

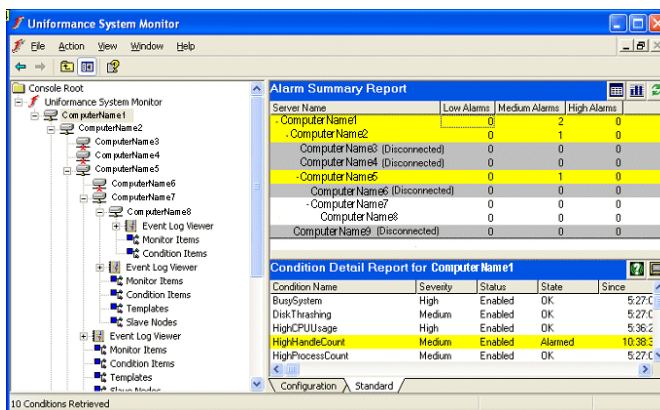
Uniformance System Monitor



Automating PHD Monitoring

Uniformance® System Monitor (USM) automates many of the repetitive tasks commonly performed by a Uniformance PHD system administrator to evaluate the health of the system and to take appropriate actions. Such personnel spend time every day determining if all system components are working as expected, and if data is flowing from system to system correctly, often repeating these tasks for many PHD servers. When such tasks are automated, human resources may be applied to other, more valuable tasks.

Uniformance System Monitor ensures the right actions are taken to bring the PHD system back to a desirable operating state. Support personnel can be notified when an error condition is detected and can be optionally notified when the situation has been corrected. Additionally, Uniformance System Monitor provides graphical and report-style methods of examining the entire system status at any time on a per node or summary basis.



Viewing the status of several monitored systems.

Preventing System Failures

In many cases, USM can detect conditions that may cause a PHD outage and deal with them before there is a problem that may result in data loss.

- USM may be configured to identify when the system is running low on disk space, and clean up log files and temporary files.
- USM can easily be set up to notify system administrators in the case of high CPU use so the problem can be investigated and corrected before key processes stop working.
- USM can create notifications when one of a pair of dual collectors is down, so that one server can be fixed while the other is still running.

One-Stop Monitoring of Many Servers

It is very common for PHD users to leverage PHD's distributed architecture, potentially having data collection, shadowing (data consolidation) servers, applications and databases running on separate physical nodes. USM provides configuration and monitoring of this complete environment from a single interface.

Quick and Easy Startup

USM startup is easy using monitoring templates shipped with the system. These templates start the user with a base set of monitor items and conditions for PHD and the various Windows operating systems. Simply apply the template and enable the monitor items and conditions to begin monitoring your system.

As users develop their own standards for what should be monitored, existing templates may be modified or new templates may be built so these new standards may easily be applied across several monitored systems.

Monitoring PHD and the IT Environment

Uniformance System Monitor comes with a comprehensive list of monitored items, including PHD-specific monitoring, Windows and network monitoring, and complex logic for combining monitor items and calculations.

Monitored items available include:

- Tag Value, Timestamp, Confidence, Status – ability to monitor the health of tags
- Performance Value – ability to monitor any value available through Windows PERFMON
- System Time – check for time drifts between various systems and tag data
- Working Variable – manipulate internal values for advanced logic
- PHD Server Command – monitor any value available through PHDMAN
- RDI Server Command – monitor any value available through RDI Server
- Log File Size – monitor file sizes
- WMI Value – provides access to the Windows Management Interface
- Ping Machine – check to see if key machines are reachable on the network
- SNMP Value - Simple Network Management Protocol connection to a specific device, such as routers, switches and UNIX hosts
- Lookup Value – store constants for use in a variety of conditions
- Condition Item – indicates whether an item is in alert status
- Slave Node – indicates whether a slave node is connected

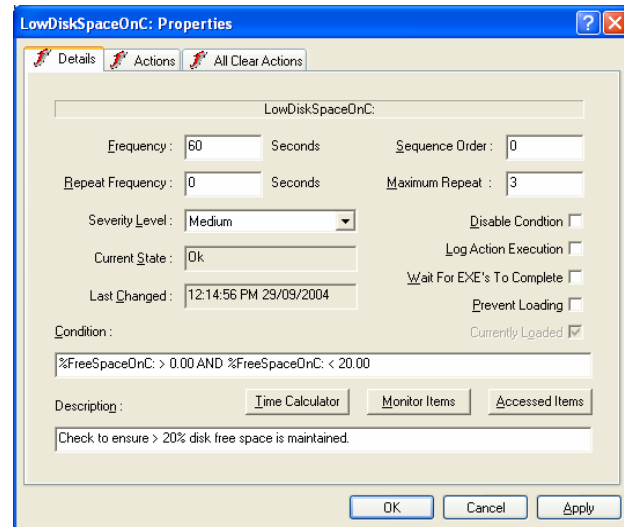
Honeywell services are available to develop interfaces for monitoring additional applications and systems.

Taking Action on Conditions

A variety of actions may be configured to occur when a USM condition is triggered. These actions are configured on a per condition basis, ensuring that the appropriate actions will be taken for any particular alert.

The following actions may be associated with any USM condition:

- Display an alert on the USM status screen (always enabled)
- Send a network broadcast message (net send)
- Send an email to individuals or a mailing list
- Execute one or more commands
- Log a message in the Windows Event Log
- Perform calculations against working variables



Configuring a condition for monitoring

Taking the Right Actions for the Situation

USM provides the ability to perform monitoring beyond the basic detection and notification capabilities available in other solutions. Different conditions have different priorities and different parts of an IT environment may be managed by different personnel. USM provides a highly configurable environment that allows the system administrator to set up the right responses and notifications for each condition.

USM allows for configuration of advanced logic involving multiple monitored items and manipulation of internal variables. These advanced features can be used to:

- Determine if a condition has been true too long and notify backup support personnel.
- Calculate the age of manual input values and notify the data owners that an update is needed.
- Identify that a key RDI is down and automatically restart it. If the RDI still does not start, notify the PHD administrator.
- Applications support about PHD alerts and notify IT of hardware and network failures.

“All Clear” actions also allow appropriate actions and notification to occur when a condition becomes inactive. This capability may be used to notify support personnel that the problem has been resolved and a trip to the site is not necessary.

Secure and Firewall-Friendly

USM has been written with security and firewall rule compliance as a key capability. USM only requires a single user-selectable port to be opened in a firewall between PHD servers. Additionally, the user may select the preferred master-to-slave or slave-to-master communications initiation.

Many security policies will not allow emails or other alerts to be sent from the secure side of the process control firewall. USM allows users to route such actions to the master node so that actions are securely performed from the master node.

Technical Prerequisites

USM is capable of monitoring PHD details for:

- PHD release 201.1.5
- PHD release 201.1.6 and later (requires USM release 101)
- PHD release 202
- PHD releases 210 & 215 (requires USM release 101)

USM should not be installed on systems running PHD 200 or 201 prior to 201.1.5.

USM is able to monitor Windows performance for:

- Windows NT
- Windows 2000
- Windows XP
- Windows 2003

More Information

For more information on Uniformance, visit www.honeywell.com/ps or contact your Honeywell account manager.

Automation & Control Solutions

Process Solutions

Honeywell

2500 W. Union Hills Dr.

Phoenix, AZ 85027

Tel: +1-602-313-6665 or 877-466-3993

www.honeywell.com/ps