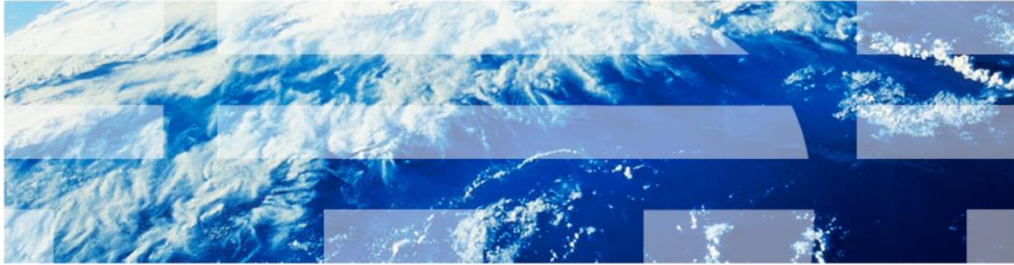


IBM Tivoli Monitoring V6.2.3

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



© 2013 IBM Corporation

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).

Objectives

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

- Use kulmapper to test log formats in the kul_configfile for the UNIX logs agent
- Format definitions that control how monitored logs are parsed into individual attribute values

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.

Process

- UNIX Log (UL) agent looks in the configuration file that the KUL_CONFIG_FILE value defines that is specified in the UNIX Log agent environment file named **ul.ini**
- The default value of KUL_CONFIG_FILE is a file called kul_configfile in the **ITM_install_dir/config** directory
- To specify these items, you must enter format statements into whatever file the KUL_CONFIG_FILE value points to:
 - The UL agent monitors a user log
 - How entries in that log are parsed into attribute values
- The entry consists of two items:
 - The path or file name of the log to monitor
 - The format for that log
- Example:

```
/home/kana/content/K9/pub_log/Publisher.log ;n ;u ;a,"%s %200[^\n]", type description
```

Path
Format

3

Using the kulmapper utility to test the log format for the UNIX Logs Agent

© 2013 IBM Corporation

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.

Attributes

- Determining which of the available attribute fields to populate with values from a user log that must be monitored is up to the user
- The UNIX logs agent uses a set of predefined attributes that can be assigned values that are parsed from entries in a monitored log
 - year
 - month
 - day
 - hour
 - minute
 - second
 - system
 - source
 - type
 - class
 - description
- The **kulmapper** utility is useful for testing formats by using sample log entries to confirm whether a log is parsed correctly

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.

Example (1 of 2)

- Determining your format statement depends on these factors:
 - The complexity of the log entries
 - What data is necessary to parse to individual attributes
 - Your requirements for data and individual attributes
- The following example shows stripping out a time stamp from the first portion of a log entry into individual fields:
 - The contents of **testlog** used with kulmapper:

```
# cat testlog
a,"%d/%d/%d %d:%d:%d %s - %400[^\n]",month day year="20%02d"
hour="%02d" minute="%02d" second="%03d" second=" %s" description
10/29/09 09:00:010 EDT - [IBM][JDBC Driver] CLI0601E Invalid
statement handle or statement is closed
```

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.

Example (2 of 2)

```
# ./kulmapper -h /opt/IBM/ITM -I ./testlog 1
a,"%d/%d/%d %d:%d:%d %s - %400[^\n]",month day year="20%02d" hour="%02d"
minute="%02d" second="%03d" second=" %s" description
10/29/09 09:00:010 EDT - [IBM][JDBC Driver] CLI0601E Invalid statement handle or
statement is closed.
  year: 2009
  month: 10
  day: 29
  hour: 09
  minute: 00
  second: 010 EDT
  system:
  source:
  type:
  class:
  description: [IBM][JDBC Driver] CLI0601E Invalid statement handle or statement is
closed
```

7

Using the kulmapper utility to test the log format for the UNIX Logs Agent

© 2013 IBM Corporation

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.

Skipping literal values

Skipping the **literal** values in the log entry when scanning data to parse into attribute fields:

```
a,"%d/%d/%d %d:%d:%d %s - %400[^\n]", month day year="20%02d" hour="%02d"
minute="%02d" second="%03d" second=" %s" description
```

- The / (forward slash) and : (colon) are literal values
 - The first %d scan directive reads characters from the log entry until it encounters the literal value, which is /
 - These characters are stored in the **month** attribute value
- The second %d scans characters from where the scanning left off
 - The first / consumes the / from the log entry
 - The second %d is the characters after the / up until it encounters another / and stores it in the **day** attribute value
- The third %d scans characters after the second /
 - It contains data until it encounters a space, and stores it in the **year** attribute
 - The year also contains formatting information to make the display data begin with the digits **20** before the two-digit year

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.

Formatting of parsed data

To change how the parsed data is displayed in the Tivoli Enterprise Portal workspace, use formatting options in the right section for the columns that the parsed data is mapped to:

```
a,"%d/%d/%d %d:%d:%d %s - %400[^\n]",month day year="20%02d" hour="%02d"
minute="%02d" second="%03d" second=" %s" description
```

- Because the log entry has only a two-digit year, if you need a four-digit year to display or sort on, you can insert or add literal data into the overall attribute value
- The year attribute value contains "**20%02d**" where the data before the % character is a literal value that is included before the value parsed from the log entry of **09**
- The result is in an overall year value as seen in the kulmapper output of **2009**
- It is possible to control how many characters are contained in the displayed data
 - The second value is three digits
 - While the parsed data for hour and minute displays only two digits because of the formatting applied to the **second**, **hour**, and **minute** attribute destinations

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.

Multiple scan directives to same target attribute

- You can define multiple scan directives in the format to parse multiple parts of the log entry in to a single attribute field
- This feature is often useful to remove extraneous text as part of an error message that might otherwise be very long when displayed in the Tivoli Enterprise Portal workspaces

```
a,"%d/%d/%d %d:%d:%d %s - %400[^\n]",month day year="20%02d" hour="%02d"
minute="%02d" second="%03d" second=" %s" description
```

```
– 10/29/09 09:00:010 EDT - [IBM][JDBC Driver] CLI0601E Invalid statement handle or
statement is closed
```

```
– Notice that there are two scan directives that both map to the second attribute so that
the overall second attribute value displays in the Tivoli Enterprise Portal this way:
```

```
second: 010 EDT
```

- You can combine multiple scan directives into a single attribute column
 - They are concatenated
 - They do not have to be sequential in the parsing

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.

Additional resources

- [IBM Tivoli Monitoring UNIX Logs Agent User's Guide](#)

http://pic.dhe.ibm.com/infocenter/tivihelp/v15r1/index.jsp?topic=/com.ibm.itm.doc_6.2.3fp1/logosagent623fp1_user.htm

- [Appendix A. Generic user log support](#)

http://pic.dhe.ibm.com/infocenter/tivihelp/v15r1/index.jsp?topic=/com.ibm.itm.doc_6.2.3fp1/logosagent623fp1_user103.htm

- [Appendix B. Tuning format commands with the kulmapper utility](#)

http://pic.dhe.ibm.com/infocenter/tivihelp/v15r1/topic/com.ibm.itm.doc_6.2.3fp1/logosagent623fp1_user107.htm

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*.

Summary

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

- Use `kulmapper` to test log formats in the `kul_configfile` for the UNIX Logs Agent
- Format definitions that control how monitored logs are parsed into individual attribute values

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

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>

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 2013. All rights reserved.