


IBM Tivoli Monitoring V6.3 - Log file agent

Gathering log file agent logs on Windows

© 2014 IBM Corporation



This presentation explains gathering agent log files for Tivoli® Monitoring V6.3

Objectives

When you complete this module, you can perform these tasks:

- Update the log file agent (LFA) variables to increase the tracing on Windows® systems
- Collect the LFA agent logs for troubleshooting

When you complete this module, you can perform these tasks:

Update the log file agent (LFA) variables to increase the tracing on Windows systems;
Collect the LFA agent logs for troubleshooting.

Increasing trace level

- From the Windows Start menu, click
Program Files >
IBM Tivoli Monitoring >
Manage Tivoli Monitoring Service

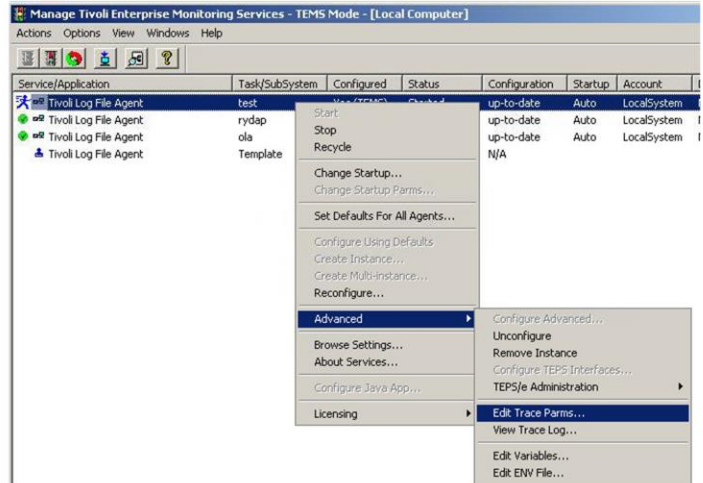


If you want to increase the trace level for an agent that is installed in a Windows box, you can use the Manage Tivoli Enterprise Monitoring Services window.

To start it, from Windows Start menu, click Program Files > IBM Monitoring > Manage Tivoli Monitoring Service.

Editing the variables

- In the listing, right-click the agent
- Click **Advanced > Edit Variables**
- If the agent is running, accept the prompt to stop the agent



From the Manage Enterprise Monitoring Services, you can set the environment variables for a specific agent. In particular, right-click the agent that you want to update, then in the menu, click **Advanced > Edit Variables**.

If the agent is running, accept the prompt to stop the agent.

Notice that a stop and start of the agent is required for the new environment variables to take effect.

Trace Parameters window

- In the Trace Parameters window, modify the trace settings
- Useful RAS1 settings:
 - (UNIT:LFAConfig ALL) turns on tracing showing the initial parsing of the fmt file and basic agent setup.
 - (UNIT:LogMonitor ALL) turns on tracing that shows when events were passed up from the low-level log code to be processed.
 - (UNIT:EIFemitter ALL) turns on tracing showing when events are being sent through EIF specifically.
 - (UNIT:WinLogQuery ALL) turns on event log tracing on Windows.
 - (UNIT:kumprmfr ALL) (UNIT:kum0regx ALL) turns on voluminous low-level tracing on the determination of records in the monitored logs and the comparison of the records against the configured regular expressions.
 - (UNIT:kumpcpu STATE METRIC) turns on tracing of CPU throttling.
 - (UNIT:kumpdcm ALL) turns on tracing of regular expression file name matching.
 - (UNIT:kumpstor STATE) turns on tracing of memory allocations and frees. Useful for a suspected storage leak; can also provide a good idea of general flow.
 - (UNIT:kum STATE) now provides a good overview of behavior in the log library, which is a lot less verbose than ALL.

In the right-click menu that is described in the previous slide, you have also the option to set a specific trace level.

You can refer to the list in this slide to define the proper trace level that is based on the error you are seeing.

Increasing trace level in agent configuration files

- Modify KBB_RAS1 variable in the file "KLOENV_<instance>" under <ITM_home>\TMAITM6 directory with useful RAS1 settings.

You can also change the trace level from the configuration files directly. You have to modify the KBB_RAS1 variable in the file "KLOENV_<instance>" under <ITM_home>\TMAITM6 directory.

After that, the agent must be restarted

Agent restart



From the Manage Tivoli Enterprise Monitoring Services, you also have the option to start the log file agent. You can see this menu by right-clicking the agent.

