

Tuning Assessment Tool

SmartConnector™ for Microsoft Windows Event Log – Unified

BETA Version

July 5, 2012



Tuning Assessment Tool for SmartConnector for Microsoft Windows Event Log – Unified

BETA Version

July 5, 2012

Copyright © 2012 Hewlett-Packard Development Company, L.P.

Confidential computer software. Valid license from HP required for possession, use or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

The information contained herein is subject to change without notice. The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

Follow this link to see a complete statement of copyrights and acknowledgements: <http://www.arcsight.com/copyrightnotice>

The network information used in the examples in this document (including IP addresses and hostnames) is for illustration purposes only.

This document is confidential.

Revision History

Date	Description
07/05/2012	First edition of this document.

Contents

Tuning Assessment Tool4

 Connector Parameter Enhancements..... 4

 Invoke the Tuning Tool 5

 Sample Tuning Report..... 6

 Notes 7

Tuning Assessment Tool

The Tuning Assessment Tool for the SmartConnector for Microsoft Windows Event Log – Unified is an offline tool provided to help collect some important statistics, such as round-trip-time for each host to be monitored and expected EPS needed, to recommend a range of parameter values. Connector users can use this range as a guideline for a configuration that works optimally for their network conditions.

As the recommendations made by this tool are based upon a snapshot of data and conditions of the network at a given point in time, this requires the network to be stable. If any network conditions change, the guidelines given by the tool may no longer apply. The tool should be rerun for more accurate results.

The tool alleviates the need for manual profiling of hosts and helps make better use of network bandwidth. Other issues, such as log rotation and time drifts, could be caused by a combination of factors. Some of these are network latency, non-optimized deployment choices such as grouping of hosts with very different EPS and CPU usage on the target server (which may contribute to slow responses), sizing of the connector in terms of number of hosts configured per connector, and so on.

With the Tuning Assessment Tool, optimal values of parameters derived from the tool in combination with the correct grouping and sizing of the connector can help alleviate these issues.

Connector Parameter Enhancements

The **eventpollcount** parameter has been added for setting an event poll count for each host and log type for security, system, and application event log types. For example: `security.eventpollcount=50`. The default value is 50.

If the log type does not have this parameter specified (for example, in legacy agent.properties files), each event poll count will take a value from the base host **eventpollcount** parameter. If custom log type names are specified, add eventpollcount to a name separated by a colon (:); for example
`agents[0].windowshoststable[1].eventlogtypes=custom1:10,custom2:50`

The host eventbuffer size parameter works in conjunction with the **eventpollcount** parameter. The recommended and default value is 512. (The buffer size requested from Microsoft's event log through the JCIFS API is the event buffer size multiplied by the specific event log event poll count.)

Sample Table Parameters Section of agent.properties

The following sample shows **eventpollcount** and **eventbuffer size** parameters for multiple Windows hosts.

```
agents[0].windowshoststable[0].system=true
agents[0].windowshoststable[0].system.eventpollcount=50
agents[0].windowshoststable[0].username=administrator
agents[0].windowshoststable[0].windowsversion=Windows Server 2008 R2
agents[0].windowshoststable[1].Domain\ Name=
agents[0].windowshoststable[1].application=false
agents[0].windowshoststable[1].application.eventpollcount=50
agents[0].windowshoststable[1].eventbuffer size=512
agents[0].windowshoststable[1].eventlogtypes=
agents[0].windowshoststable[1].eventpollcount=50
agents[0].windowshoststable[1].hostname=10.3.4.3
agents[0].windowshoststable[1].locale=en_US
agents[0].windowshoststable[1].password=OBFUSCATE.4.8.1\6TGf8Ptx3cjBLTkNgN6TGQ\=\=
agents[0].windowshoststable[1].readmode=seek
agents[0].windowshoststable[1].security=true
agents[0].windowshoststable[1].security.eventpollcount=50
agents[0].windowshoststable[1].startatend=true
agents[0].windowshoststable[1].system=true
agents[0].windowshoststable[1].system.eventpollcount=50
agents[0].windowshoststable[1].username=administrator
agents[0].windowshoststable[1].windowsversion=Windows Server 2008 R2
agents[0].windowshoststable[2].Domain\ Name=
agents[0].windowshoststable[2].application=true
```

```

agents[0].windowshoststable[2].application.eventpollcount=50
agents[0].windowshoststable[2].eventbuffersize=512
agents[0].windowshoststable[2].eventlogtypes=
agents[0].windowshoststable[2].eventpollcount=50
agents[0].windowshoststable[2].hostname=10.3.4.4
agents[0].windowshoststable[2].locale=en_US
agents[0].windowshoststable[2].password=OBFUSCATE.4.8.1\6TGf8Ptx3cjBLTkNgN6TGQ\=
agents[0].windowshoststable[2].readmode=seek
agents[0].windowshoststable[2].security=true
agents[0].windowshoststable[2].security.eventpollcount=50
agents[0].windowshoststable[2].startatend=true
agents[0].windowshoststable[2].system=true
agents[0].windowshoststable[2].system.eventpollcount=50
agents[0].windowshoststable[2].username=administrator
agents[0].windowshoststable[2].windowsversion=Windows Server 2008 R2
agents[0].windowshoststable[3].Domain\ Name=

