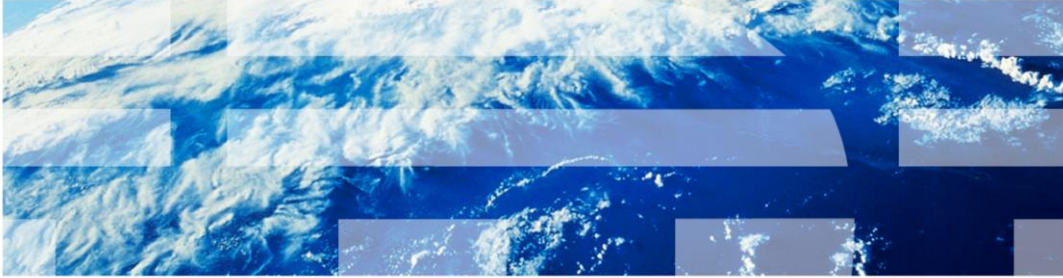


IBM Tivoli Monitoring V6.2

Reading agent logs, Part 1: Locating and collecting, log types, and naming conventions



© 2013 IBM Corporation

IBM Tivoli® Monitoring V6.2, Reading agent logs, part one: locating and collecting, log types, and naming conventions.

Assumptions

- This module is the first of three that provide guidelines about how to identify and collect Tivoli Monitoring agent logs
- Subsequent modules provide an introduction to reading logs, locating and identifying errors, and potentially resolving problems in frequently used logs
- Because a single error can have various root causes, detecting the errors might not always provide a solution. But it can reduce the amount of time that is required to resolve the problem.
- You must understand how IBM Tivoli Monitoring is installed and configured in your environment
 - For example, which agents are installed, the host names that the agents are installed on, the Tivoli Enterprise Monitoring Servers (TEMS) and the Tivoli Enterprise Portal Servers (TEPS) that these agents report to
- You must understand the directory structure that Tivoli Monitoring is installed under and the Windows® or UNIX® operating systems

This module is the first of three that provide guidelines on how to identify and collect Tivoli Monitoring agent logs.

Subsequent modules provide an introduction to reading logs, locating and identifying errors and potentially resolving problems in frequently used logs.

Since a single error can have various root causes, detecting the errors might not always provide a solution, but it can dramatically reduce the amount of time that is required to resolve the problem.

You should have a good understanding of how IBM Tivoli Monitoring (ITM) is installed and configured in your environment. For example, you should understand which agents are installed. You should know the host names the agents are installed on, the Tivoli Enterprise Monitoring Server (TEMS), and the Tivoli Enterprise Portal Servers (TEPS) that these agents report to.

You should understand the directory structure that Tivoli Monitoring is installed under and possess a good understanding of the Windows or UNIX operating systems.

Objectives

- When you complete this module, you can perform these tasks:
 - Describe the function of logs
 - Locate and collect logs
 - Identify the type and name of the logs that are collected for different Tivoli Monitoring agents
- The second and third modules present information on how to:
 - Search log collections for known errors
 - Search individual logs for unknown problems
 - Identify errors in logs
 - Identify possible solutions for the errors that you find

- When you complete this module, you can perform these tasks:
 - Describe the function of logs
 - Locate and collect logs
 - Identify the type and name of the logs that are collected for different Tivoli Monitoring agents
- The second and third modules present information on how to:
 - Search log collections for known errors
 - Search individual logs for unknown problems
 - Identify errors in logs
 - Identify possible solutions for the errors found

Overview

- Introduction to logs
- Locating and collecting logs
- Types of Tivoli Monitoring agent logs and naming conventions

This module has three sections. They are introduction to logs; locating and collecting logs; and types of Tivoli Monitoring agent logs and naming conventions.

Introduction to logs

- Log files provide the details behind messages and the actions that are taken by an agent
- Installation problems are captured in installation or abort logs to help you determine the cause of the problem
- Some agents provide logs that isolate the cause of the problem to a specific component and a specific log
- The default level of log tracing is set to ERROR, which shows many errors without excessive clutter or chatter in the logs

Log files provide the details behind messages that appear during the installation or the use of applications.

