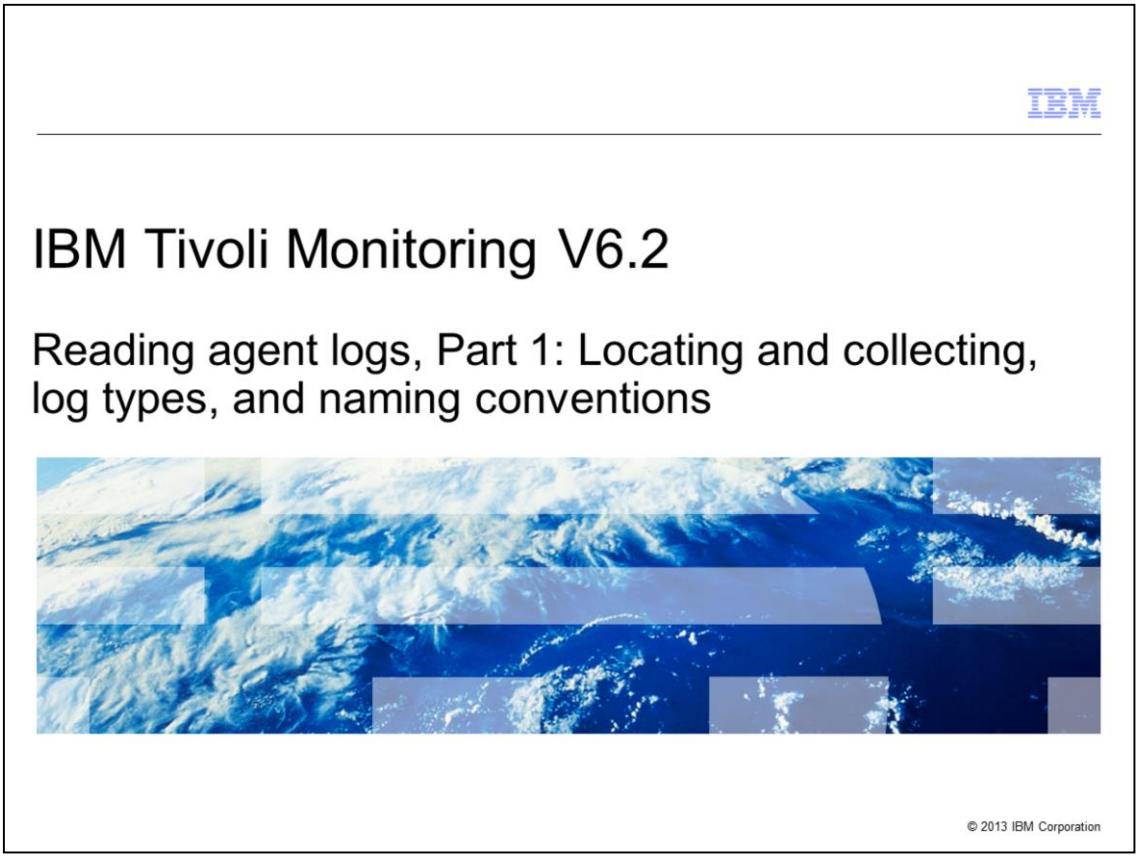
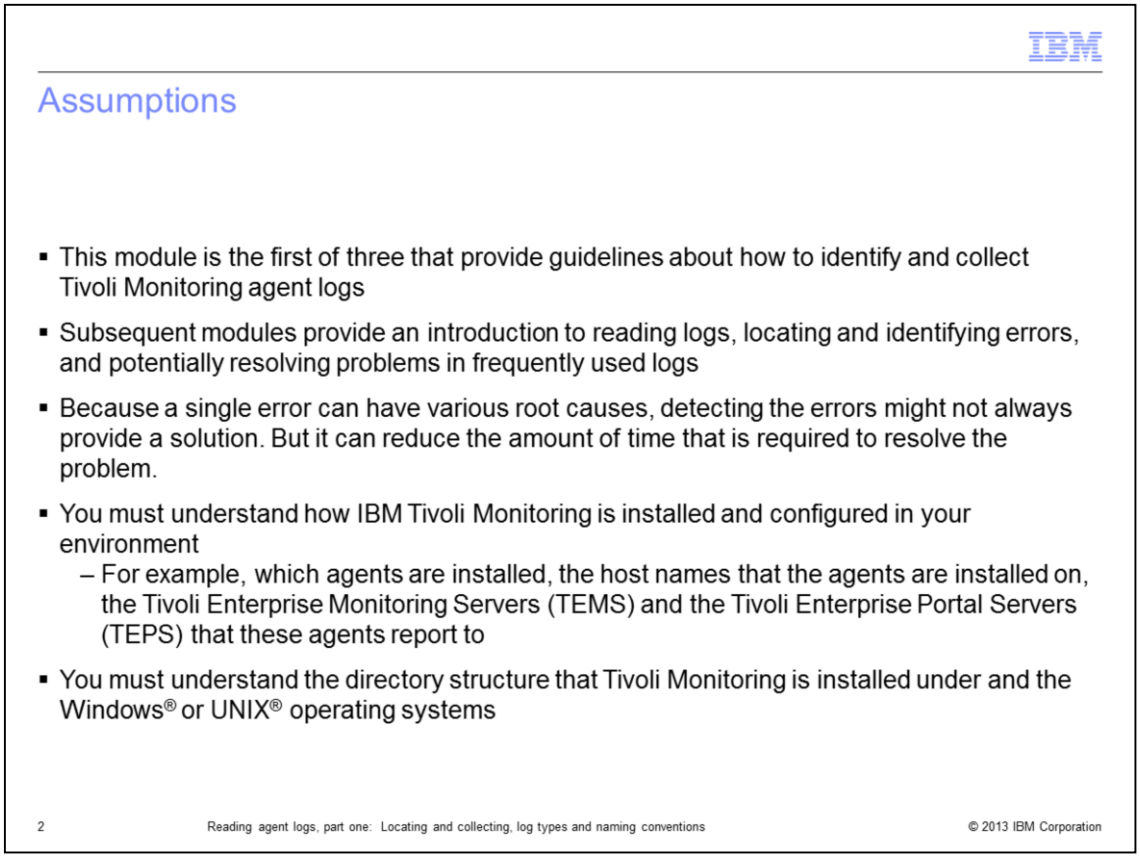


IBM Tivoli® Monitoring V6.2, Reading agent logs, part one: locating and collecting, log types, and naming conventions.



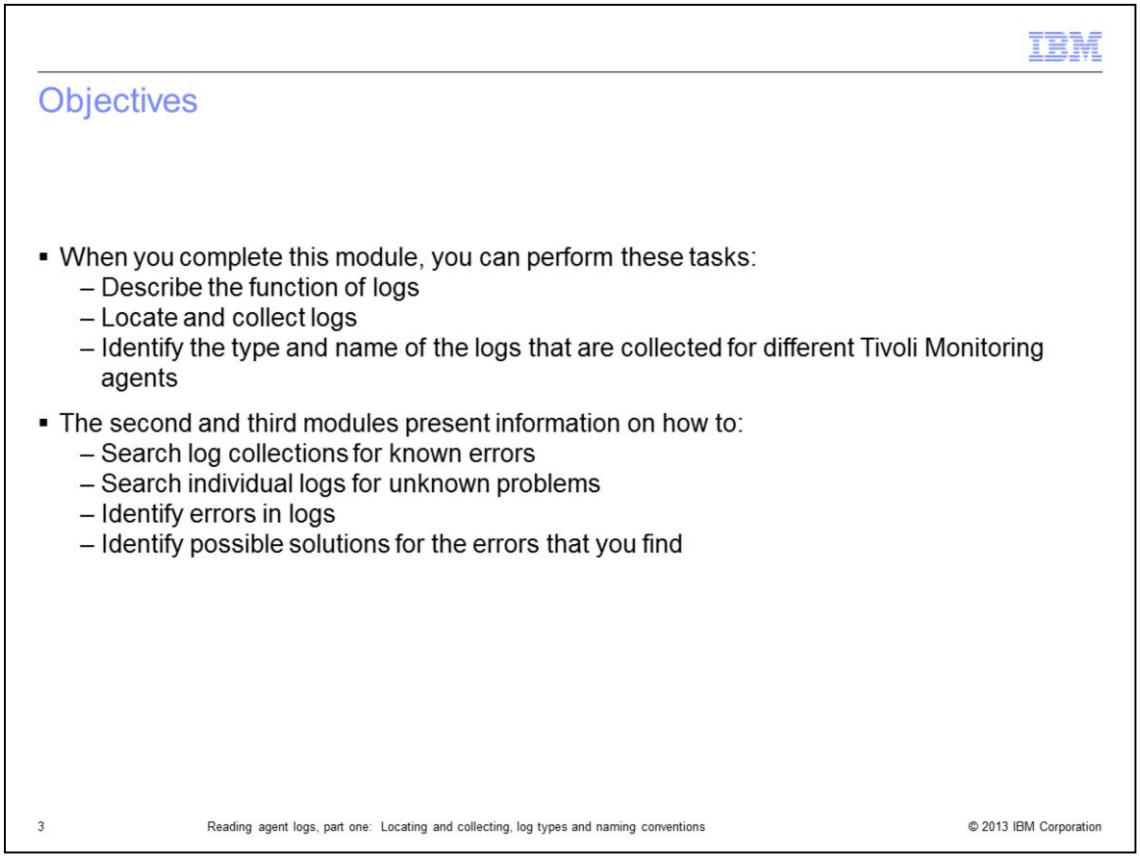
This module is the first of three that provide guidelines on how to identify and collect Tivoli Monitoring agent logs.

