WatchDog

Lets say you have installed Advanced Host Monitor on reliable server and setup thousand test items to monitor entire network (or several networks). HostMonitor will inform you in case of any problem. Unless... unless something happens to system where HostMonitor is running. What if power supply dies, motherboard fries or Windows crashes due to some buggy driver? What if your main router stops responding?
There are various solutions. Lets start from less effective and go to the most effective.

1) You may setup HostMonitor to check connection to your router or ISP and use “network independent” alerts (such as “Send SMS using GSM modem”) to inform you about this problem.
2) You may setup HostMonitor to start alerts when another operator stops monitoring or disables alerts (using “Pause monitoring/alerting” dialog window) or just allow to stop monitoring for single administrator account using User Profiles

Sure, this will not help when system where HostMonitor is running crashes. There is another option:

3) You may use HostMonitor’s built-in Scheduler to start some action(s) on regular basis. E.g. you may setup HostMonitor to send e-mail to your smart phone every 30 min. If you do not receive e-mail then you know something is wrong.

You think this is annoying and not effective solution? We agree. There are much better solutions. There are other ways to monitor the monitor.

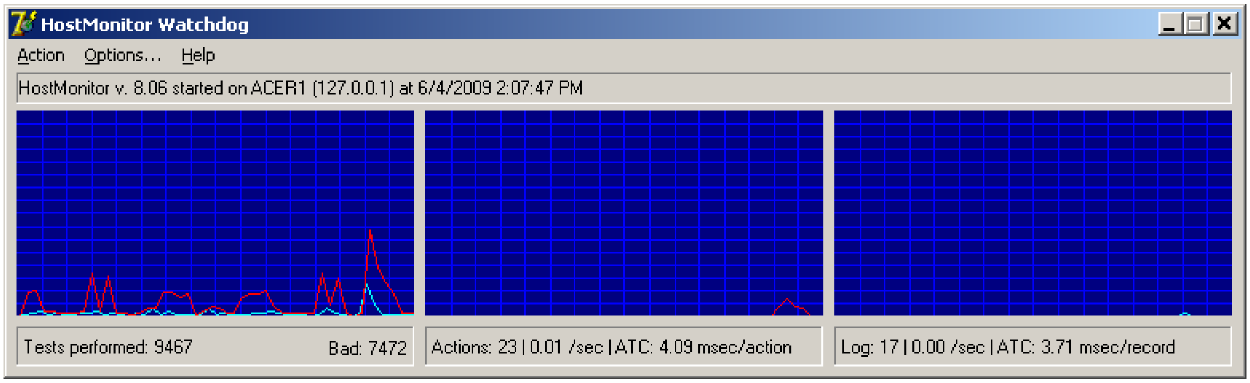
4) Manually: You may use RCC, Web Service or Telnet Service to check HostMonitor remotely. This way you may see what is going on, what test fails, what actions executed; you may acknowledge statuses and change test parameters. You can do anything but you should do everything by yourself. RCC will not be able to take any actions when HostMonitor stop responding (except call for help in case you set “play sound” action)

5) There is another way: install WatchDog (and optionally another instance of HostMonitor) on another system and use this system to monitor primary monitor automatically 24/7. Even better: you may setup 2nd system to start network monitoring when primary HostMonitor does not respond.

6) And finally you may monitor primary HostMonitor using another copy of HostMonitor! In such case all necessary action can be started automatically. Also there is another good feature: primary HostMonitor may monitor backup HostMonitor so each system will monitor colleague!
While WatchDog provides charts and alerts in one application at no additional cost (it is included into Enterprise package), 2nd instance of HostMonitor will provide great flexibility and reliability. See HM Monitor test method.
Note: If you want to install HostMonitor on 2 systems, you need to order 2 licenses.

So, lets talk about WatchDog.

