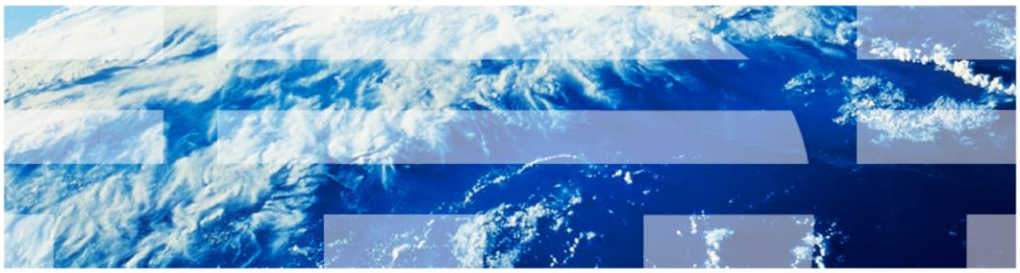
IBM

# IBM Tivoli Monitoring V6.2.3

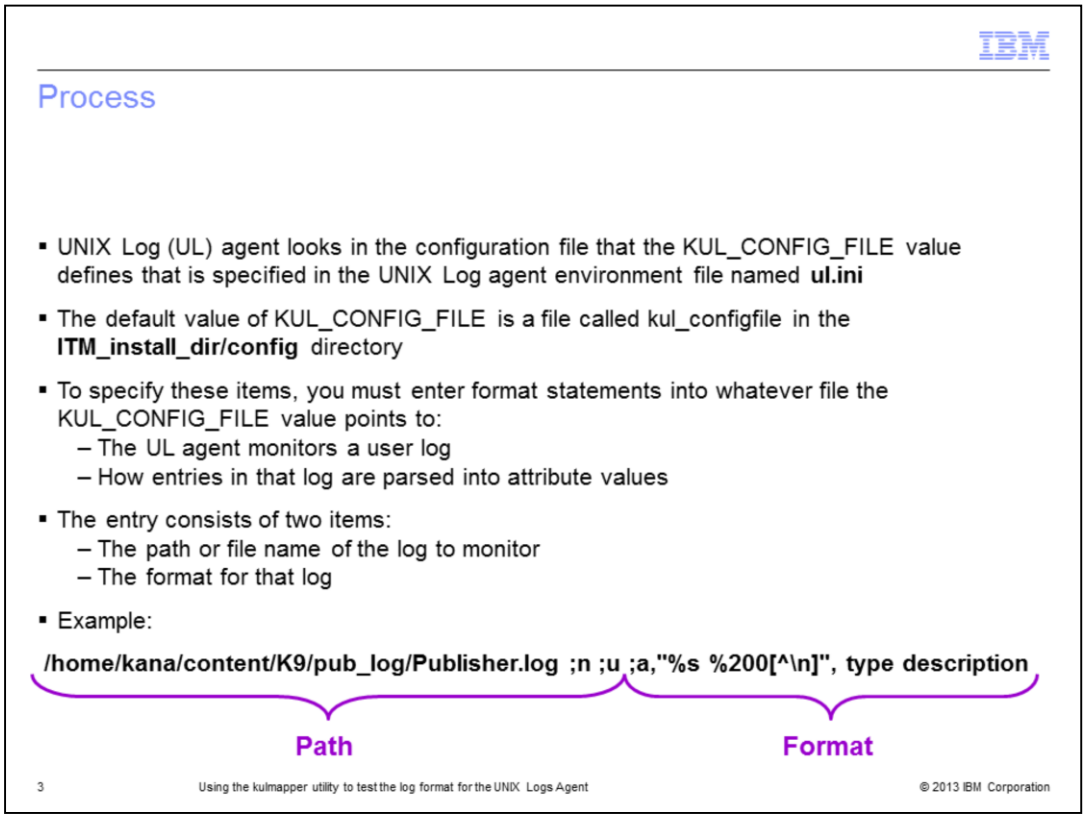
## Using the kulmapper utility to test the log format for the UNIX logs agent





IBM Tivoli® Monitoring V6.2.3, Using the kulmapper utility to test the log format for the UNIX® logs agent. In this module, you learn the steps to use kulmapper utility that is included with the UNIX Logs (UL) agent for determining format statements to parse generic user logs (GULS).