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.



- 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

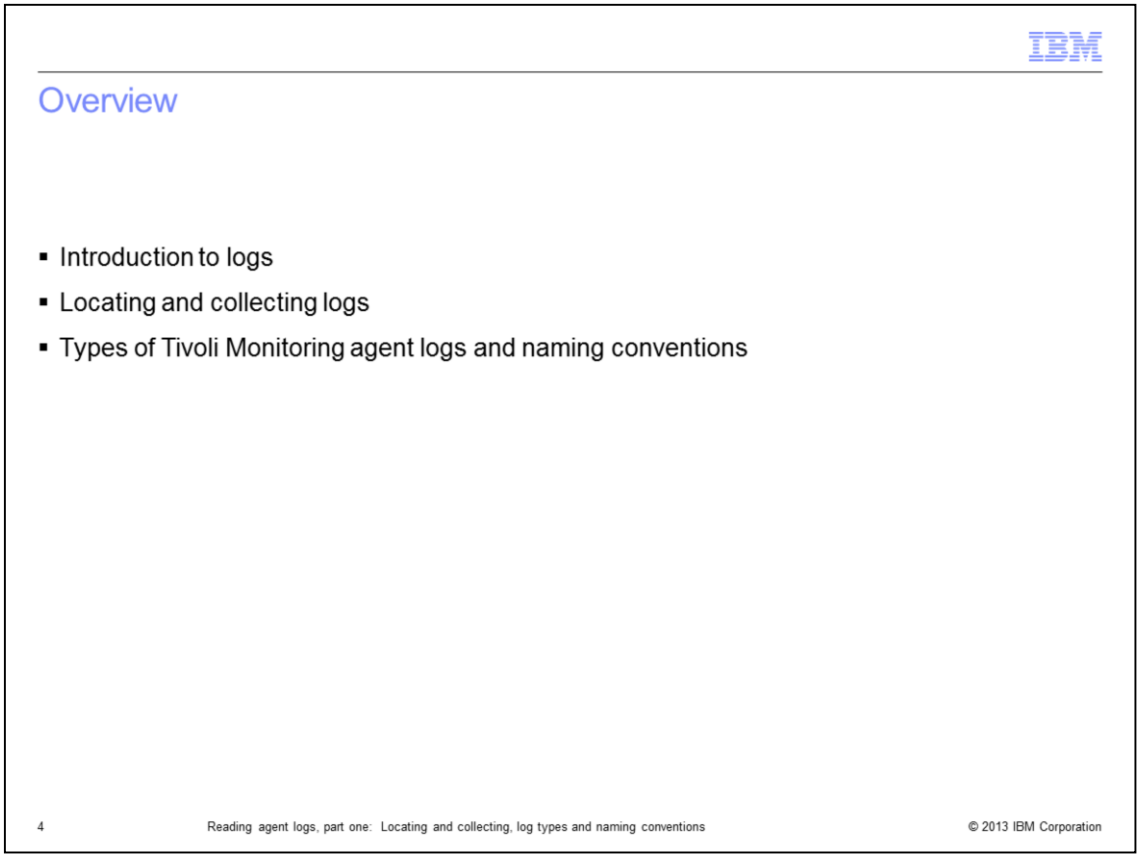
- The second and third modules present information on how to:

    -- Search log collections for known errors

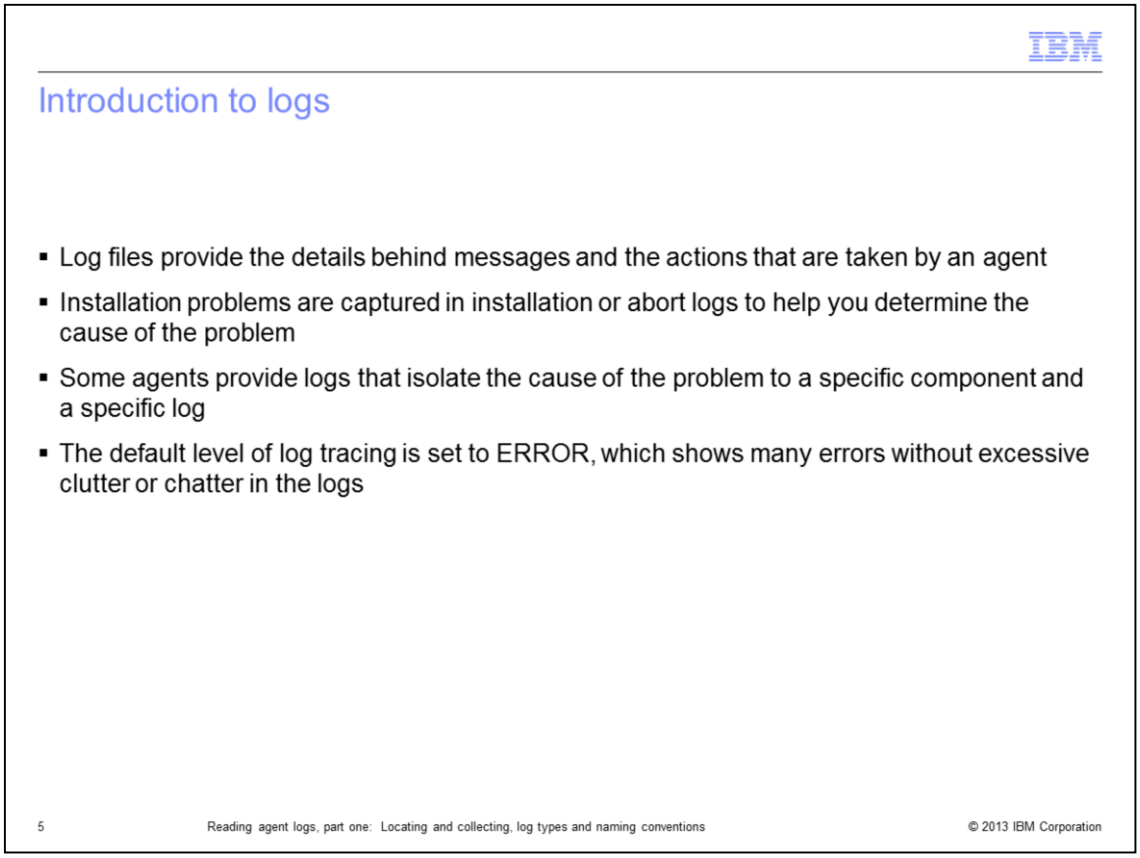
    -- Search individual logs for unknown problems

    -- Identify errors in logs

    -- Identify possible solutions for the errors found



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



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.