WatchDog can be used as interactive application that displays statistic information and charts in real-time. It does not allow you to manage test items like Remote Control Console. It provides just basic information about HostMonitor health: you will see is monitoring started and actions enabled, how many test probes HostMonitor performs, how many test probes failed, how many actions started, etc.



HostMonitor v. 8.06 started on ACER1 (127.0.0.1) at 6/4/2009 2:07:47 PM

Tests performed: 9467 Bad: 7472

Actions: 23 | 0.01 /sec | ATC: 4.09 msec/action

Log: 17 | 0.00 /sec | ATC: 3.71 msec/record

In case you have many thousands of test items, Remote Control Console may increase network load and put additional load on HostMonitor (HostMonitor needs to encrypt information about each performed test probe and send data to RCC).
In the same case WatchDog requests just general statistics information and does not increase resource usage.

On the other hand, you may start WatchDog as Win32 service, setup some actions and leave it unattended. Service will be started automatically on system boot, WatchDog will try to connect to HostMonitor and examine connection almost constantly. If connection drops, WatchDog will execute specified actions and try to reconnect. If connection recovered, service will start another set of actions.
For example you may use the following set of actions:

“bad” actions

- Visual/sound alert when connection drops and 1st reconnect attempt failed
- Send syslog message to some console if connection cannot be established for 1 minute
- Start external program (sendmail): send e-mail to admin if connection cannot be established for 1 minute
- Start external program: start backup HostMonitor if connection cannot be established for 2 minutes

“good” actions

- Visual/sound alert when connection restored
- Start external program (sendmail): send e-mail to admin if connection is stable for 1 minute
- Start external program: stop backup HostMonitor if connection is stable for 2 minutes

Windows version: also WatchDog shows icon in system tray and changes icon image depending on conditions: connection dropped; connection established while HostMonitor alerts disabled; connection established but monitoring stopped; everything is Ok (connection established, monitoring started and alerts enabled).

WatchDog configuration

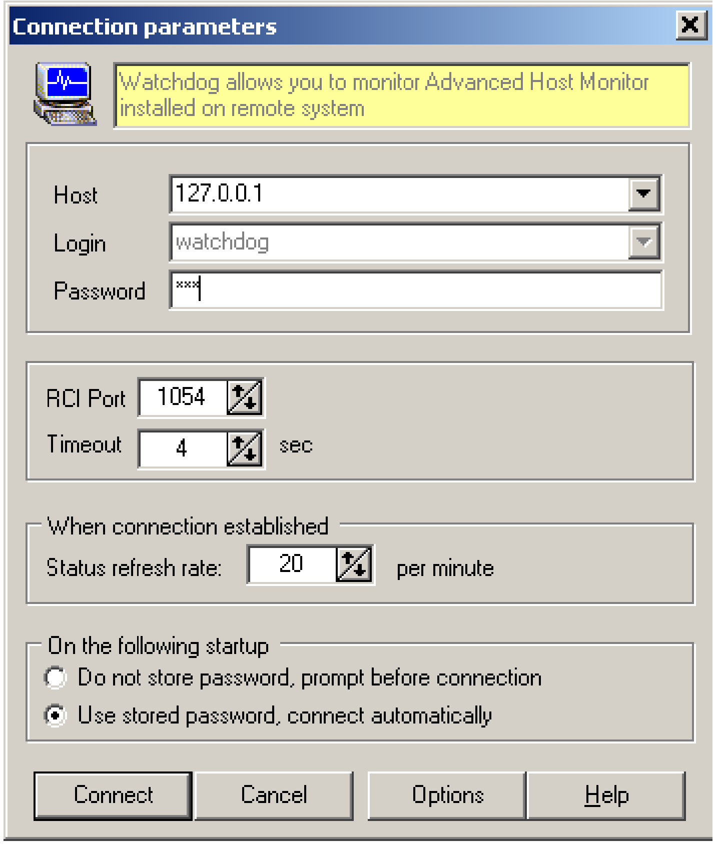
To allow remote monitoring of HostMonitor please follow these simple steps:

- start HostMonitor
- configure HostMonitor's Remote Control Interface on RCI page in the Options dialog (menu Options)
- setup “watchdog” user account: specify password and list of acceptable IP addresses using HostMonitor's menu "User"->"Operators"

Now you may start WatchDog, type address of the system where HostMonitor is running (**Host**), enter password (**Password**) and click "Connect" button. That's it.