Some messages might indicate an error condition or might be informational.

If you are installing a new product and encounter a problem, the installation software may not have written the directory structure and log files for the agent yet.

In this situation, you might only have an installation or abort log file to help you determine the cause of the problem.

When a product like an IBM Tivoli Monitoring Operating System agent is successfully installed and has been running before a problem is detected, very often the log files for the agent can provide details that indicate where the problem occurred.

The default level of tracing is set to ERROR.

This tracing level produces the least amount of detail that can potentially clutter the log files, but it detects many of the errors described in this presentation.

If additional details are required, the IBM support staff might ask you to increase the trace level depending on the type of problem that occurred.

Section

Locating and collecting logs

In the next section, you learn where to locate the log files for analysis and how to collect them.

Log locations

- Trace logs are at these locations:
 - On Windows:
%ITM_Install\TMAITM6\logs\<<hostname>>_<pc>_k<pc>agent_<timestamp>-01.log
 - On Linux® or UNIX:
\$ITM_Install/logs/<<hostname>>_<pc>_k<pc>agent_<timestamp>-01.log
- RAS (Reliability, Availability, and Serviceability) logs are in these same directories
- PC is the Product Code that describes the agent that the log collects data on
- For a comprehensive list of product codes, visit this page:
<http://www-01.ibm.com/support/docview.wss?uid=swg21265222>
- These product codes are common:
 - nt: Monitoring Agent for Windows OS
 - lz: Monitoring Agent for Linux OS
 - ux: Monitoring Agent for UNIX OS
 - lo: Tivoli Log File Agent

Trace and RAS log files are found in the locations shown in this chart for Windows, Linux, and UNIX operating systems.

The log file names have a two character **Product Code** that describes the agent the log collects data on.

For a complete list of product codes see the link shown.

Some of the more common product codes are:

- nt for the Monitoring Agent for Windows OS
- lz for the Monitoring Agent for Linux OS
- ux for the Monitoring Agent for UNIX OS
- lo for the Tivoli Log File Agent

Collecting logs: PDCollect

- You can use the PDCollect tool to gather logs and other environmental information from a problematic system
 - For more details about PDCollect, see this web page:
Collecting problem determination data for ITM components
(<http://www-304.ibm.com/support/docview.wss?uid=swg21446655>)
- For security reasons, PDCollect might be disabled on some systems

PDCollect is a great tool to collect logs and other environmental information from a problematic system.

For security reasons, some companies might want to limit the information collected and might disable the PDCollect tool.

You can run PDCollect on Windows, Linux, and UNIX systems.

If you are not comfortable with UNIX search tools, PDCollect creates compressed files that allow you to export Linux and UNIX data onto a Windows system.

For more details on PDCollect, see the link shown.

Collecting logs: digup

- An alternate method to collect agent logs is to use the digup command
- Digup is an older script-based log-gathering tool, but it is available on many UNIX and Linux systems

If PDCollect is not available to you, consider the **digup** command.

Digup is an older script-based log gathering tool, but is still available on many UNIX and Linux systems.

The next slide provides the syntax and options available for the digup command.

Collecting logs: digup syntax

- Syntax for invoking the digup shell script:
digup [-h <ITM_directory>][-a] [-s] [-k] [-i] [-t] [-l label]
- where:
 - h Specifies the \$CANDLEHOME directory
 - a Builds a .tar file of your site information. Without this option, digup adds only system-identification information to the \$CANDLEHOME/logs/candle_installation.log file
 - s Generates a one-line summary of your operating system information
 - k Keeps the working directory after completion
Typically, the temporary directory \$CANDLEHOME/tmp/DIG (used for collected data) is packed and removed on completion
Option -k means that this directory is not removed; this feature is useful when you want to review the collected data
 - i Ignores the agent logs when building the .tar file
 - t Gets Tivoli Enterprise Monitoring Server tables
 - l Defines a label or text identifier to display on the output
 - ? Requests help information
- It is typical to always specify the -a option with the digup command

This slide shows and explains the various options that can be used with the **digup** command and the command syntax. It is typical to always specify the **-a** option for the digup command.