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

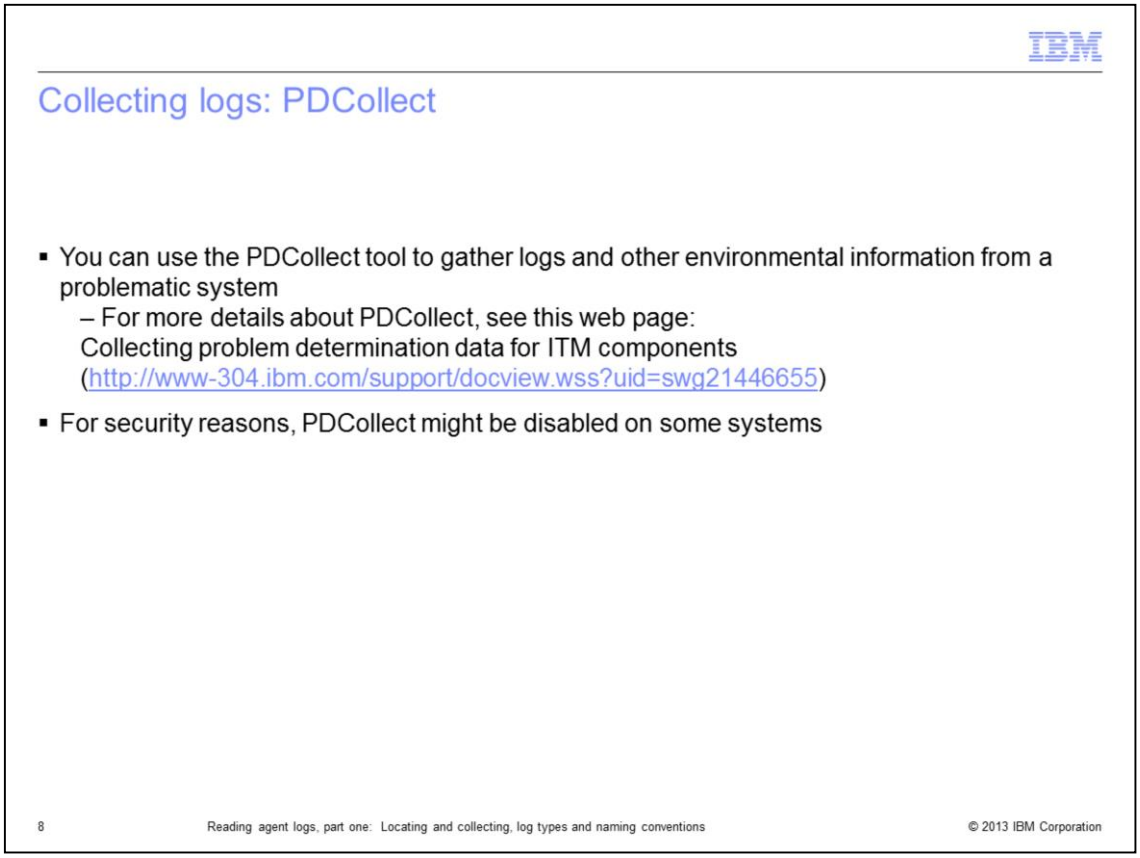
Trace and RAS log files are found in the locations shown in this chart for Windows, Linux, and UNIX operating systems.

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



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.

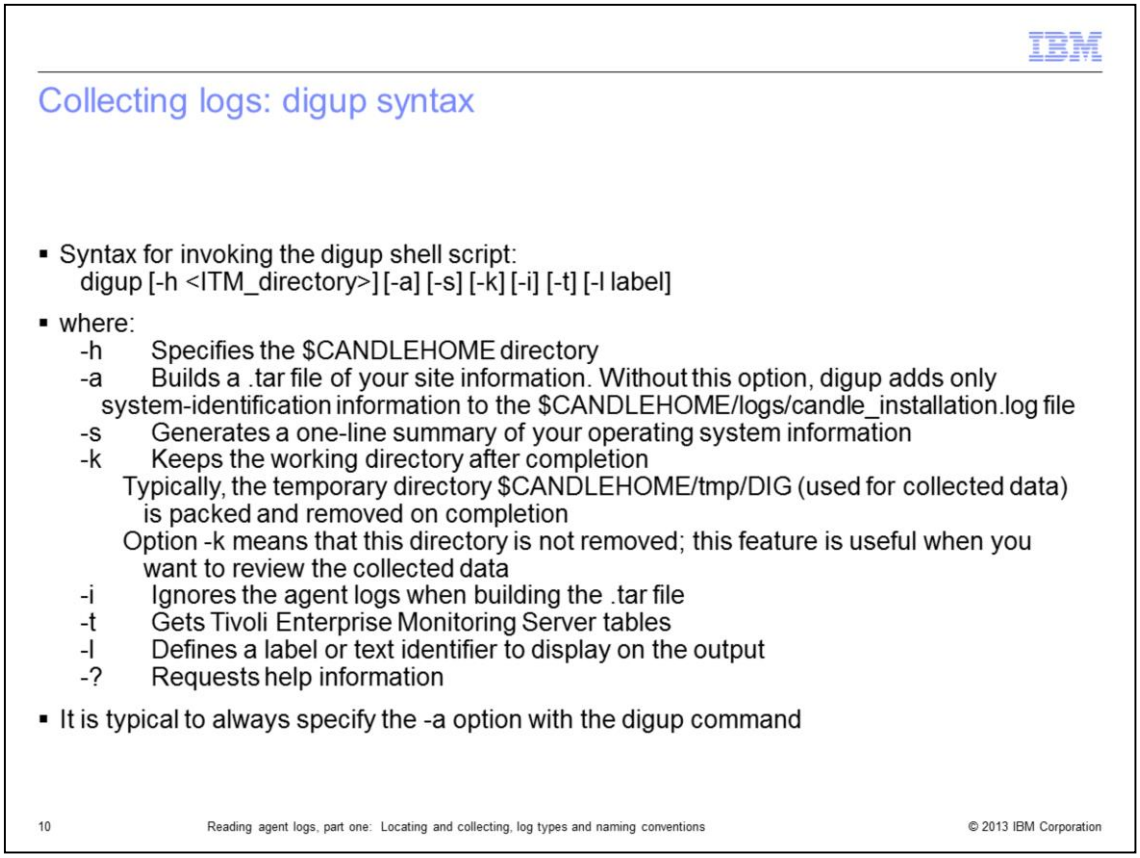
If you are not comfortable with UNIX search tools, PDCollect creates compressed files that allow you to export Linux and UNIX data onto a Windows system.

For more details on PDCollect, see the link shown.

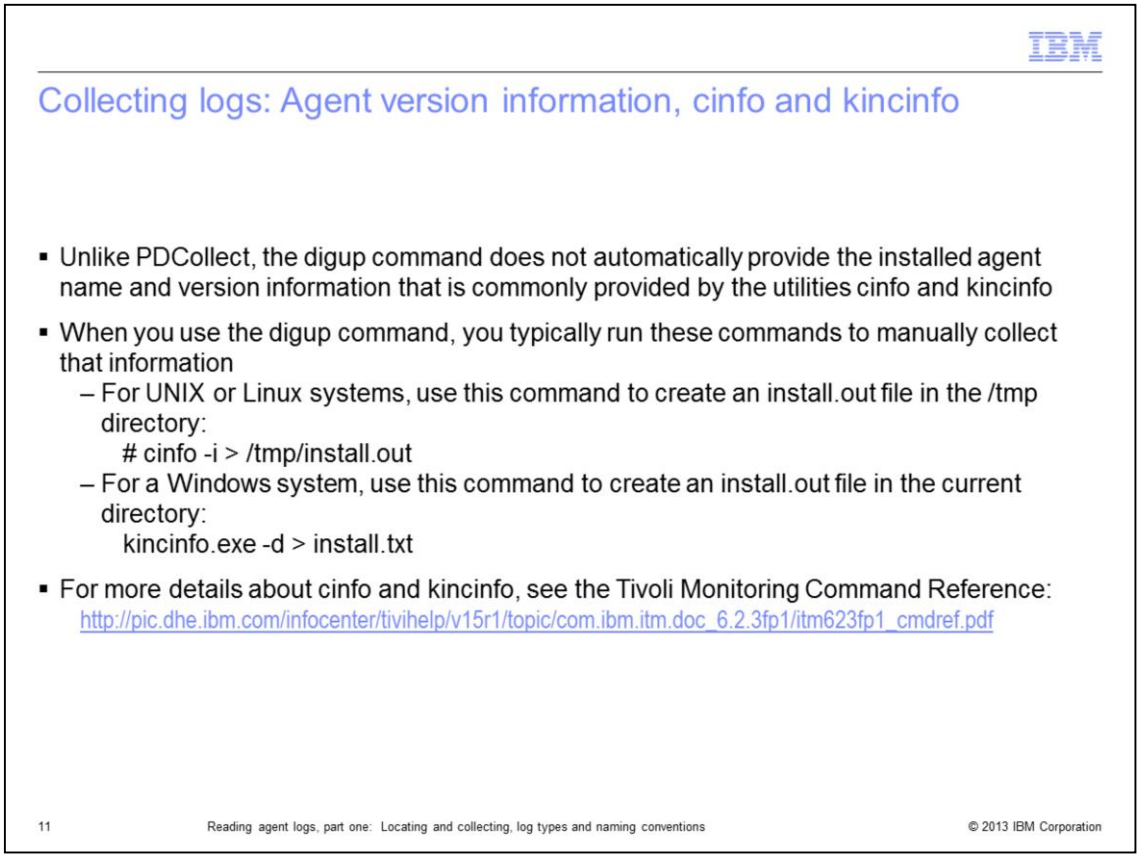
If PDCollect is not available to you, consider the **digup** command.