When TCP connection established and authentication passed, WatchDog will display information about HostMonitor, show real-time charts, etc.

Optionally you may change TCP port used by HostMonitor, RCC, Web Service and WatchDog (RCI port); specify timeout and status refresh rate.



Connection parameters

Watchdog allows you to monitor Advanced Host Monitor installed on remote system

Host: 127.0.0.1
Login: watchdog
Password: ***

RCI Port: 1054
Timeout: 4 sec

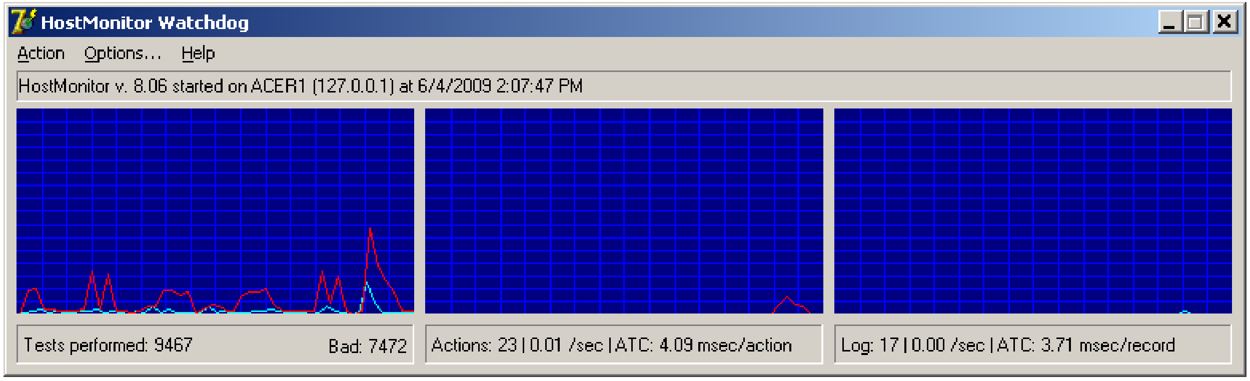
When connection established
Status refresh rate: 20 per minute

On the following startup
○ Do not store password, prompt before connection
● Use stored password, connect automatically

- **RCI Port**:
  if you setup HostMonitor to use other than the default TCP port (default port is 1054), please specify the same port to be used by WatchDog; If system where HostMonitor is running protected by firewall, make sure firewall does not reject TCP requests on RCI port
- **Timeout**:
  the maximum amount of time (in seconds) WatchDog will keep waiting for the reply from HostMonitor before returning an error response;
- **Status refresh rate**:
  WatchDog requests HostMonitor at regular intervals and retrieves statistical information. Refresh rate option specifies how often such requests should be made.
- **Do not store password, prompt before connection**
  if this option selected, WatchDog will show “Connection parameters” dialog and ask for password on every startup
- **Use stored password, connect automatically**
  use this option when you want to start WatchDog without human interaction. Application will store password and connect to HostMonitor automatically at startup. If you want to start WatchDog as service, you should use this option.

