

Ready for

IBM. | **Tivoli.**

software



*Blue Medora ITM Agent for
Files and Directories
(Updated for version 6.21.02)*

Jason Pliml
jason.pliml@bluemedora.com
+1.616.504.1725

November 1, 2010



*Products sold only under
IBM License Agreements

Tivoli Certified ITM Agents

IBM® Tivoli® Directory Server ITM agent

Symantec® Endpoint Protection ITM agent

Files and Directories ITM agent

Ping Probe ITM agent

Remote SSL Certificates ITM agent

Amazon® Elastic Computer Cloud (EC2) ITM agent

Amazon® Simple Storage Service (S3) ITM agent

Citrix® XenServer™ ITM agent (≈ Q4/10)

Google® App Engine ITM agent (≈ Q1/11)

Tivoli Certified TCR Reporting Packages

IBM® Tivoli® Directory Server (ITDS) Reporting

Ping Probe Reporting

Remote SSL Certificates Reporting

Certified ITM Agents

ITCAM for Applications:

PeopleSoft® Enterprise 6.2.2

ITCAM for Applications:

Siebel® CRM 6.2.4

Certified TCR Reporting Packages

ITCAM for Applications:

PeopleSoft® Reporting Package

Ready for

IBM | **Tivoli.**

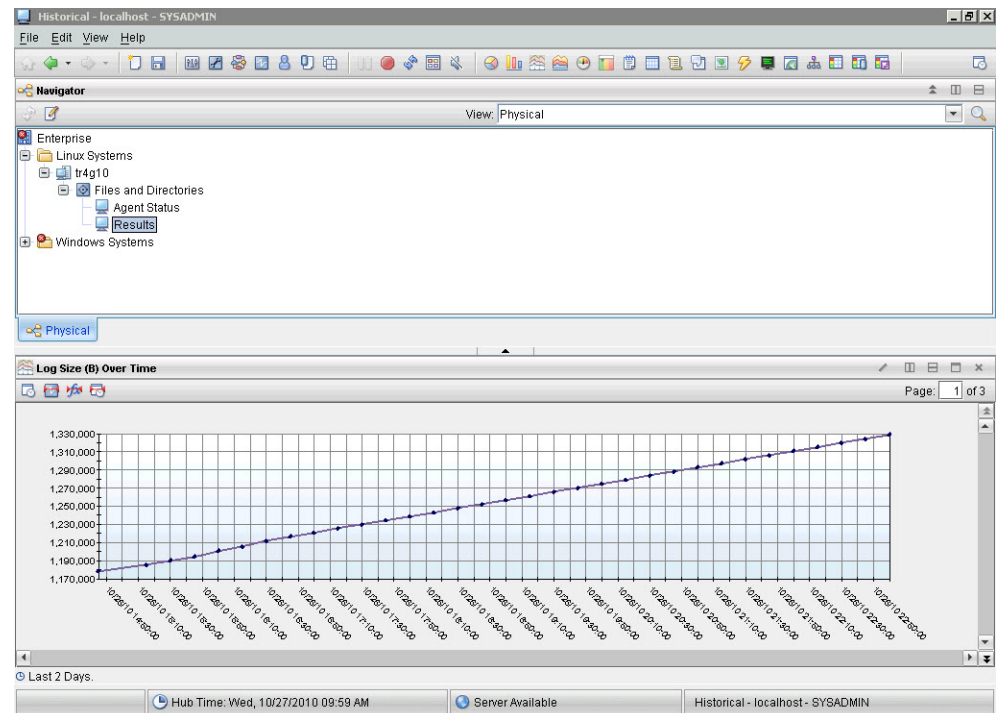
software

- Extends IBM® Tivoli® Monitoring (ITM) by adding in-depth monitoring of files and directories
- Inspect only the files and directories you want with optional directory recursion and regular expressions
- User configurable option to enable computation of MD5 checksums for individual monitored files *(New in v6.21.02)*
- Two new attributes in ‘Results’ attribute group that provide MD5 related details *(New in v6.21.02)*
- New Situation that can initiate an alert when the MD5 checksum of a file changes *(New in v6.21.02)*
- Two new attributes in ‘Results’ attribute group provide timestamp information for the newest files in a regex-based fileset definition
- IBM Certified
 - Ready for IBM® Tivoli®



The Files and Directories Agent for ITM helps answer:

- Which files have been modified recently in a specific directory?
- What is the cumulative size of all files in a directory and its subdirectories that match a regular expression?
- While log files have exceeded a size threshold?
- How many new files are in a set of directories?
- Which log files have changed?
- How has a file changed over time?
example: file size trend >>



Innovative uses of the Blue Medora ITM agent for Files and Directories:

- System Security – monitoring password, group, and network configuration files can quickly alert a system admin to a potentially compromised system
- Backup Verification – was a new backup created? Was the backup file at least #Gb in size? Was it successfully transferred to a remote device?
- Resource Allocation – have we reached a threshold for used disk space? Is the paging / swap file growing regularly indicating memory constraint?
- Implement Payment Card Industry Data Security Standard (PCI DSS)
https://www.pcisecuritystandards.org/security_standards/index.php
 - ❖ From PCI DSS requirements (11.5): “Deploy file-integrity monitoring software to alert personnel to unauthorized modification of critical system files, configuration files, or content files; and configure the software to perform critical file comparisons at least weekly.”