Re-creating the problem and taking a screen capture

The screenshot shows the 'Data Collection Status - BEST - SYSADMIN' application. The 'Data Collection Status' table is as follows:

Node	Timestamp	Query Name	Object Name	Object Type	Object Status	Error Code
testDONALO	11/07/13 15:52:42	LogfileEvents	LogfileEven...	LOG FILE	ACTIVE	NO ERROR
testDONALO	11/07/13 15:52:42	LFAPProfiles	LFAPProfiles	CONFIG DISCOVERY	ACTIVE	NO INSTANCES RETURNED

The 'Thread Pool Status' table is as follows:

Node	Timestamp	Thread Pool Size	Thread Pool Max Size	Thread Pool Active Threads	Thread Pool Avg Active Threads	Thread Pool Min Active Threads	Thread Pool Max Active Threa
testDONALO	11/07/13 15:52:42	5	5	0	1,00	1	1

The 'Monitored File Status' table is as follows:

Node	Timestamp	Table Name	File Name	RegEx Pattern	File Type	File Status	Num Records Matched	Num t
testDONALO	11/07/13 15:52:42	LogfileEvents	c:\test-1.log	c:\test-1.log	REGULAR FILE	OK	0	0
testDONALO	11/07/13 15:52:42	LogfileEvents	\\pipe\WLO_test_LogfileEvents_ev(pgm)	\\pipe\WLO_test_LogfileEvents_ev(pgm)	PIPE	OK	0	0

At the bottom of the interface, it shows 'Hub Time: Cct, 11/07/2013 03:50 PM', 'Server Available', and 'Data Collection Status - BEST - SYSADMIN'.

8

Gathering log file agent logs on Windows

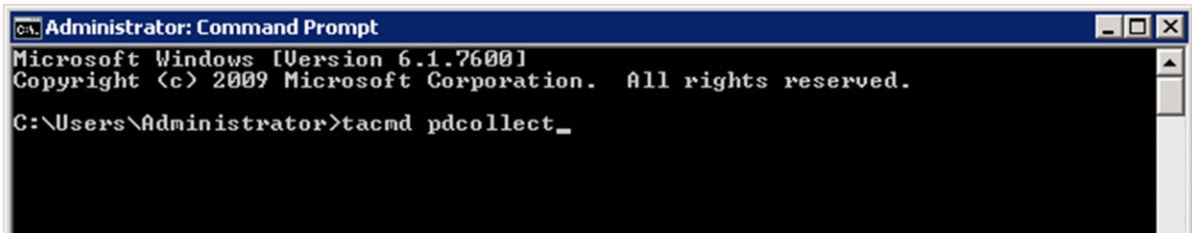
© 2014 IBM Corporation

Next, re-create the problem.

Take a screen capture of the issue and then immediately stop the agent.

Log collection (1 of 3)

- After the problem recurs, collect log files
- Run the command `tacmd pdcollect`

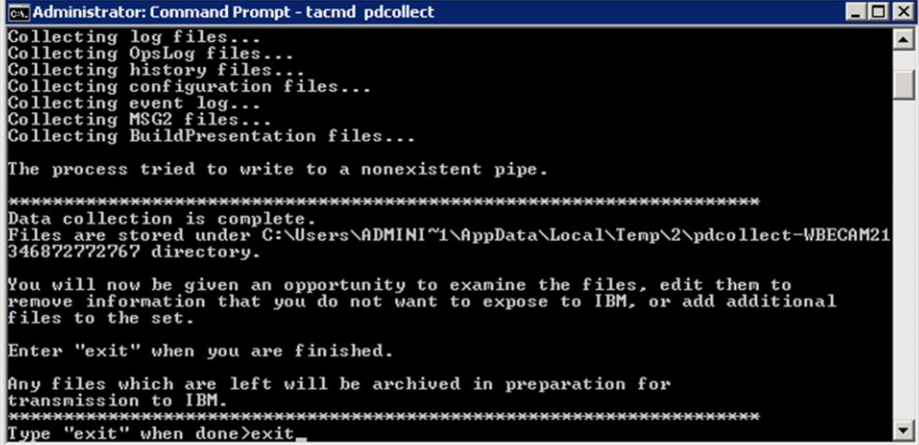


```
Administrator: Command Prompt
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.
C:\Users\Administrator>tacmd pdcollect_
```

After the problem recurs, collect log files with the increased trace settings. From a Command Prompt, run the command `tacmd pdcollect`.

Log collection (2 of 3)