Note: you may change connection parameters at any time using menu “Action”->”Connect to HostMonitor”

If you just want to watch HostMonitor performance charts, your setup is done. WatchDog will request HostMonitor, retrieve statistics, display charts, information about performed tests, actions, logging



HostMonitor v. 8.06 started on ACER1 (127.0.0.1) at 6/4/2009 2:07:47 PM

Tests performed: 9467 Bad: 7472

Actions: 23 | 0.01 /sec | ATC: 4.09 msec/action

Log: 17 | 0.00 /sec | ATC: 3.71 msec/record

Note: ATC means Average Time Consumption.
E.g. “Actions: 230 | 0.01/sec | ATC: 4.09 msec/action” means the following:

- HostMonitor performed 230 actions
- HostMonitor started 0.01 action per second (in average)
- HostMonitor used 4.09 milliseconds for each action execution (in average). Note: HostMonitor calculates time used by main thread for logging and actions, it does not include time used by auxiliary threads because its not so important

This information can be useful for investigation of some 3rd party software related problems (e.g. if ODBC driver specified for ODBC logging consumes too much time).

Options/Actions

If you want to receive alerts while you away from HostMonitor and WatchDog, you need to setup “actions”.

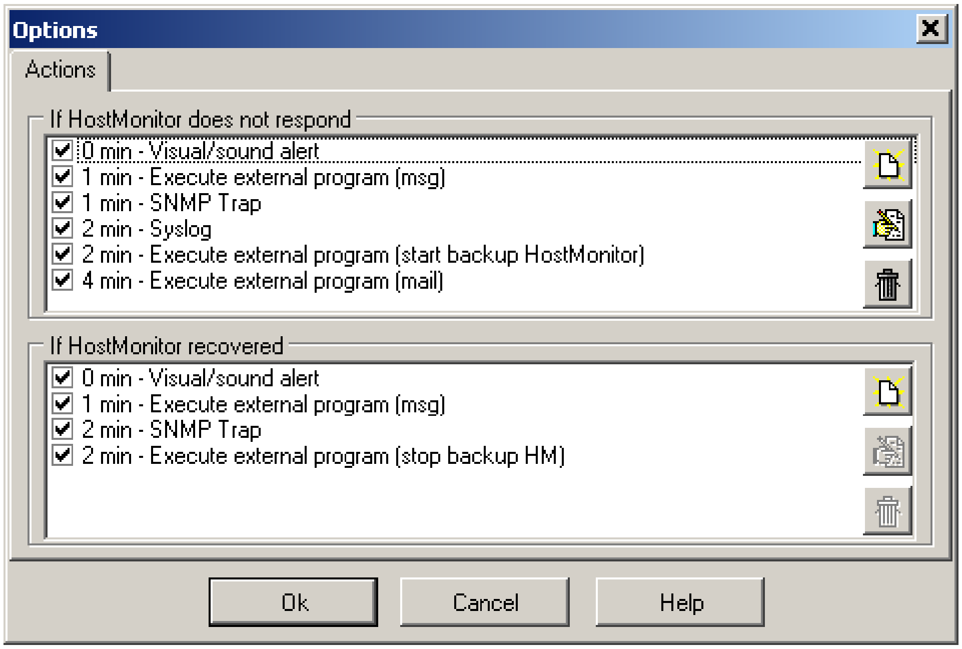
You may setup 2 lists of actions

- one set will be executed when HostMonitor does not respond for some time
- another set will be executed when connection established and it is stable for specified period of time

To work with actions you can use the Options dialog. To bring up this dialog use menu Options

To modify each set of actions use buttons located on right side of the list:

Add	Add new action into set
Edit	Bring up Action Properties dialog for editing parameters of the selected action
Delete	Remove selected action



If HostMonitor does not respond

- ☑ 0 min - Visual/sound alert
- ☑ 1 min - Execute external program (msg)
- ☑ 1 min - SNMP Trap
- ☑ 2 min - Syslog
- ☑ 2 min - Execute external program (start backup HostMonitor)
- ☑ 4 min - Execute external program (mail)