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.



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.

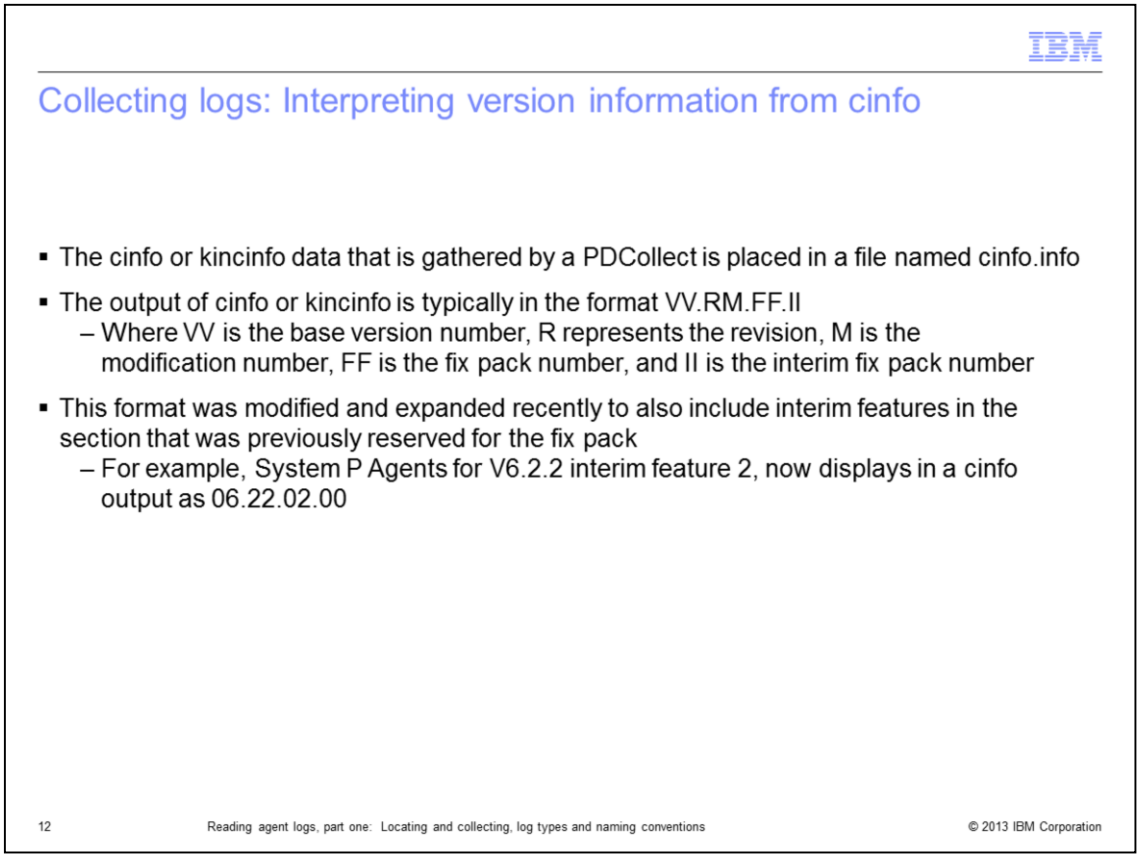


Because problems can be associated with a specific version of an agent, it is import to understand which agents and their versions, are installed and running. The utilities **cinfo** and **kincinfo** provide this information from the systems they are run on.

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.

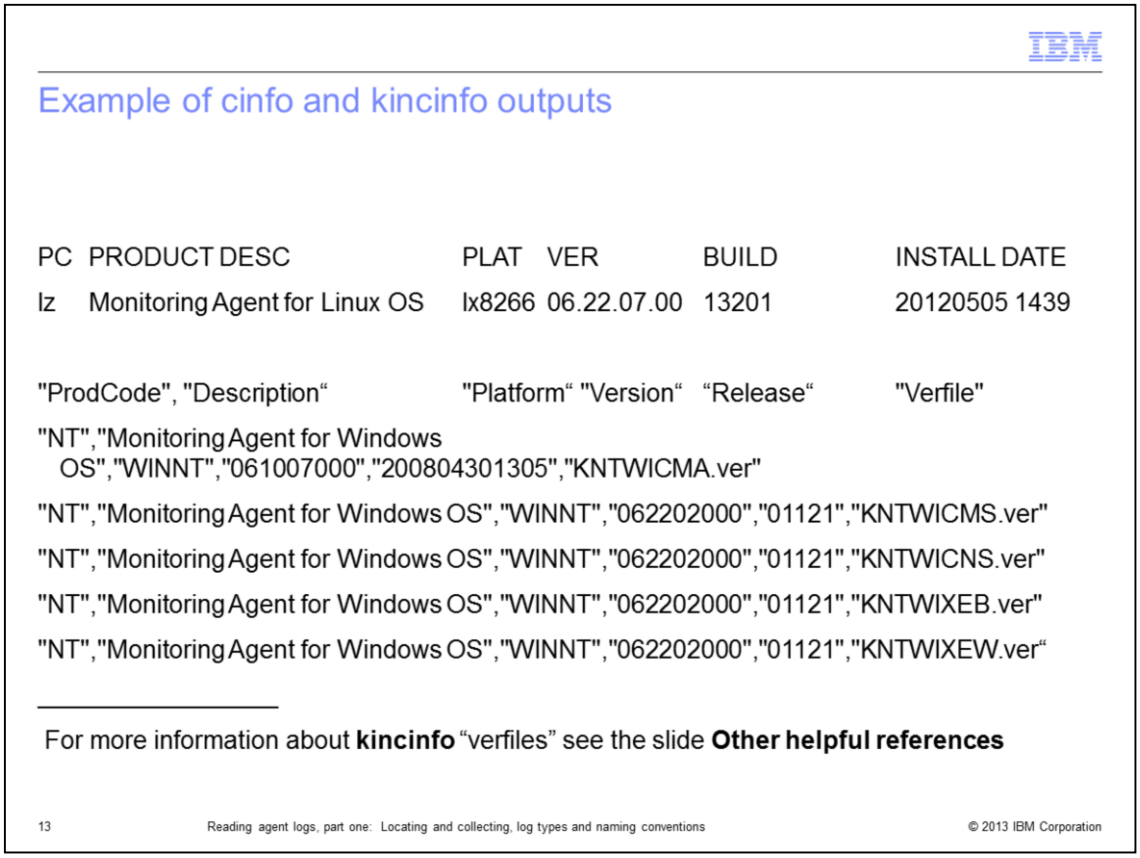


Version information collected by a PDCollect is placed in a file named **cinfo.info** located in the **ITM** directory of the extracted file.