When you complete this module, you can create and test format definitions for parsing attribute values from generic user logs with the UNIX Logs Agent.

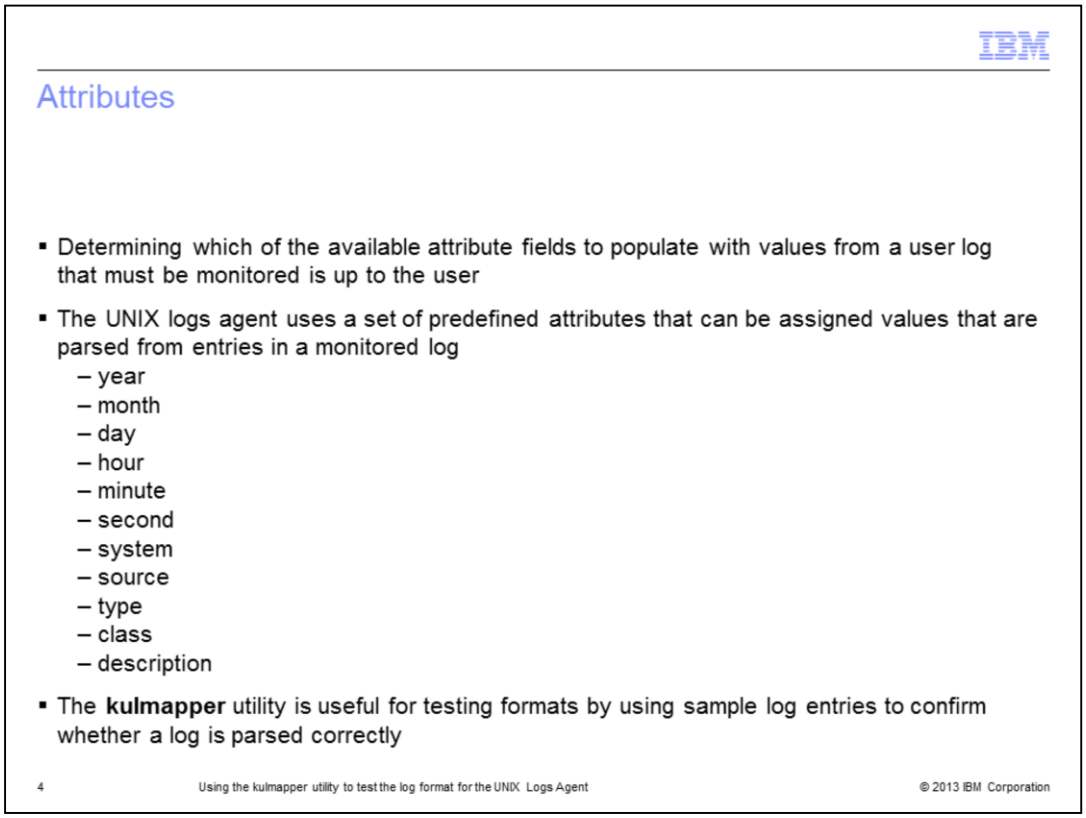



The UNIX Logs Agent uses statements in the KUL_CONFIG_FILE to determine which logs to monitor. For user logs, KUL_CONFIG_FILE provides a format statement that controls how to parse the log entries in to attribute fields.

The entry in the KUL_CONFIG_FILE consists of the **full path** and **file name** for the log to monitor. The next item is a semicolon and the letter **y** or **n** to indicate whether the tool writes debug statements when it parses the log. The next item is a second semicolon and a letter that represents the log type. For **user** logs, the value of the letter is **u**.

There is a third semicolon, followed by the letter **a**, and a comma. Double quotation marks contain the list of scan directives. After the quotation marks is a comma and a list of destination statements, which are the attribute values that the parsed data is sent to.

The **format** is the entire part of the line beginning with the **;a,** to the end of the line.




With the UNIX logs agent, values can be parsed into a limited set of attributes.

The provided kulmapper utility is used for testing formats. It can be simple or complex. Sometimes it is as simple as reading an entire log entry in to the description attribute. It can be as complex as stripping individual values from different parts of the log entry in to each of the attribute fields.