Collecting logs: Agent version information, cinfo and kincinfo

- Unlike PDCollect, the digup command does not automatically provide the installed agent name and version information that is commonly provided by the utilities **cinfo** and **kincinfo**
- When you use the digup command, you typically run these commands to manually collect that information
 - For UNIX or Linux systems, use this command to create an install.out file in the /tmp directory:
cinfo -i > /tmp/install.out
 - For a Windows system, use this command to create an install.out file in the current directory:
kincinfo.exe -d > install.txt
- For more details about **cinfo** and **kincinfo**, see the Tivoli Monitoring Command Reference: http://pic.dhe.ibm.com/infocenter/tivihelp/v15r1/topic/com.ibm.itm.doc_6.2.3fp1/itm623fp1_cmdref.pdf

Because problems can be associated with a specific version of an agent, it is important to understand which agents and their versions, are installed and running. The utilities **cinfo** and **kincinfo** provide this information from the systems they are run on.

Notice that the UNIX and Linux versions of **cinfo** use the **-i** option, that displays an inventory of installed products.

The Windows version of **kincinfo** uses the **-d** option, which displays a list of installed products, which can be parsed.

For more details on **cinfo** and **kincinfo** see the link shown.

Collecting logs: Interpreting version information from cinfo

- The cinfo or kincinfo data that is gathered by a PDCollect is placed in a file named cinfo.info
- The output of cinfo or kincinfo is typically in the format VV.RM.FF.II
 - Where VV is the base version number, R represents the revision, M is the modification number, FF is the fix pack number, and II is the interim fix pack number
- This format was modified and expanded recently to also include interim features in the section that was previously reserved for the fix pack
 - For example, System P Agents for V6.2.2 interim feature 2, now displays in a cinfo output as 06.22.02.00

Version information collected by a PDCollect is placed in a file named **cinfo.info** located in the **ITM** directory of the extracted file.

The data presented in the output of a cinfo or kincinfo command typically displays in the format **VV.RM.FF.II** (Capital i).

This format was recently modified and expanded to include interim features in the section that was previously reserved for the fix pack. For example, System P Agents for V6.2.2 Interim Feature 2 now displays in a **cinfo** output as **06.22.02.00**.

The next slide presents an example of both a **cinfo** and a **kincinfo** output. You can see the information is self explanatory; there is a slight difference in format.

Example of cinfo and kincinfo outputs

PC	PRODUCT DESC	PLAT	VER	BUILD	INSTALL DATE
Iz	Monitoring Agent for Linux OS	Ix8266	06.22.07.00	13201	20120505 1439

"ProdCode", "Description"	"Platform"	"Version"	"Release"	"Verfile"
"NT", "Monitoring Agent for Windows OS", "WINNT", "061007000", "200804301305", "KNTWICMA.ver"				
"NT", "Monitoring Agent for Windows OS", "WINNT", "062202000", "01121", "KNTWICMS.ver"				
"NT", "Monitoring Agent for Windows OS", "WINNT", "062202000", "01121", "KNTWICNS.ver"				
"NT", "Monitoring Agent for Windows OS", "WINNT", "062202000", "01121", "KNTWIXEB.ver"				
"NT", "Monitoring Agent for Windows OS", "WINNT", "062202000", "01121", "KNTWIXEW.ver"				

For more information about **kincinfo** "verfiles" see the slide **Other helpful references**

Here are examples of **cinfo** and **kincinfo** outputs.

For more information on **kincinfo** "verfiles", see the slide at the end of this presentation called *Other helpful references*.