Detailed instructions for implementing these uses and more at: <http://bluemedora.com/blog/?p=752>

Files and Directories Attributes *(updated for v6.21.02)*



Attribute	Sample Value	Description
Alias	ITM Logs	Alternate name for files or directories being monitored
Path	/opt/IBM/ITM/logs	Absolute path to file or directory being monitored
Include Subdirectories	Yes	Indicates whether subdirectories are included with a directory
Regular expression	^.*\.log\$	Regular expression matches filenames within a directory
Path Exists	yes	Indicates whether file or directory path was found
File Count	59	Number of files matching the monitoring criteria
File Count Delta	3	Change in number of files matching the monitoring criteria from prior collection interval
File Count % Change	0	Percentage change in number of files matching monitoring criteria
File Count Rate of Change	3	Rate of change (per second) in number of files matching the monitoring criteria
Size in Bytes	522661	Size in bytes of all files matching the monitoring criteria
Size Delta in Bytes	1926	Change in size (in bytes) of all files matching the monitoring criteria
Size % Change in Bytes	0	The percentage of change in the size in bytes of all the files that match the monitoring criteria
Size Rate of Change in bytes	7	The rate of change per second of the size in bytes of all the files that match the monitoring criteria
Path Modified Datetime	10/26/10 13:41:17	The most recent time that a file that matches the monitoring criteria was modified
Initial File Count	59	The number of files that matched the monitoring criteria during the first collection interval
Initial Size in Bytes	522661	The size in bytes of all the files that matched the monitoring criteria during the first collection interval
Initial Sample Time	10/26/10 13:41:17	The date and time of the initial data collection interval
Agent Uptime In Seconds	2170	Time agent data provider has been running (in seconds)

Attribute	Sample Value	Description
Size in KB	510.4	Size in kilobytes of all files matching monitoring criteria
Size in MB	0.50	Size in megabytes of all files matching monitoring criteria
Size in GB	1.21	Size in gigabytes of all files matching monitoring criteria
File Count Delta Since Start	24	Number of files that match the monitoring criteria that have changed since the first collection interval
File Count % Change Since Start	6	Percentage of change in number of files that match the monitoring criteria since the first data gathering interval
First Count Rate of Change Since Start files/sec	2	The rate of change per second in the number of files that match the monitoring criteria since the first data gathering interval
Size Delta Since Start	65498	The difference in size of the directive matching the monitoring criteria since the first data collection interval
Size % Change Since Start	6	Percent growth on monitoring criteria since first collection interval
Size Rate of Change Since Start bytes/sec	9	The percentage of growth of the monitoring criteria since the agent's first collection interval
Regular Expression Modified Datetime	10/26/10 15:48:04	The date/time of the file most recently modified that matches the monitoring criteria
MD5 Checksum <i>(new)</i>	c471c6161ab4f566b11b57cb2bcdefcc	MD5 checksum value of the file
MD5 Changed <i>(new)</i>	True	Indicates whether MD5 checksum of file has changed since last data collection
Oldest Modified Datetime <i>(new)</i>	10/26/10 13:41:07	Modification date of the oldest file in a directory OR the oldest modification date of a file
Oldest Regular Expression Modified Datetime <i>(new)</i>	10/26/10 15:48:04	Modification date of the oldest file in a directory that matches the monitoring criteria OR the oldest modification date of a file

Consistency With Existing ITM Infrastructure



ITM Agent for Files and Directories **has been designed from the ground up to look, feel, and operate like IBM®-developed ITM agents** in terms of remote deployment, manageability via ITM command-line utilities, installation and configuration

The screenshot shows the 'Files and Directories' management console. The left pane displays a tree view of the system hierarchy, including 'Enterprise', 'Linux Systems', 'UNIX Systems', 'Windows Systems', and 'AW3G2'. The right pane displays a table of files and directories.

Node	Alias	Type	Path Exists	File Count	Size in bytes	Modified Datetime
two:AW3G2:P7	fdm agent two log	File	yes	1	20774	09/08/09 15:43:44
two:AW3G2:P7	Documents and Settings	Directory	yes	0	0	03/11/09 10:32:53
one:AW3G2:P7	ITM Logs	Directory	yes	56	793829	09/08/09 15:44:10
one:AW3G2:P7	fdm agent one log	File	yes	1	106006	09/08/09 15:43:46
one:AW3G2:P7	PS Domain AW3G21 Logs	Directory	yes	10	69537	03/15/09 22:29:23
one:AW3G2:P7	PS Scheduler Logs	Directory	yes	6	43376	03/15/09 22:42:52
one:AW3G2:P7	TEMP	Directory	yes	0	0	09/08/09 15:40:07
one:AW3G2:P7	Files and Directories agent trace log	Directory	yes	2	127196	09/08/09 15:44:10

1st Class Citizens of the Tivoli Monitoring Ecosystem



ITM Agent for Files and Directories operates as **first-class citizens of the ITM ecosystem**

File and Directories agent **leverages ITM's Tivoli® Enterprise Portal (TEP) visualization capabilities** to include expert advice, customized workspaces, and historical data gathering

The screenshot shows the 'File and Directories - Results - localhost - SYSADMIN' window. The 'Navigator' pane on the left shows a tree structure: Enterprise > Linux Systems > tr4g10 > Files and Directories > Agent Status > Results. The main area displays a table of results for the 'Physical' view.