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

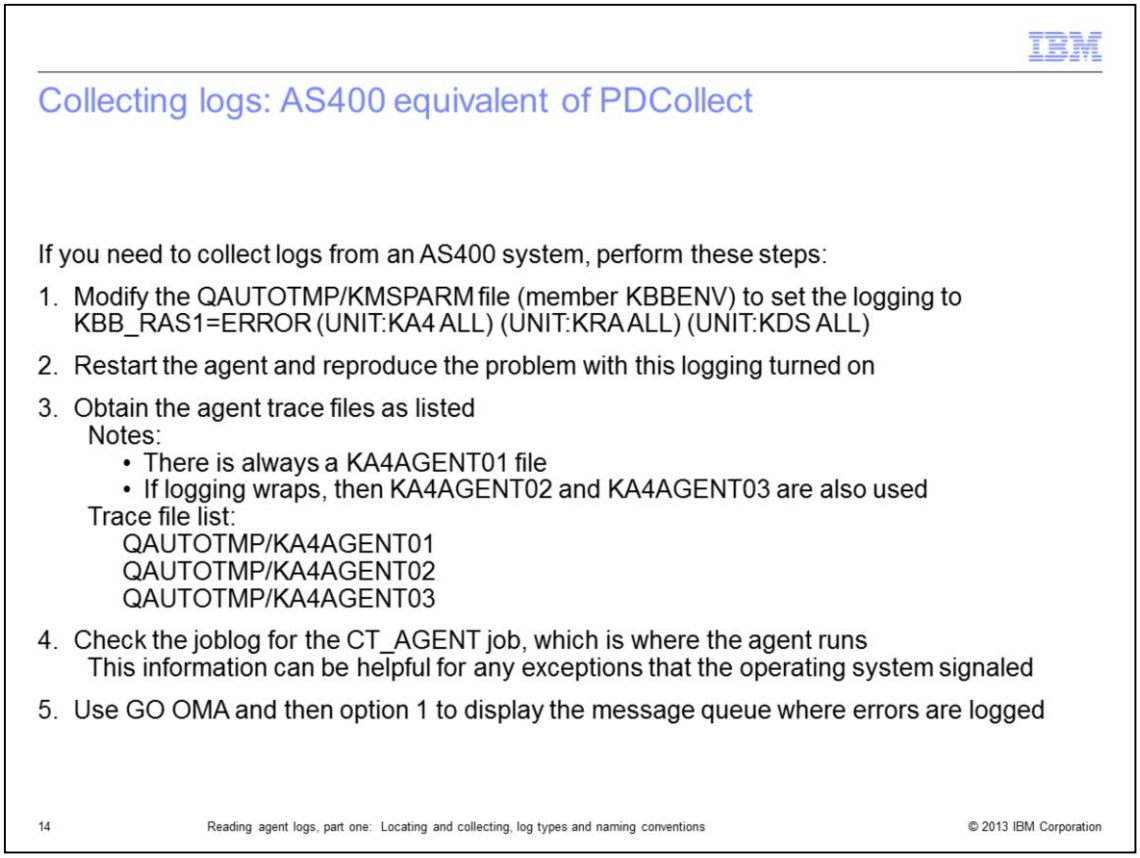
This format was recently modified and expanded to include interim features in the section that was previously reserved for the fix pack. For example, System P Agents for V6.2.2 Interim Feature 2 now displays in a **cinfo** output as **06.22.02.00**.

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.

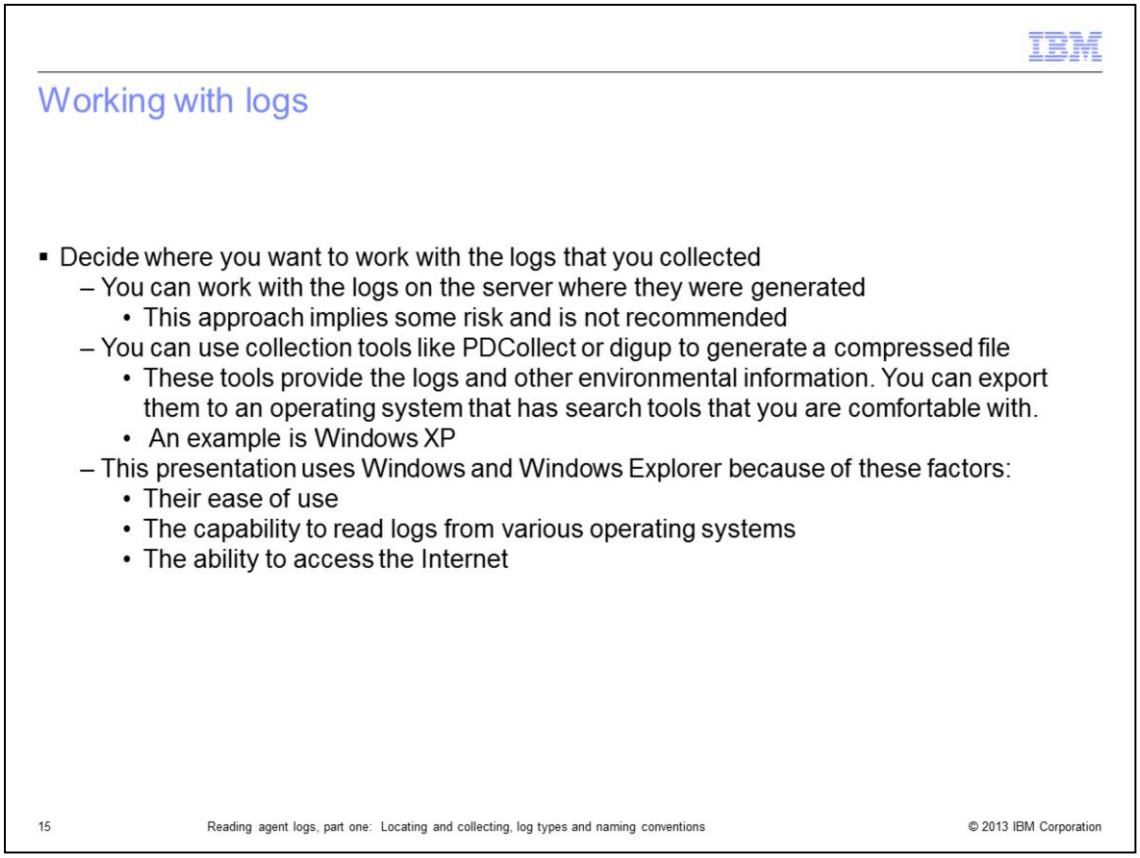


Here are examples of **cinfo** and **kincinfo** outputs.

