EventTracker
Secure. Comply. Succeed.

Agent health check enhancements

Detailed Document

Publication Date: Jul. 25, 2016

EventTracker
8815 Centre Park Drive
Columbia MD 21045
www.eventtracker.com

Abstract

This document is to guide the user about the EventTracker Agent Updates **ET82UA16-012** and its functionalities.

Target Audience

EventTracker users, Support Team.

How the EventTracker Agent update works?

The update includes few Agent Health Check Enhancements. Once the user applies the EventTracker Agent update **ET82UA16-012**, a new service named '**EventTracker Monitoring Daemon**" gets added. It monitors the EventTracker agent activities including Memory, Handles, CPU Time, Registry Bookmark and Counter Check (evtViewerLog.etw).

The EventTracker Agent update will perform the below mentioned functions:

1. The watch dog service (**EventTracker Monitoring Daemon**) will be created on target agent and manager system to monitor the EventTracker Agent service.

2. If EventTracker agent service is down, then the daemon service will start the agent service and send a trap to reporting manger.

3. If the Agent Memory is consuming more than 1GB then the daemon service will restart the agent service and send a trap to reporting manger.

4. If the Agent CPU time is more than 6 Hour then the daemon service will restart the agent service and send a trap to reporting manger.

5. If the agent handle count crossed more than 10,000 then the daemon service will restart the agent service and send a trap to reporting manger.

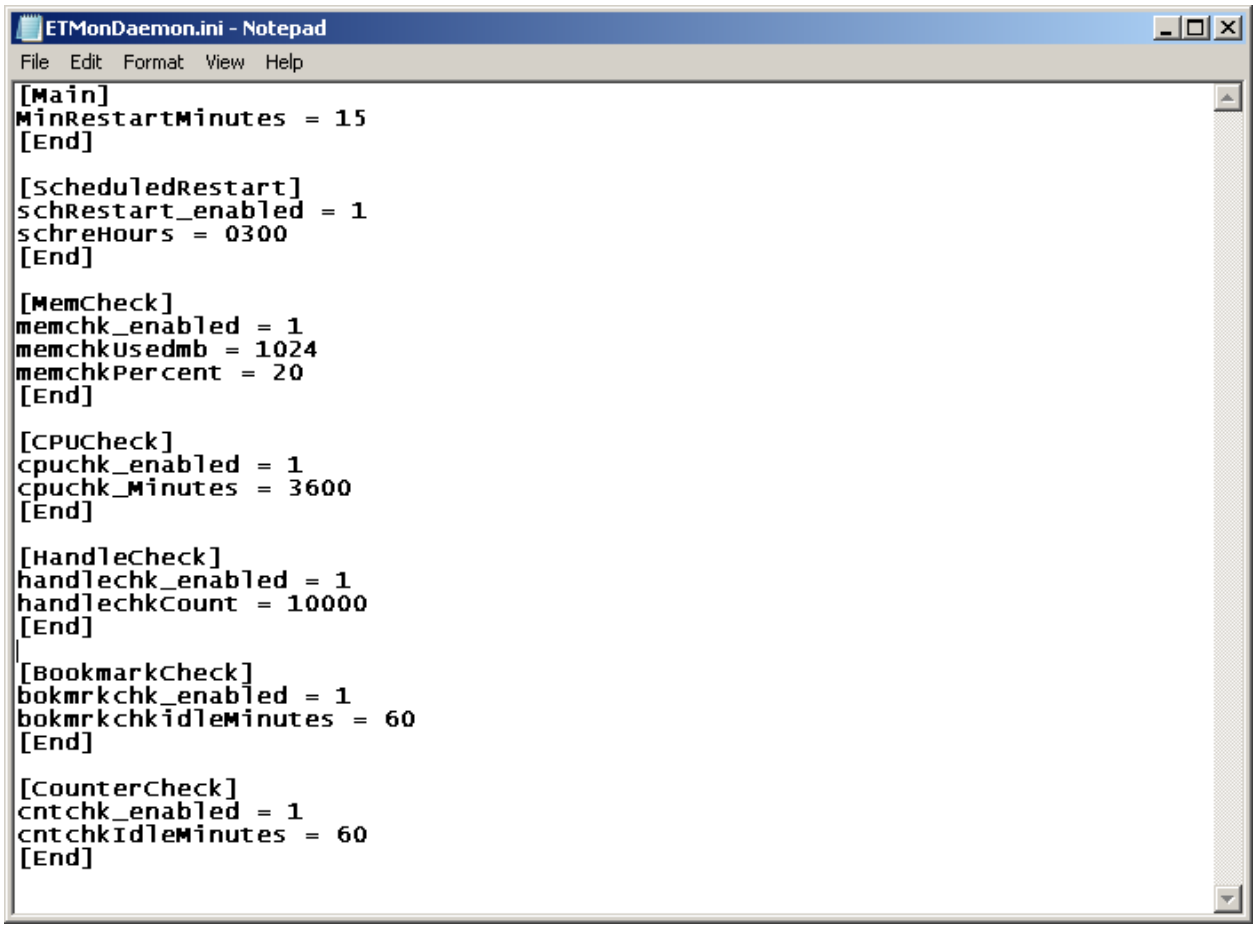
6. If the Registry (Bookmark) is not updated for 1 hour, then the daemon service will restart the agent service and send a trap to reporting manger.

7. If the ETW file (evtViewerLog.etw) is not updated for 1 hour, then the daemon service will restart the agent service and send a trap to reporting manger.

8. Schedule restart of agent service by 3:00 AM every day.

9. The trap will contain information like system name and OS type.

10. The threshold values are hardcoded. If the user wants to change the threshold values then the user should provide a custom ETMonDaemon.ini in \\install directory\Prism Microsystems\EventTracker\Agent folder, which holds the threshold values as shown below:



Audit Trail event

- Event ID 3520 will be generated when the agent is started or restarted successfully, with Event Type as Information. The same event id will be generated when the default threshold is crossed by the agent.

Sample Description:

Sample 1:

Event Type: Information
Log Type: Application
Category Id: 2
Description:
EventTracker Monitoring Daemon:
System Name: R1S4-VM1
Operating System Type: Windows 7
EventTracker Agent service started successfully.

Sample 2:

Event Type: Information
Log Type: Application
Category Id: 2
Description:
EventTracker Monitoring Daemon:
System Name: R1S4-VM1
Operating System Type: Windows 7
CounterCheck is not updated from last 60 min, restarted the agent service.

- When the agent fails to start or restart agent service, then it generates the event id 3520, with Event Type as: Error.

Sample Description:

Sample 1:

Event Type: Error
Log Type: Application
Category Id: 2
Description:
EventTracker Monitoring Daemon:
System Name: R1S3VM1
Operating System Type: Windows Server 2008 R2
Handle threshold crossed the limit of (1200), stopping the agent service failed.