	MD5 Checksum	MD5 Changed	Path Modified Datetime	Oldest Modified Datetime	Regular Expression Modified Datetime	Oldest Regular Expression Modified Datetime	Initial Sample Time	Agent Uptime In Seconds
	c471c6161ab4f566b11b57cb2bcdefcc	False	10/26/10 11:22:23	10/26/10 11:22:23			10/26/10 11:22:23	2170
	N/A	False	10/26/10 13:41:07	10/26/10 13:41:07	10/26/10 14:17:18	10/26/10 14:17:18	10/26/10 13:41:07	2170
	N/A	False	10/26/10 10:24:25	10/26/10 10:24:25	10/26/10 14:07:50	10/26/10 14:07:50	10/26/10 10:24:25	2170

At the bottom of the window, there are status indicators: 'Hub Time: Tue, 10/26/2010 02:17 PM', 'Server Available', and the window title 'File and Directories - Results - localhost - SYSADMIN'.

Go beyond Monitoring and **Manage** your environment



Manage and automate your environment with comprehensive Take-Actions built into Blue Medora agents

The screenshot displays the Blue Medora management console interface. The main window is titled "KP7_Size_High - localhost - SYSADMIN". It features a "Navigator" on the left showing a tree view of the environment, with "KP7_Size_High" selected under "Results". The main area is divided into two panes: "Initial Situation Values" and "Current Situation Values". Both panes show a table with the following data:

Size in bytes	Node	Timestamp	Line Number	Alias	Type	Path	Include Subdirect
1181601792	rhelFiles.fdm-rhel5:P7	08/20/09 11:31:38	3	Two-Digit	Directory	/root/myDir	Yes

Below the tables is a "Command View" panel titled "Take Action". It includes a "Name" dropdown menu (currently showing "<Select Action>"), a "Command" text box, and a "Run" button. The "Destination Systems" section is currently empty. To the right is an "Expert Advice" panel for the "KP7_Size_High" situation. It provides a "Situation Description" (Size High) and "Suggested Actions" (The size in bytes of a file or directory is high. Use this example situation to determine whether the combined size in bytes of a file or directory has crossed a threshold setting.). The interface also shows a status bar at the bottom with "Hub Time: Thu, 08/20/2009 01:27 PM", "Server Available", and the current window title "KP7_Size_High - localhost - SYSADMIN".



- **Blue Medora Sales Contact**

- Jason Pliml
 - Blue Medora Email: sales@bluemedora.com
 - Phone: +1.616.504.1725

- **Online Resources**

- Product Page >> <http://bluemedora.com/product/page/21>
- Product Demo >> http://bluemedora.com/flash_demos/FDM/
- Blue Medora Blog >> <http://blog.bluemedora.com> (search “Files and Directories”)
- Documentation >> <http://bluemedora.com/page/48>
- Evaluation Download >> <http://bluemedora.com/evaluation>

Backup

Who is Blue Medora?



- Largest Independent Software Vendor (ISV) focused exclusively on developing extensions for the Tivoli® SAPM product portfolio
- Focused on integrating emerging technologies with IBM® Tivoli® Service Availability and Performance Management (SAPM) product portfolio
 - Cloud Monitoring
 - Virtualization / VDI
 - Fine grained security technologies and applications
- Trusted IBM® Partner: IBM® partners with Blue Medora for complex ITM / ITCAM monitoring solutions via OEM licensing of Blue Medora's Siebel® and PeopleSoft® monitoring solutions
- 13 new IBM® 'Ready for Tivoli®' Certified Solutions in past 18 months

- **IBM Tivoli Monitoring (ITM)**
 - ITM 6.2.0 FP3 +
 - ITM 6.2.1 FP2 +
 - ITM 6.2.2 +
- **Operating systems**
 - Windows 2003 and 2008 (32 and 64-bit)
 - Red Hat Enterprise Linux 4 and 5 on Intel (32 and 64-bit)
 - Red Hat Enterprise Linux 4 and 5 on Power (64-bit)
 - Red Hat Enterprise Linux 4 and 5 on IBM zSeries (32 and 64-bit)
 - Suse Linux Enterprise Server (SLES) 10 and 11 on Intel (32 and 64-bit)
 - Suse Linux Enterprise Server (SLES) 10 and 11 on Power (64-bit)
 - Suse Linux Enterprise Server (SLES) 10 and 11 on IBM zSeries (32 and 64-bit)
 - AIX 5.3 and 6.1
 - Solaris 9 and 10 (Sparc)
 - HP-UX IA64