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



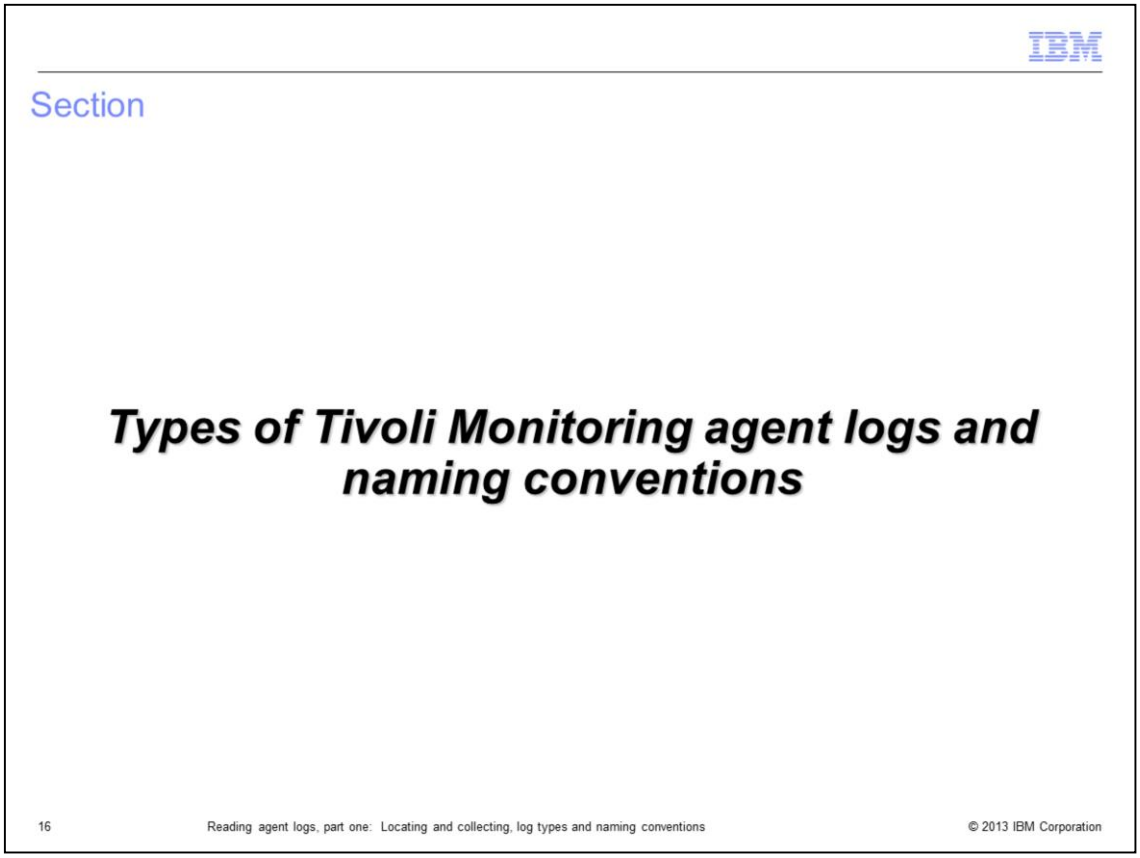
This slide is included for future reference. Since a **PDCollect** utility does not run on AS400 systems, the steps that are presented in this slide enable you to collect logs from an AS400 system to review.



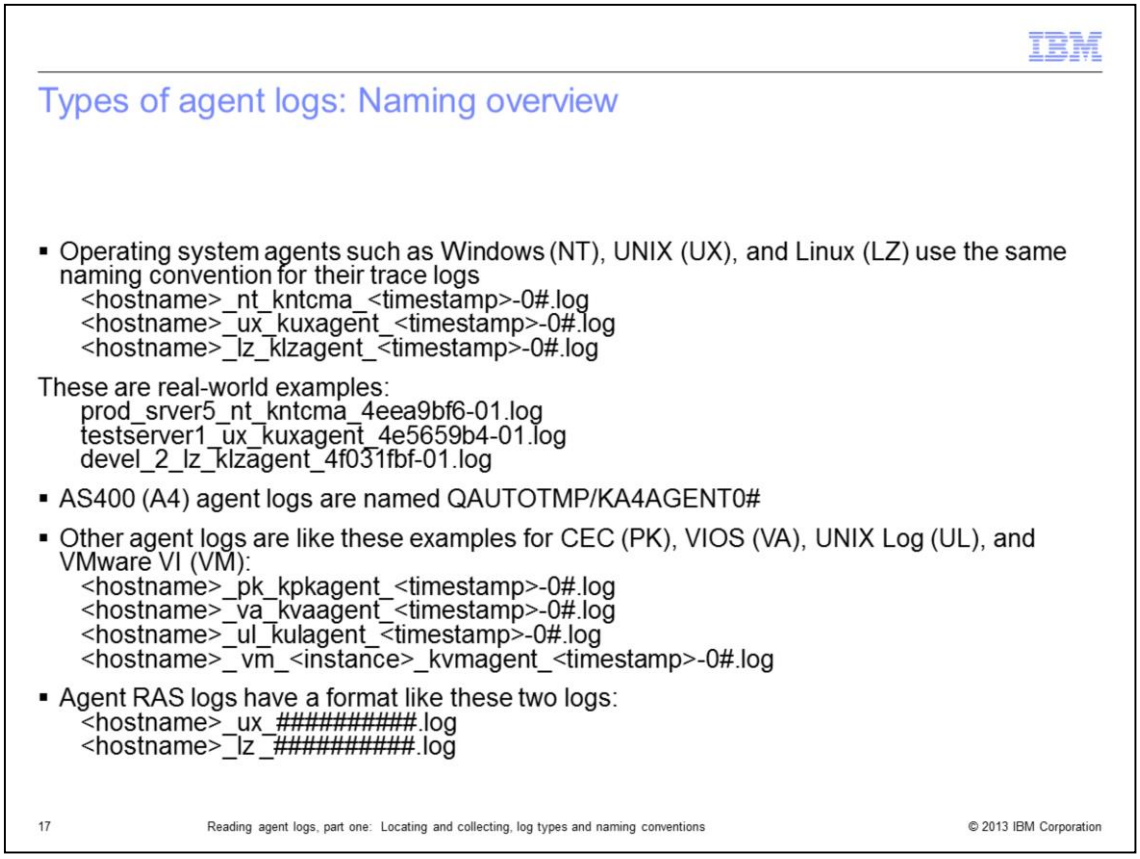
You can work with the logs on the server where they were generated. This approach implies some risk and is not recommended.

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.



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.



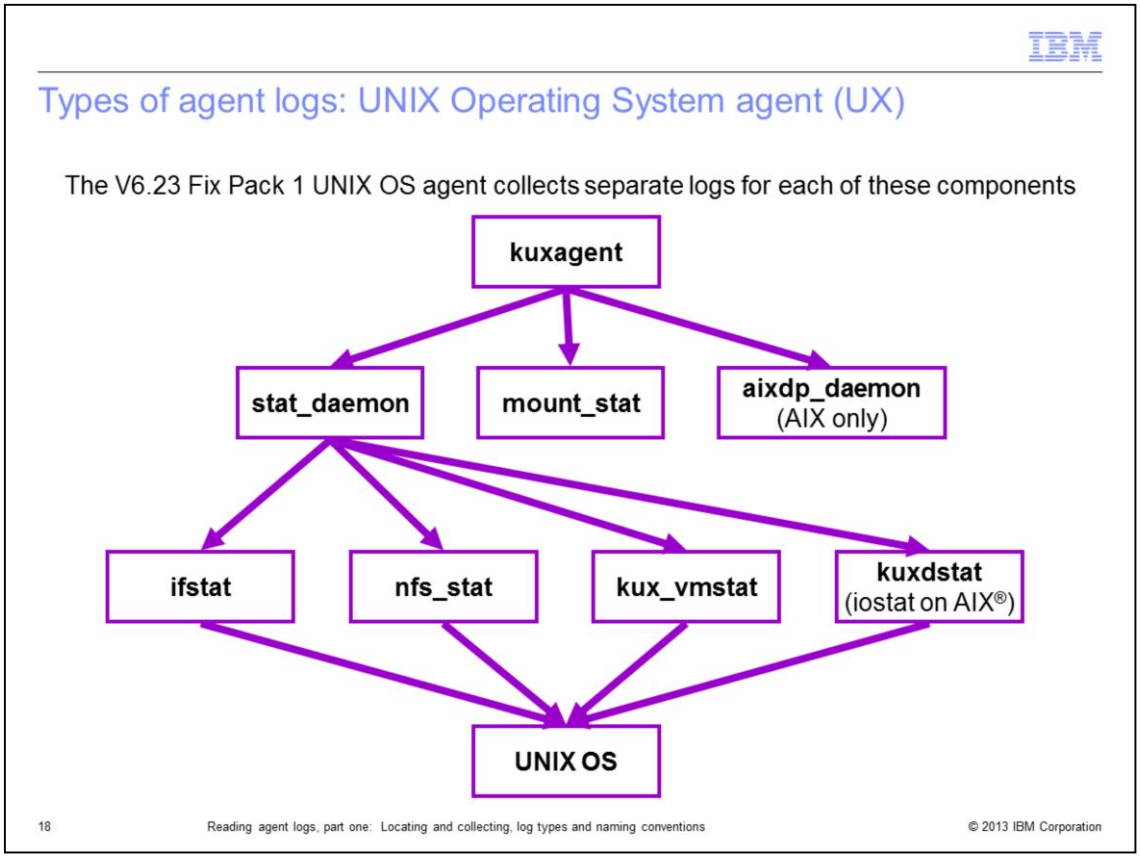
An important part of identifying the cause of agent-related problems is being able to read the logs that the various agents generate.