```

Invoke the Tuning Tool

From the command line of a command window, run the following from the \$ARCSIGHT_HOME\current\agent\bin directory:

```
arcsight agent runwuctuningtool [arg1 arg2 ...]
```

Where the arguments can be:

```

-d domain
-s server (host) name or IP address
    (If there are no host names, a filename is expected; if there is a host name, the filename is not processed.)
-u user name
-p password
-l <logTypes>
    List log types to assess for the host; for example: Security System Application Custom_log1
    ([security,system])
-f Input file path
    (parameter for the input file; must be CSV format (*.csv)). CSV file has the following fields for each line:
    domain, host, user, password, logType1:logType2:logType3:logType4... (log types are
    colon separated). Order is important and only host, user, and password,log type are required. If no domain
    is specified, the file must contain a comma preceding the host. For example:
    ,10.3.4.4,administrator,password,security:system:application
-o Output file path
    (for report, formatted as CSV, with headers). If not specified, the report goes to
    $ARCSIGHT_HOME\current\user\agent\WUCRuningReport.csv. If the tool runs long enough to
    pass a few time intervals, the results are added to outputFile, one line per host. Each host report line
    has average events generated per second, OS type fetched (not currently available), and for each log type,
    the round trip time for 1 or 2KB, as well as recommended minimum and maximum interval for
    eventpollcount values.
-t Time interval for collecting samples in minutes
    Samples are collected in the beginning, then after the time interval, and again after time interval, and so on.
    Each time the new average results are calculated and reported, but there are no accumulated values. The
    default time interval is 10 minutes.

```

For each log type and each host the average event generation rate is calculated from the timestamps of the newest and oldest events in a log. The difference is divided by the number of total events and the averages are reported in the report output.csv at each interval (-t).

An example of the command, with arguments:

```
W:\bin>arcsight agent runWUCTuningTool -f C:\development\WUC_tool\test2hosts.csv
```

Sample Tuning Report

```
## time stamp, domain, host, and for each suggested parameters per log type one
log type in one column with all data separated by colon
##
logTypeName:Avg_Round_Trip_Time_for_1KB_Milliseconds:AVG_Events_Generated_Per_Secon
d:MIN_Events_Poll_Count-MAX_Events_Poll_Count:Comment_If_Any

2012-07-02 17:09:15,,10.3.4.2,,system:0:0:0-0:Cannot connect to the
host,security:0:0:0-0:Cannot connect to the host
2012-07-02 17:09:16,,10.3.4.3,,system:180:1:2-4:,security:180:56:40-55:The
connector may still lag despite recommendation
2012-07-02 17:10:40,,10.3.4.4,,application:240:1:2-4:,system:240:1:2-
10:,security:239:1:2-4:Cannot read events from the log
2012-07-02 17:19:51,,10.3.4.2,,system:0:0:0-0:Cannot connect to the
host,security:0:0:0-0:Cannot connect to the host
2012-07-02 17:19:52,,10.3.4.3,,system:180:1:2-10:,security:179:56:40-55:The
connector may still lag despite recommendation
2012-07-02 17:21:17,,10.3.4.4,,application:239:1:2-8:,system:240:1:2-
4:,security:240:56:40-50:The connector may still lag despite recommendation
```

The following information provides recommendations for error messages you may encounter, such as those shown in the Sample Tuning Report.:

Avg_Round_Trip_Time

The connector ideally should have an average round trip time of 120 ms or less in order to minimize event log collection impact. Increased RTT can have an adverse affect on the event collection speed.

The connector may still lag despite recommendation

The test completed, the recommended settings provided may not prevent the connector from lagging in the event collection process. If the event log issues still exist after using the recommended settings, it might be necessary to move the connector closer to the Windows server to resolve the latency issues or isolate the target Windows host. If the RTT value is greater than 230 ms, the connector may not be able to keep up with the log event generation rate. Correct the network latency issues or offload event log generation on the target Windows host, and rerun the test.

Cannot connect to the host

Test was unable to be run due to target system event logs not being accessible, log collection severely impacted. Work with system administrator to correct the accessibility to the target Windows host's event logs.

Cannot read events from the log

Cannot identify the exact reason for inability to read the logs. The connector's log may provide more data regarding the issue. If you see this error for all log types for the host for more than two time intervals, it may help to restart the assessment tool.

Notes

- The connector does not navigate the event log after it has been manually cleared out while the connector is running. The solution is to shut down the connector, clear persistent files, and restart the connector after the log is cleared.
- Passwords for the Tuning Assessment Tool must be clear text in a .csv file. This will be addressed in a future release.
- Any connector that is collecting events over a network is directly impacted by the health of the network conditions, in terms of speed, latency, bandwidth, geographical location of dispersed network nodes, and so on. For example, the network's performance directly affects the Windows Unified connector's event collection performance. Furthermore, Windows events are transient in nature, have very short life spans (especially security events that live only a few seconds), and are not retained on the system indefinitely or for long periods of time, and thus may not provide adequate time for the connector to collect events.