## Command syntax

- To use the kulmapper utility, create a file that contains these items:
  - Format string that is specified in the **KUL_CONFIG_FILE** as its first line
  - Sample log entries from the log file in subsequent lines
- The syntax of the command requires that you specify two items in the first line:
  1. The `-h` option specifies the Tivoli Monitoring installation directory (also referred to as CANDLEHOME)
  2. The `-l` option specifies the example log file with the format
  3. The last digit is a parameter that specifies the number of log entries to parse

  Example:

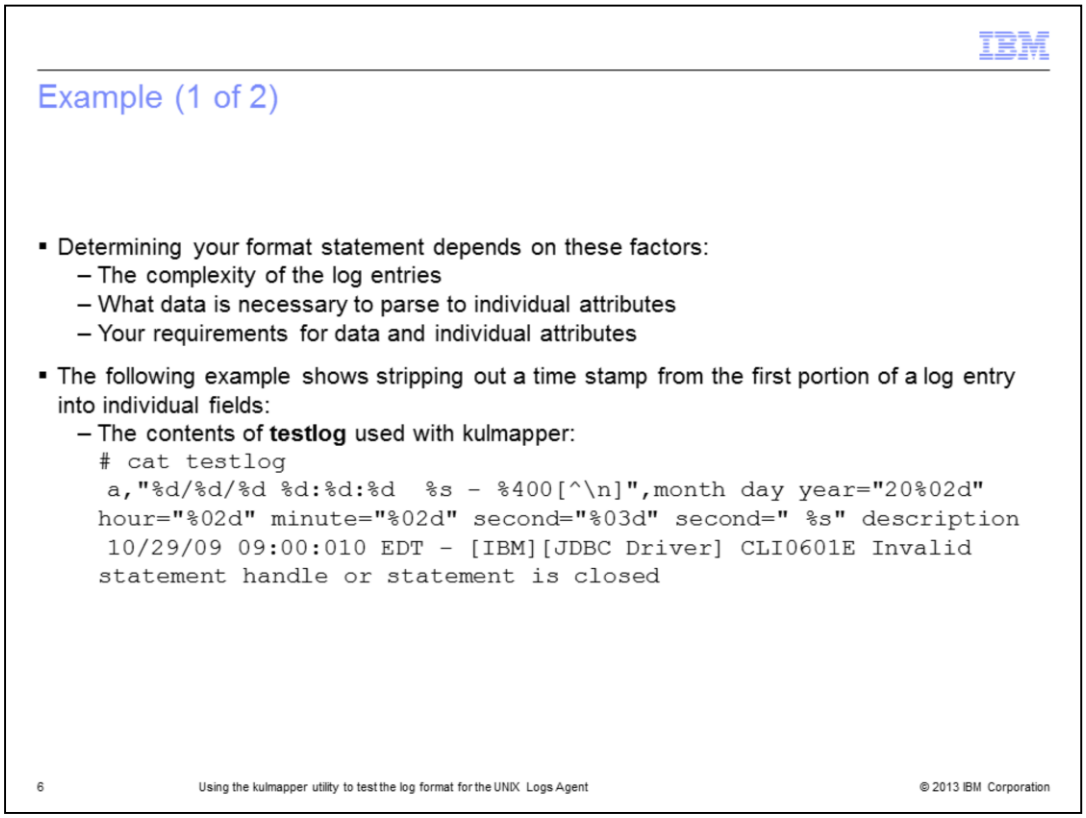
```
# ./kulmapper -h /opt/IBM/ITM -l ./testlog 1
```