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.

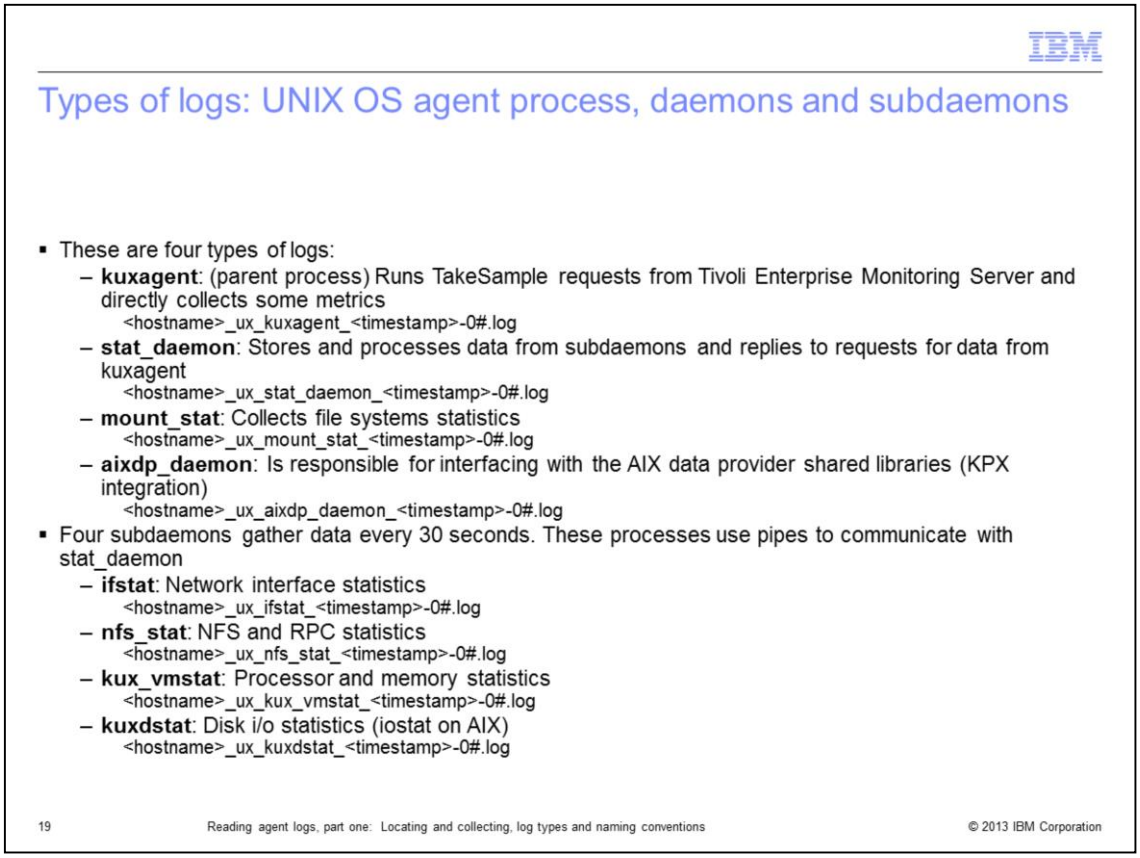
With Windows Explorer, you can sort the log files by name and that makes it easier to find names similar to those names shown in the presentation.



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.

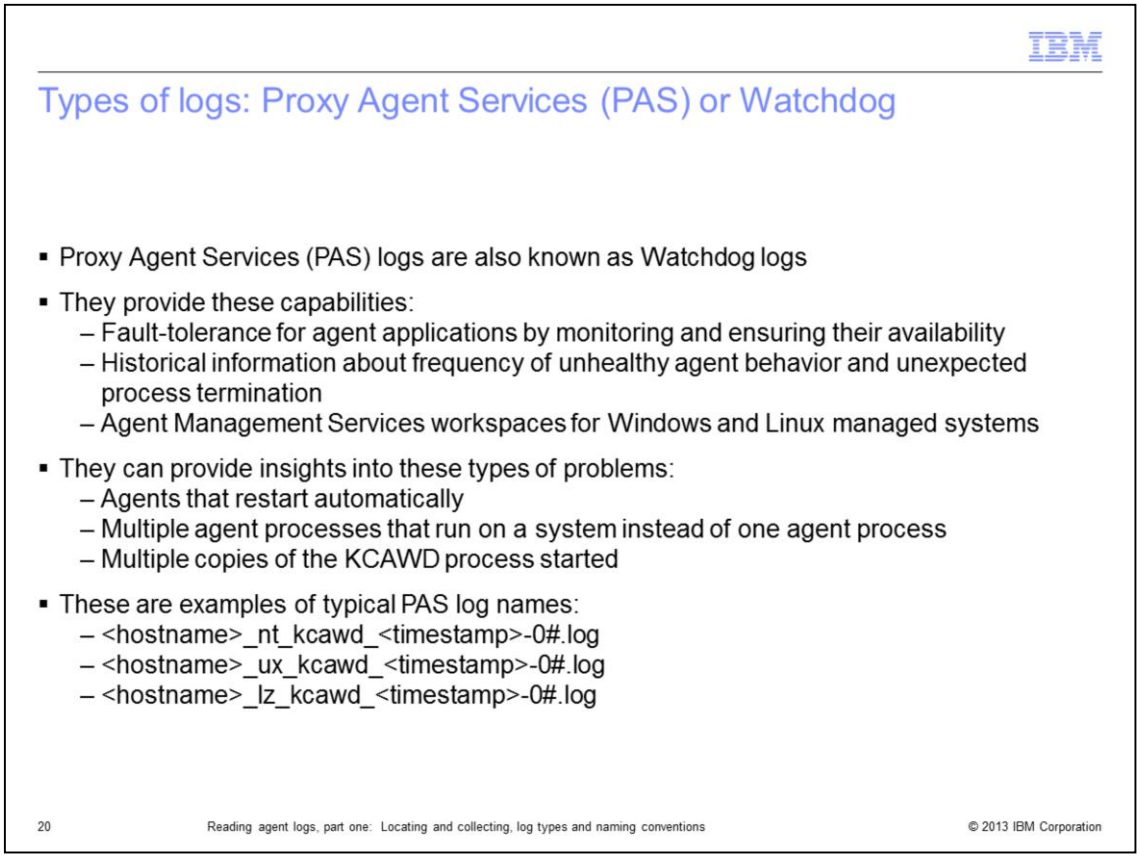


Here are the UNIX OS agent process, daemons, and subdaemons as well as the file names that they populate.

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.