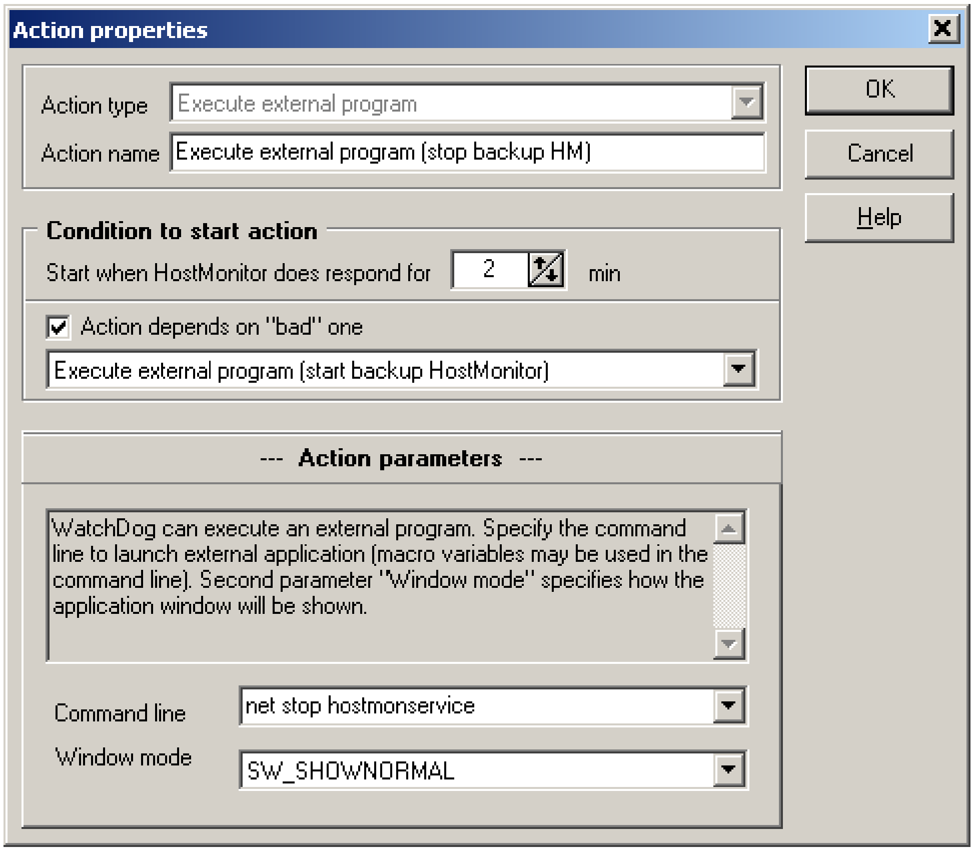
If HostMonitor recovered

- ☑ 0 min - Visual/sound alert
- ☑ 1 min - Execute external program (msg)
- ☑ 2 min - SNMP Trap
- ☑ 2 min - Execute external program (stop backup HM)

Here is a list of available actions to kick off in response to a problem:

- Visual/Sound alert
- Execute external program
- Syslog
- SNMP Trap

Action properties are defined in the Action Properties dialog. Some properties are common across all action types. However, each type of action has a set of parameters that are specific to the action type. Let's have a look at the common properties first (these parameters located in the upper half of the Action Properties dialog):



Action type: Execute external program

Action name: Execute external program (stop backup HM)

Condition to start action

Start when HostMonitor does respond for 2 min

☑ Action depends on "bad" one

Execute external program (start backup HostMonitor)

--- Action parameters ---

WatchDog can execute an external program. Specify the command line to launch external application (macro variables may be used in the command line). Second parameter "Window mode" specifies how the application window will be shown.

Command line: net stop hostmonservice

Window mode: SW_SHOWNORMAL

Action name

The name of the action; WatchDog auto populates this field with a suggested name based on the type of action; you can change that name to whatever name you want.