Collecting logs: AS400 equivalent of PDCollect

If you need to collect logs from an AS400 system, perform these steps:

1. Modify the QAUTOTMP/KMSPARM file (member KBBENV) to set the logging to KBB_RAS1=ERROR (UNIT:KA4 ALL) (UNIT:KRAALL) (UNIT:KDS ALL)
2. Restart the agent and reproduce the problem with this logging turned on
3. Obtain the agent trace files as listed
Notes:
 - There is always a KA4AGENT01 file
 - If logging wraps, then KA4AGENT02 and KA4AGENT03 are also usedTrace file list:
 - QAUTOTMP/KA4AGENT01
 - QAUTOTMP/KA4AGENT02
 - QAUTOTMP/KA4AGENT03
4. Check the joblog for the CT_AGENT job, which is where the agent runs
This information can be helpful for any exceptions that the operating system signaled
5. Use GO OMA and then option 1 to display the message queue where errors are logged

This slide is included for future reference. Since a **PDCollect** utility does not run on AS400 systems, the steps that are presented in this slide enable you to collect logs from an AS400 system to review.

Working with logs

- Decide where you want to work with the logs that you collected
 - You can work with the logs on the server where they were generated
 - This approach implies some risk and is not recommended
 - You can use collection tools like PDCollect or digup to generate a compressed file
 - These tools provide the logs and other environmental information. You can export them to an operating system that has search tools that you are comfortable with.
 - An example is Windows XP
 - This presentation uses Windows and Windows Explorer because of these factors:
 - Their ease of use
 - The capability to read logs from various operating systems
 - The ability to access the Internet

You can work with the logs on the server where they were generated. This approach implies some risk and is not recommended.

You can use collection tools like **PDCollect** or **digup** to generate a compressed file. The logs and other environmental information can be exported to an operating system that has search tools you are comfortable with, for example Windows XP.

Windows and Windows Explorer are used in this presentation because of their ease of use, the capability to read logs from various operating systems, and the ability to access the Internet.

Types of Tivoli Monitoring agent logs and naming conventions

The next section presents the types of agent logs that are most likely to contain errors and the naming conventions that you can use to identify the files.

Types of agent logs: Naming overview

- Operating system agents such as Windows (NT), UNIX (UX), and Linux (LZ) use the same naming convention for their trace logs

```
<hostname>_nt_kntcma_<timestamp>-0#.log
<hostname>_ux_kuxagent_<timestamp>-0#.log
<hostname>_lz_klzagent_<timestamp>-0#.log
```

These are real-world examples:

```
prod_srver5_nt_kntcma_4eea9bf6-01.log
testserver1_ux_kuxagent_4e5659b4-01.log
devel_2_lz_klzagent_4f031fbf-01.log
```

- AS400 (A4) agent logs are named QAUTOTMP/KA4AGENT0#
 - Other agent logs are like these examples for CEC (PK), VIOS (VA), UNIX Log (UL), and VMware VI (VM):
- ```
<hostname>_pk_kpkagent_<timestamp>-0#.log
<hostname>_va_kvaagent_<timestamp>-0#.log
<hostname>_ul_kulagent_<timestamp>-0#.log
<hostname>_vm_<instance>_kvmagent_<timestamp>-0#.log
```

- Agent RAS logs have a format like these two logs:

```
<hostname>_ux_#####.log
<hostname>_lz_#####.log
```

An important part of identifying the cause of agent-related problems is being able to read the logs that the various agents generate.

Typically Operating System agents such as Windows, UNIX, and Linux follow the same naming convention.