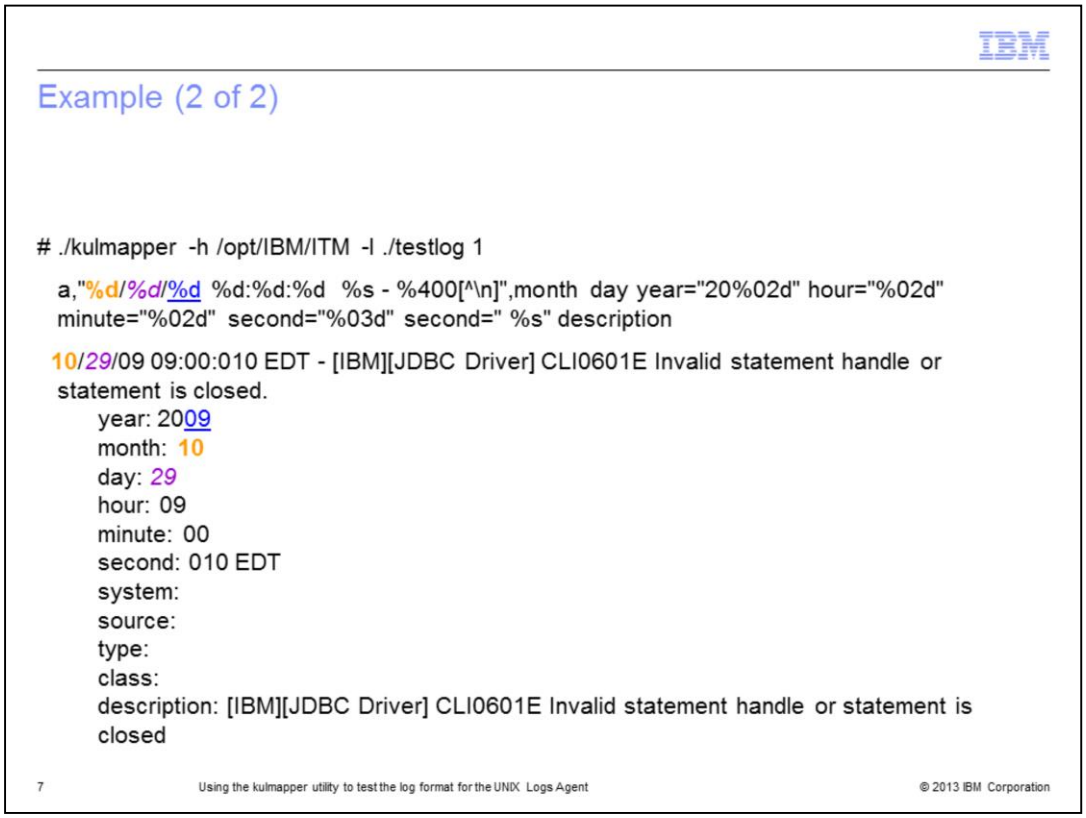
To use the kulmapper utility, create a file that contains as its first line the format string that you want to test. The rest of the file contains sample entries from the log that you want to monitor to test parsing. In the sample command syntax, the kulmapper utility reads the format from the first line of the **testlog** file and parses one more line. It parses one line because the command specifies 1 as the number of sample entries to test.

This slide shows the command syntax to run the kulmapper utility. The next slide explains the actual format statement.




As stated previously, the format statement begins with the characters **;a,** and double quotation marks that enclose the scan directives for parsing the log entry text. Then, a comma follows the scan directive and a space-separated list of attribute targets.

Here you see an example of what the **testlog** file contains. The next slide shows the output from kulmapper with the values parsed to the different attribute values.




This slide shows an example of output from kulmapper that shows the scan directives and the resulting values in each attribute field. The scan directives in the format begin with a percent sign (%). The colors, bold, italic, and underscore formats are in the slide for clarification. The code and output do not contain formatting.