Condition to start action

Start when HostMonitor does not respond for N min

This parameter tells when “bad” action should be executed – when connection to HostMonitor is dropped and reconnect attempts fail for N minutes

Start when HostMonitor does respond for N min

This parameter tells when “good” action should be executed – when connection to HostMonitor is established and it is stable for N minutes (0 means action should be executed when connection just established)

Action depends on "bad" one

This optional parameter is available for "Good" actions only. You can set "Good" action dependable on a "Bad" action. Why do you need it? For example you defined "Bad" action to send an e-mail notification to the network administrator when connection lost for 3 minutes, also you defined «Good» action to send a notification when connection restored and it is stable for 2 minutes. What happens if connection was lost for 1 minute then everything works fine for an hour? WatchDog will not send a notification about failure (because connection restored after 1 minute) but the program will send notification about restoring "Good" status. To avoid unnecessary "Good" action execution you can mark "Action depends on bad one" option and select "Bad" action. In this case WatchDog will start "Good" action only if corresponding "Bad" action was executed.

Action-specific settings:

Visual/Sound alert

This action is designed to play a sound file (WAV, MID, etc). In addition to the common action parameters, the «Visual/Sound alert» action has the following options:

Sound file

Specify full path to the sound file or click small button on the right side and select file from the Open File dialog.

Show WakeUP window and play sound every N sec

With this option enabled WatchDog will display a popup window with information about the event and will play a sound repeatedly until you click "Stop sound" button.
Note: If you start WatchDog on Windows Vista, 2008 or Windows 7 using service mode, WatchDog ignores this option and plays sound file just one time (because you cannot stop sound using GUI).

Execute external program

Name of this action tells for it self, it launches specified external application. In addition to the common action parameters this action has 2 more parameters:

Command line

Specify command line to launch external application. Macro variables may be used in the command line.
E.g. on Windows system you may

- send message to another system in the LAN using command like net send * “%HMSystemAddr% %EventText%”;
- start backup HostMonitor as application: c:\program files\HostMon8\hostmon.exe;
- start backup HostMonitor as service: net start HostMonService;
- start sendmail program to send e-mail message
- and so on.

There is no HostMonitor for Linux so you cannot start backup HostMonitor there, however this action may help in some cases.

Window mode

This option enabled on Windows systems only, it specifies how the application window will be shown.
Choose one of the possible options:

SW_SHOWNORMAL	displays an application window in its original size and position.
SW_HIDE	starts application without displaying its window.
SW_MAXIMIZE	displays an application window as a maximized window.
SW_MINIMIZE	displays an application window as a minimized window.
SW_SHOWMINNOACTIVE	displays an application window as a minimized window. The active window remains active.
SW_SHOWNOACTIVATE	displays an application window in its original size and position. The active window remains active.

Syslog

This action sends data using the Syslog protocol. Syslog is the standard event logging subsystem for Unix, also you can install some Syslog service for Windows. Syslog daemon receives standard UDP Syslog messages sent from routers, switches, UNIX hosts, HostMonitor, other network devices and can display the details on screen, log to files, terminal devices, etc. Syslog also allows you to forward log entries to another machine for processing, in this way syslog functions as a distributed error manager
In addition to the common action parameters, the «Syslog» action has the following parameters:

Server
This is the name or IP address of the Syslog server.

Port
The default Syslog port is 514, but you can specify a non-standard port.

Message
Provide text message to send. Macro variablesare supported in the message to be substituted with their actual values at the action execution time.

Severity
Log messages are prioritized by a combination of facility and urgency level. Levels (severity) can be considered various levels of a problem (e.g. warning, error, emergency) whereas facilities are considered to be service areas (e.g. printing, email, network, etc). The levels available are the following:

-	Emergency	A panic condition. System is unusable.
-	Alert	A condition that should be corrected immediately, such as a corrupted system database.
-	Critical	Critical conditions, e.g., hard device errors.
-	Error	Errors.
-	Warning	Warning messages.
-	Notice	Conditions that are not error conditions, but should possibly be handled specially.
-	Info	Informational messages.
-	Debug	Messages that contain information normally of use only when debugging a program.