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

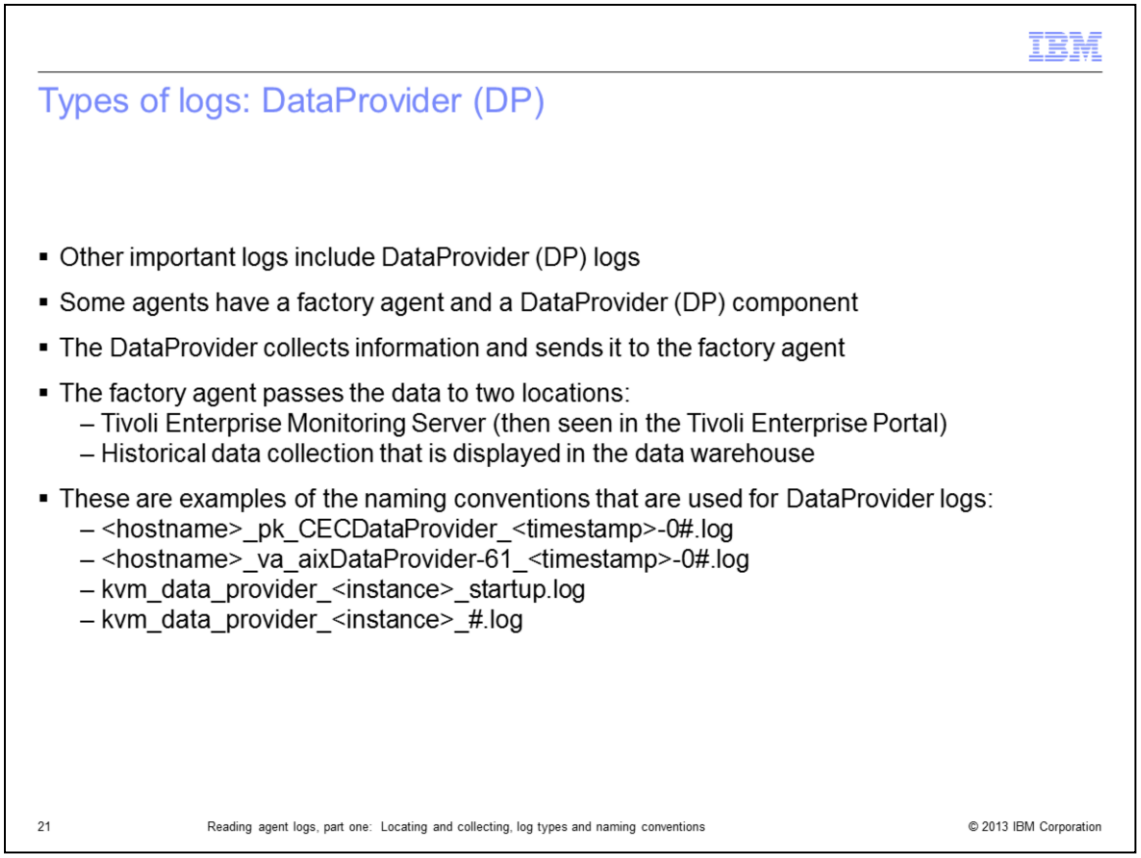
    -- Agent Management Services workspaces for Windows and Linux managed systems

- 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



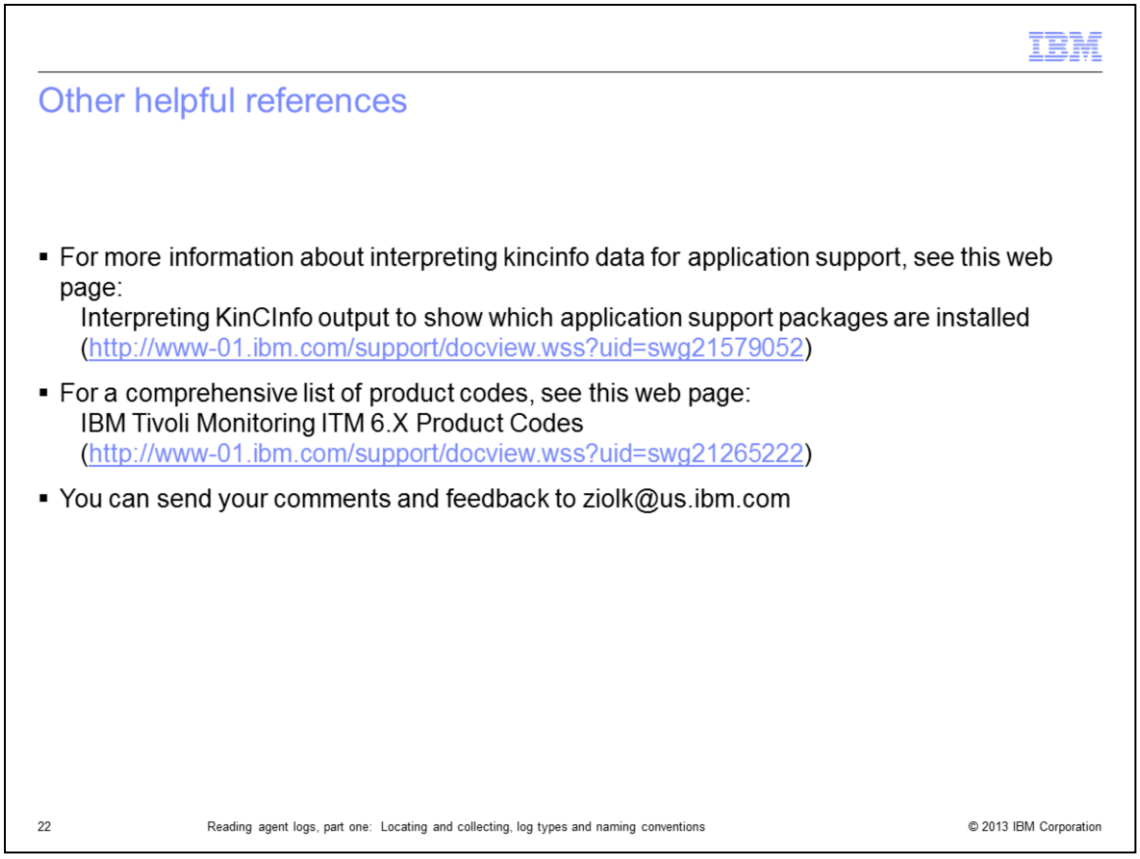
Other important logs to be aware of include DataProvider (DP) logs.

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

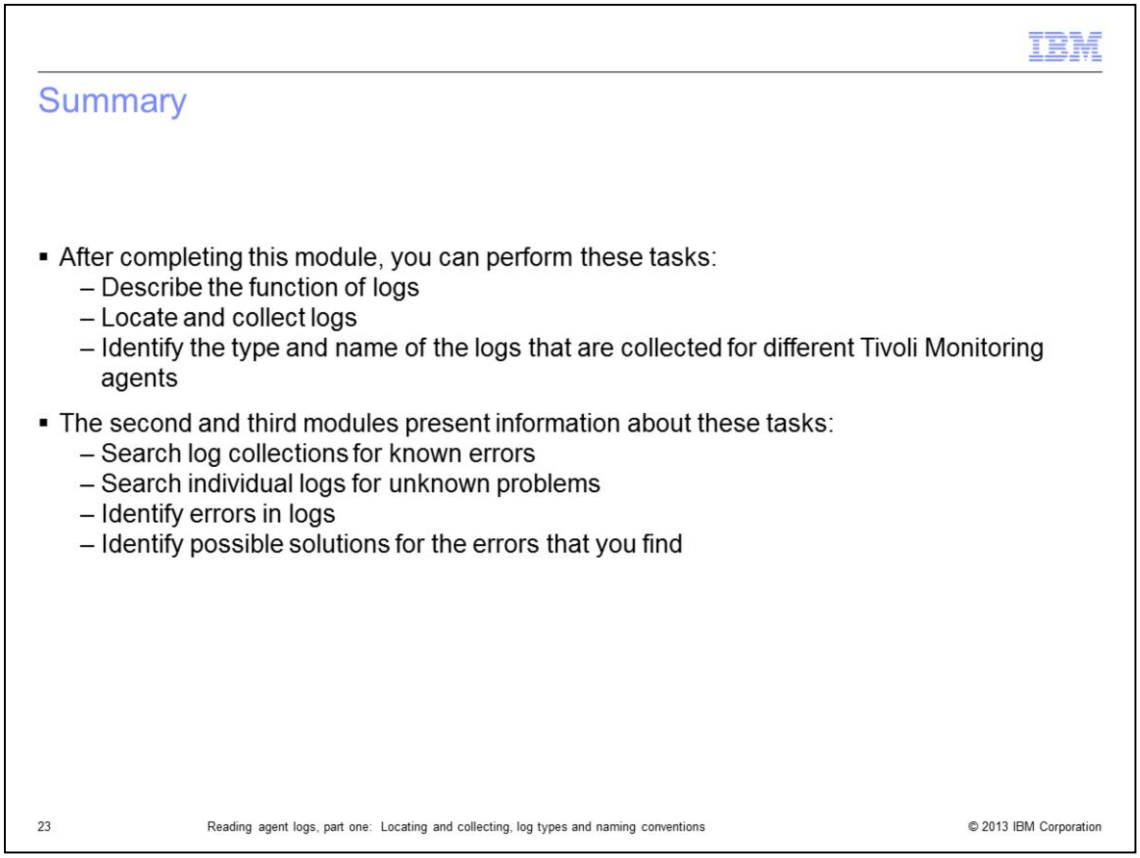
The DataProvider collects information and sends it to the factory agent.

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.



Here are a few helpful references.



- 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