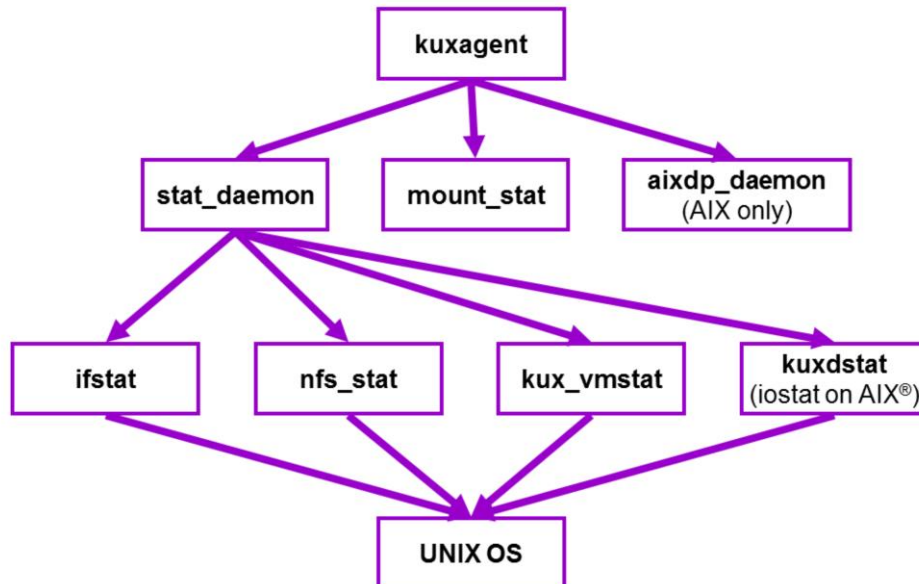
Some examples are shown.

The naming conventions that are presented in the next few slides are intended to give you a sample of the names you are likely to encounter when looking at the logs directory.

With Windows Explorer, you can sort the log files by name and that makes it easier to find names similar to those names shown in the presentation.

## Types of agent logs: UNIX Operating System agent (UX)

The V6.23 Fix Pack 1 UNIX OS agent collects separate logs for each of these components



18

Reading agent logs, part one: Locating and collecting, log types and naming conventions

© 2013 IBM Corporation

This slide represents the components of the 6.23 Fix Pack 1 version of a UNIX OS agent.

The UNIX OS agent product code (UX) uses a separate log for each of the various components that it collects information about.

The next slide shows the log name that is associated with the component that is monitored.

## Types of logs: UNIX OS agent process, daemons and subdaemons

- These are four types of logs:
  - **kuxagent**: (parent process) Runs TakeSample requests from Tivoli Enterprise Monitoring Server and directly collects some metrics  
     <hostname>\_ux\_kuxagent\_<timestamp>-0#.log
  - **stat\_daemon**: Stores and processes data from subdaemons and replies to requests for data from kuxagent  
     <hostname>\_ux\_stat\_daemon\_<timestamp>-0#.log
  - **mount\_stat**: Collects file systems statistics  
     <hostname>\_ux\_mount\_stat\_<timestamp>-0#.log
  - **aixdp\_daemon**: Is responsible for interfacing with the AIX data provider shared libraries (KPX integration)  
     <hostname>\_ux\_aixdp\_daemon\_<timestamp>-0#.log
- Four subdaemons gather data every 30 seconds. These processes use pipes to communicate with stat\_daemon
  - **ifstat**: Network interface statistics  
     <hostname>\_ux\_ifstat\_<timestamp>-0#.log
  - **nfs\_stat**: NFS and RPC statistics  
     <hostname>\_ux\_nfs\_stat\_<timestamp>-0#.log
  - **kux\_vmstat**: Processor and memory statistics  
     <hostname>\_ux\_kux\_vmstat\_<timestamp>-0#.log
  - **kuxdstat**: Disk i/o statistics (iostat on AIX)  
     <hostname>\_ux\_kuxdstat\_<timestamp>-0#.log

Here are the UNIX OS agent process, daemons, and subdaemons as well as the file names that they populate.

Depending on the type of problem you encounter, you might be able to determine which logs are most likely to capture the problem symptoms.

For example, if you are encountering errors that are related to file systems, a good place to start is to check the mount\_stat file shown.

For errors or problems that are related to the network, look at the ifstat logs.