Facility
Facility is a number that considered as a service area. The various facilities are listed below:

0	kernel messages
1	user-level messages (messages generated by random user processes)
2	mail system
3	system daemons
4	security/authorization messages
5	messages generated internally by syslogd
6	line printer subsystem
7	network news subsystem
8	UUCP subsystem

9	clock daemon
10	security/authorization messages
11	FTP daemon
12	NTP subsystem
13	log audit
14	log alert
15	clock daemon
16-23	reserved for local use

SNMP Trap

This action sends a message to the management station using the SNMP protocol. The SNMP (Simple Network Management Protocol) is the Internet standard protocol for exchanging management information between management console applications and managed entities (hosts, routers, bridges, hubs, etc).

In addition to the common action parameters, the «SNMP Trap» action has the following parameters:

Destination address

Here you should provide the host name (e. g. mail.maincorp.com) or IP address (e. g. 204.71.200.68) of the host that will receive SNMP Trap messages. This machine should be running a SNMP console in order to receive the trap message. You can use macro variables in this field.

Also you may specify non-standard UDP port. Port number can be provided after a colon following the destination address (e.g. 195.168.10.10**:1162**).

Agent address

Provide IP address of the agent that generated the SNMP Trap. If you keep default value “localhost”, WatchDog will use IP address of the system where it is running.

Community

Specify the SNMP community name used for this trap. The default community for most systems is "public". The community string must match the community string used by the SNMP console.

Enterprise

This field identifies the type of the object causing the trap.

Trap type

Choose one of the generic trap types:

- Cold Start
- Warm Start
- Link Down
- Link Up
- Authentication Failure
- EGP Neighbor Loss
- Enterprise Specific

Specific

If Trap type is Enterprise Specific, provide an ID of the trap.

MIB OID
SNMP Trap message can include OID relevant to the message and its value. Define object identifier in this field (object identifier is the name that uniquely identifies the object, e.g. OID "1.3.6.1.2.1.2.1" represents the number of network interfaces on which system can send/receive IP datagrams).

MIB Value
Define an object’s value. You can use macro variables in this field as well.

MIB Type
Choose type of the data. It can be one of the following:

- NULL
- INTEGER
- OCTET STRING
- OBJECT IDENTIFIER
- IP ADDRESS
- UNSIGNED32
- COUNTER
- GAUGE32
- TIMETICKS
- OPAQUE
- COUNTER64

Macros

While defining some of the alert action's parameters you can use special macro variables:

%HMVersionText%	Version of HostMonitor, like HostMonitor v. 10.70
%HMVersionBin%	Binary version, like 0812
%HMSystemName%	Name of the system where HostMonitor is running
%HMSystemAddr%	Host name or IP address of the system where HostMonitor is running (address that was specified as connection parameter)
%HMStartedTime%	Date and time when HostMonitor was started
%HMStatusString%	String that represents status of target HostMonitor, like the following - monitoring started, alerts enabled, modifications stored - monitoring stopped, alerts disabled, modifications not stored If connection to HostMonitor was dropped, this variable returns 'request failed' string
%WDSystemAddr%	IP address of the system where WatchDog is running
%WDSystemName%	Host name of the system where WatchDog is running
%ConnectedAt%	Date and time when connection to HostMonitor was established, can be used for “good” actions

%ConnectedTime%	Time when connection to HostMonitor was established, can be used for “good” actions
%DisconnectedAt%	Date and time when connection was lost, can be used for “bad” actions
%DisconnectedTime%	Time when connection was lost, can be used for “bad” actions
%EventText%	Returns 'Connection established' string for “good” actions and ‘Connection lost’ for “bad” actions

The following table illustrates where you can use macro variables:

Action	**Macros applicable**	**Action parameters where macros are applicable**
Visual/sound alert	No	
Execute external program	Yes	Command line
Syslog	Yes	Message
SNMP Trap	Yes	Destination address MIB value