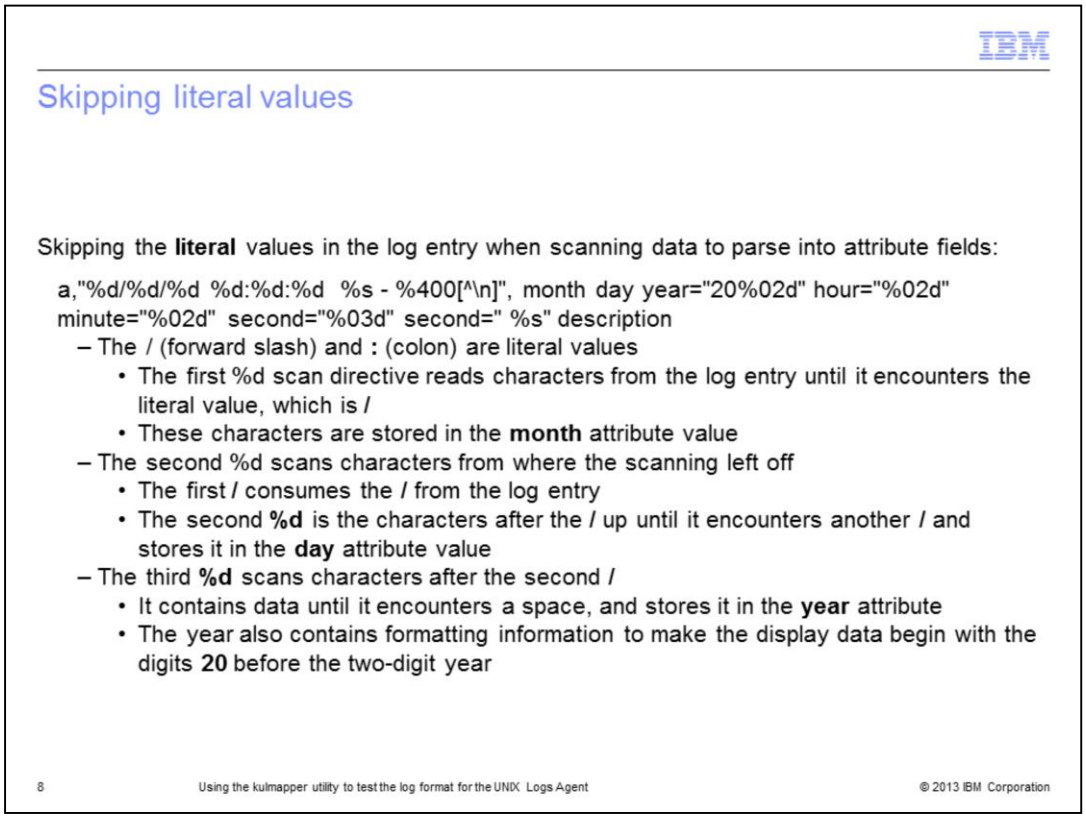
The number of scan directives that parse data from the log entry must be equal to the number of target destinations specified. The next three sentences explain which characters are copied in the example.

The first scan directive copies the characters **10** to the month field (marked in bold orange).

The second scan directive copies characters *29* to the day field (marked in italic purple).

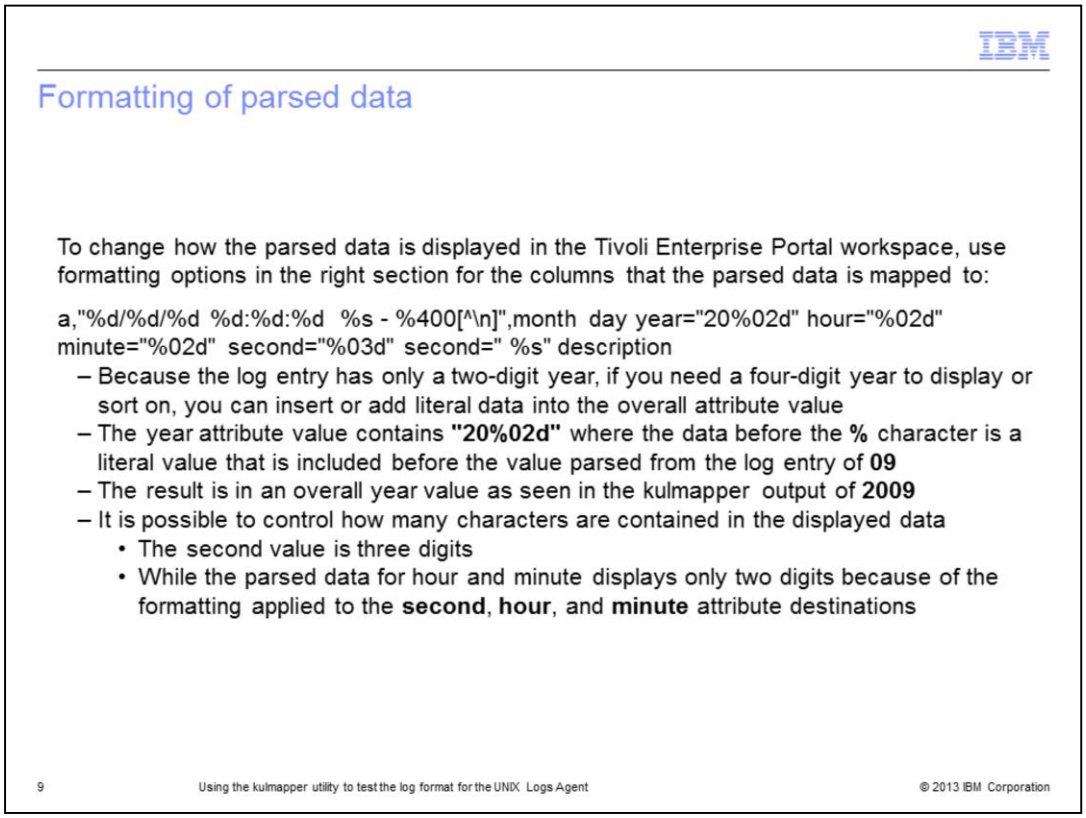
The third scan directive copies the characters 09 to the year field (marked in underscored blue).