- When the prompt returns, type exit



```
C:\>Administrator: Command Prompt - tacmd pdcollect
Collecting log files...
Collecting OpsLog files...
Collecting history files...
Collecting configuration files...
Collecting event log...
Collecting MSG2 files...
Collecting BuildPresentation files...

The process tried to write to a nonexistent pipe.

*****
Data collection is complete.
Files are stored under C:\Users\ADMINI~1\AppData\Local\Temp\2\pdcollect-WBECAM21
34687272767 directory.

You will now be given an opportunity to examine the files, edit them to
remove information that you do not want to expose to IBM, or add additional
files to the set.

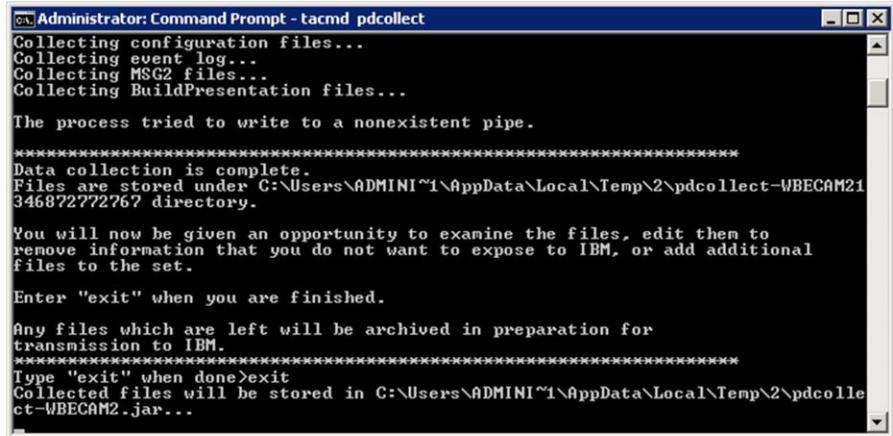
Enter "exit" when you are finished.

Any files which are left will be archived in preparation for
transmission to IBM.
*****
Type "exit" when done>exit_
```

When the command prompt returns as shown in the image, type exit.

Log collection (3 of 3)

- The directory where the collected files are stored is displayed



```
Administrator: Command Prompt - tacmd pdcollect
Collecting configuration files...
Collecting event log...
Collecting MSG2 files...
Collecting BuildPresentation files...

The process tried to write to a nonexistent pipe.

*****
Data collection is complete.
Files are stored under C:\Users\ADMINI~1\AppData\Local\Temp\2\pdcollect-WBECAM21
34687272767 directory.

You will now be given an opportunity to examine the files, edit them to
remove information that you do not want to expose to IBM, or add additional
files to the set.

Enter "exit" when you are finished.

Any files which are left will be archived in preparation for
transmission to IBM.
*****
Type "exit" when done>exit
Collected files will be stored in C:\Users\ADMINI~1\AppData\Local\Temp\2\pdcolle
ct-WBECAM2.jar...
```

After you enter exit, the directory where the collected files are stored displays.

Needed documentation for troubleshooting

- After you collect the logs, reset all of the increased trace settings
- Review pdcollect .jar file and corresponding LFA instance conf and fmt files
- The screen capture that is made after the issue recurred

After you collect the log files, remember to reverse all of the increased trace settings. Use the screen captures and file copies that you created at the beginning of this process. If you leave the increased trace settings in place, that might affect the physical disk space and processor usage of the box. Review the collected .jar file together with conf and fmt files and the screen capture saved that shows the issue for analysis.

Summary

- Now that you have completed this module, you can perform these tasks:
 - Update the LFA agent collector variables to increase the tracing
 - Collect the LFA agent logs for troubleshooting

Now that you have completed this module, you can perform these tasks:

Update the LFA agent collector variables to increase the tracing;

Collect the LFA agent logs for troubleshooting.

Trademarks, disclaimer, and copyright information

IBM, the IBM logo, ibm.com, and Tivoli are trademarks or registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of other IBM trademarks is available on the web at "[Copyright and trademark information](http://www.ibm.com/legal/copytrade.shtml)" at <http://www.ibm.com/legal/copytrade.shtml>

Windows, and the Windows logo are registered trademarks of Microsoft Corporation in the United States, other countries, or both.

Other company, product, or service names may be trademarks or service marks of others.

THE INFORMATION CONTAINED IN THIS PRESENTATION IS PROVIDED FOR INFORMATIONAL PURPOSES ONLY. WHILE EFFORTS WERE MADE TO VERIFY THE COMPLETENESS AND ACCURACY OF THE INFORMATION CONTAINED IN THIS PRESENTATION, IT IS PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. IN ADDITION, THIS INFORMATION IS BASED ON IBM'S CURRENT PRODUCT PLANS AND STRATEGY, WHICH ARE SUBJECT TO CHANGE BY IBM WITHOUT NOTICE. IBM SHALL NOT BE RESPONSIBLE FOR ANY DAMAGES ARISING OUT OF THE USE OF, OR OTHERWISE RELATED TO, THIS PRESENTATION OR ANY OTHER DOCUMENTATION. NOTHING CONTAINED IN THIS PRESENTATION IS INTENDED TO, NOR SHALL HAVE THE EFFECT OF, CREATING ANY WARRANTIES OR REPRESENTATIONS FROM IBM (OR ITS SUPPLIERS OR LICENSORS), OR ALTERING THE TERMS AND CONDITIONS OF ANY AGREEMENT OR LICENSE GOVERNING THE USE OF IBM PRODUCTS OR SOFTWARE.

© Copyright International Business Machines Corporation 2014. All rights reserved.