bug that caused error 24056 to be intermittently displayed in the log window.

Previously, the Mib Explorer screen would not display any MIB objects downloaded from the SNMP agent if the STOP button was clicked during the MIB walk (download). This did not support stopping the MIB walk early on very large MIBs. Now, if the STOP button is clicked, the SNMP objects downloaded to that point are displayed and can be selected.

The Disk File MO can now monitor the size of files.

The Search Strings function on various monitored objects now supports matching on strings not found. Search strings may be prefixed with the ! character to invert or not the result of the search string match to the target text supplied by the monitored object. See the online help for string searching.