Parsing the log entry can be complex; this example shows several useful concepts.

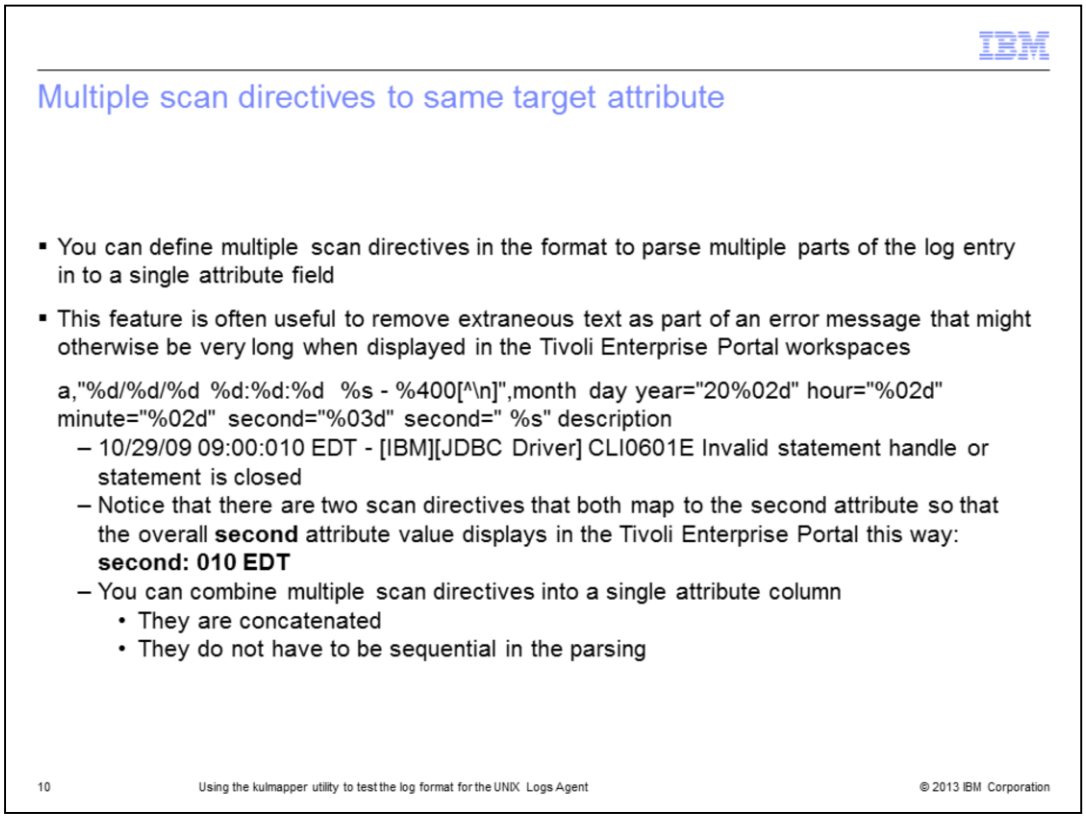



Literal values are the portions of the log entry that are specified in the format statement but not part of a scan directive.