## Types of logs: Proxy Agent Services (PAS) or Watchdog

- Proxy Agent Services (PAS) logs are also known as Watchdog logs
- They provide these capabilities:
  - Fault-tolerance for agent applications by monitoring and ensuring their availability
  - Historical information about frequency of unhealthy agent behavior and unexpected process termination
  - Agent Management Services workspaces for Windows and Linux managed systems
- They can provide insights into these types of problems:
  - Agents that restart automatically
  - Multiple agent processes that run on a system instead of one agent process
  - Multiple copies of the KCAWD process started
- These are examples of typical PAS log names:
  - <hostname>\_nt\_kcawd\_<timestamp>-0#.log
  - <hostname>\_ux\_kcawd\_<timestamp>-0#.log
  - <hostname>\_lz\_kcawd\_<timestamp>-0#.log

Another type of log to be aware of is the Proxy Agent Services or “watchdog”.

The **KCAWD** process watches over and performs agent restarts and other functions.

- Such as:

- Fault-tolerance for agent applications by monitoring and ensuring their availability
- Historical information on frequency of unhealthy agent behavior and unexpected process termination
- Agent Management Services workspaces for Windows and Linux managed systems

- PAS logs can provide insights into problems like these:

- Agents apparently restarting by themselves
- Multiple agent processes running on a system that should only have one
- Multiple copies of the KCAWD process started

## Types of logs: DataProvider (DP)

- Other important logs include DataProvider (DP) logs
- Some agents have a factory agent and a DataProvider (DP) component
- The DataProvider collects information and sends it to the factory agent
- The factory agent passes the data to two locations:
  - Tivoli Enterprise Monitoring Server (then seen in the Tivoli Enterprise Portal)
  - Historical data collection that is displayed in the data warehouse
- These are examples of the naming conventions that are used for DataProvider logs:
  - <hostname>\_pk\_CECDataProvider\_<timestamp>-0#.log
  - <hostname>\_va\_aixDataProvider-61\_<timestamp>-0#.log
  - kvm\_data\_provider\_<instance>\_startup.log
  - kvm\_data\_provider\_<instance>\_#.log

Other important logs to be aware of include DataProvider (DP) logs.

Some agents are composed of a factory agent and a DataProvider component.

The DataProvider collects information and sends it to the factory agent.

The factory agent passes the data on to the Tivoli Enterprise Management Server to show in the Tivoli Enterprise Portal, and to historical data collection to show in the data warehouse.

Various naming conventions are used for DataProvider log files as shown.

## Other helpful references

- For more information about interpreting kincinfo data for application support, see this web page:  
Interpreting KinCInfo output to show which application support packages are installed  
(<http://www-01.ibm.com/support/docview.wss?uid=swg21579052>)
- For a comprehensive list of product codes, see this web page:  
IBM Tivoli Monitoring ITM 6.X Product Codes  
(<http://www-01.ibm.com/support/docview.wss?uid=swg21265222>)
- You can send your comments and feedback to [ziolk@us.ibm.com](mailto:ziolk@us.ibm.com)

Here are a few helpful references.

## Summary

- After completing this module, you can perform these tasks:
  - Describe the function of logs
  - Locate and collect logs
  - Identify the type and name of the logs that are collected for different Tivoli Monitoring agents
- The second and third modules present information about these tasks:
  - Search log collections for known errors
  - Search individual logs for unknown problems
  - Identify errors in logs
  - Identify possible solutions for the errors that you find

- After completing this module, you can perform these tasks:
  - Describe the function of logs
  - Locate and collect logs
  - Identify the type and name of the logs that are collected for different Tivoli Monitoring agents
- The second and third modules present information about these tasks:
  - Search log collections for known errors
  - Search individual logs for unknown problems
  - Identify errors in logs
  - Identify possible solutions for the errors that you find

## Trademarks, disclaimer, and copyright information

IBM, the IBM logo, ibm.com, AIX, 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>

Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both.

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

UNIX is a registered trademark of The Open Group in the United States and other countries.

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 2012. All rights reserved.