With literal values, portions of the log entry can be used without storing that data in any attribute value sent to the Tivoli Enterprise Monitoring Server.

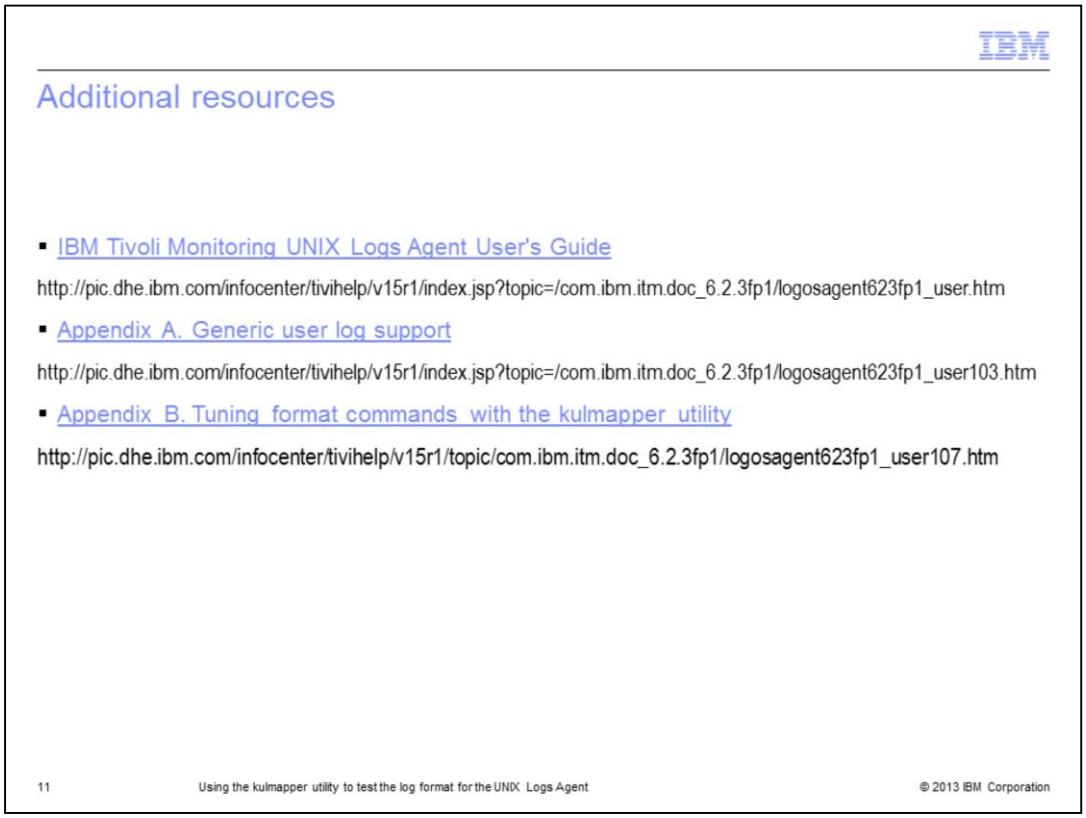



Often a monitored log does not contain the data in the same format that the resulting attribute value requires. A log can contain a two-digit year, when the resulting attribute requires a four-digit year. To control how Tivoli Enterprise Portal shows the data, use formatting options on the destinations for parsed data.




To avoid format errors, there must be the same number of scan directives as there are attribute targets to map the data to. However, you can use the same destination more than once when the tool parses a log entry.

Parsing multiple portions of a log entry and mapping the scan directives to the same attribute destination results in a concatenated overall value for the multiple scan directive results.




This lesson is not all inclusive; it does provide a beginning for you to use the kulmapper utility to test format statements that the tool uses to parse user logs with the UL agent.

After you test a format string and determine that it provides the needed results when parsing a log entry, you can use the format string in an entry in the KUL_CONFIG_FILE.

You can see more information in Appendices A and B of the *IBM Tivoli Monitoring UNIX Logs Agent User's Guide*.


Now that you completed this module, you can use the kulmapper utility to test or verify format statements to use to monitor generic user logs (GULS) with the UNIX Logs Agent.

# Trademarks, disclaimer, and copyright information