

In this module, you learn the main steps in the configuration of log file agent on  $\text{UNIX}^{\texttt{R}}$  and  $\text{Linux}^{\texttt{R}}$ .

	IBM
Assumptions	
<ul> <li>Before you proceed, you must have these prerequisites in place:         <ul> <li>Basic administration skills on UNIX and Linux</li> <li>Knowledge of Tivoli<sup>®</sup> Monitoring</li> <li>A Tivoli Monitoring environment that includes Tivoli Monitoring Enterprise Server, Tiv Portal Server, a Portal desktop, and Log File Agent</li> <li>Knowledge of regular expressions</li> </ul> </li> </ul>	oli Monitoring
2 Configure log file agent on UNIX and Linux	© 2014 IBM Corporation

The expectation is that you have basic administration skills on UNIX and Linux and knowledge of Tivoli Monitoring. You also need to have a functioning Tivoli Monitoring environment that includes Tivoli Enterprise Monitoring Server, Tivoli Enterprise Portal Server, Tivoli Portal client, and Log File Agent.

Log File Agent uses regular expressions to parse logs; hence this module requires basic knowledge of regular expressions.

## **Objectives**

3

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

- Configure Log File Agent
- View data that is obtained by Log File Agent on Tivoli Enterprise Portal in order to monitor custom logs

When you complete this module, you can configure Log File Agent and connect to Tivoli Enterprise Portal to view data that is collected by the monitoring agent.

Configure log file agent on UNIX and Linux

IBM

© 2014 IBM Corporation

						IBM
Conf	ïguring Log File Agent – proc	cess steps				
1. Lo	og in to the UNIX/Linux system					
2. Ri ar in:	un \$CANDLEHOME/bin/cinfo -i nd ensure that Log File Agent is stalled	r	Tivoli E aix523 aix526 tpj	Nterprise Version: Version: Version:	-supplied JRE 07.04.02.00 07.04.02.00 07.05.00.00	
		kf	IBM Ecli aix533	pse Help : Version:	Server 06.30.02.00	
	Log File Agent	10	Tivoli L aix526 tms tps tpw	og File A Version: Version: Version: Version:	gent 06.30.00.00 06.30.00.00 06.30.00.00 06.30.00.00	
		lz	Monitori tms tps tpw	ng Agent Version: Version: Version:	for Linux OS 06.30.02.00 06.30.02.00 06.30.02.00	
4	Configu	ure log file agent on UNIX an	d Linux			© 2014 IBM Corporation

Run the command "cinfo -i" to see a list of the Tivoli Monitoring components that are installed on the system. Make sure that Log File Agent is installed. The product code of Log File Agent is "lo".

Configuring Log File Agent		
Configure Log File Agent using the <b>\$CANDLEHOME/bin/itmcmd config -A lo</b> command	<pre>[tapsaix637:root:/opt/IBM/ITM/bin:] ./itmcmd config -A lo Agent configuration statted Enter instance name (default is: ): inst2 Edit "Juoil Log File Agent" settings? [ ="Yes, 2=No ] (default is: 1): Edit 'Log File Adapter Configuration' settings? [ ]=Yes, 2=No ] (default is: /opt/IBM/ITM/config/Int2.int): Format File (default is: /opt/IBM/ITM/config/Int2.int): Send ITM Ferret [ ]=Yes, 2=No ] (default is: 2): 2 Send ITM Ferret [ ]=Yes, 2=No [ Send ITM Ferret [ ]=Yes, 2=No, 3=Use ] Auromatically initialite UNIX syslog [ ]=Yes, 2=No, 3=Use .conf file value ] Frocess File Adapter Global Settings' settings? [ ]=Yes, 7=Use .conf file value ] Frocess Findium CPU percentage (default is: 10): Configuration file autodiscovery directory (default is: %(CANDLF_HOME)/confi Will this agent connect to a TEMS? [ ]=YES, 2=NO ] (Default is: 2): 1 Network Protocol [ 1p, sna, 1p.phpe, 1p.spipe, 1p6, 1p6.phpe or 1p6.spipe] (D</pre>	<pre>1): (default is: 2): 2 s: 1): 1 e ] (default is: 7): g/lo): efault is: none):</pre>
	<pre>KCIIN0530W 8-( Value entered is not allowed )-8 Network Protocol [ip, sna, ip.pipe, ip.spipe, ip6, ip6.pipe or ip6.spipe] (D</pre>	efault is: none): ip.pipe
	Now choose the next protocol from one of these: - ip - sna - ip.spipe - ip6. - ip6.pipe - ip6.pipe - 0 for none Network Frotocol 2 (Default is: 0): TEMS Host Name for IPv4 (Default is: tapsaix637): IF.PTFF Fort Number (Default is: 1818): Enter name of KDC_PARTITION (Default is: null): Configure connection for a secondary TEMS? [1=YES, 2=NO] (Default is: 2): Enter onneal Primary Network Name or 0 for "none" (Default is: 2):	
	Agent configuration completed As a reminder, you should restart appropriate instance(s) for new configurat [tapsaix65/ricot/opt/IMW/ITM/bin]]	ion settings to take effect.
5 Confi	igure log file agent on UNIX and Linux	© 2014 IBM Corporation

Configuring Log File Agent requires several parameters. Log File Agent is an instancebased agent. So the first thing that is required during the configuration is the instance name.

When the agent is configured for the first time, you must select 'Yes' for both Edit "Tivoli Log File Agent" settings and Edit 'Log File Adapter Configuration' settings.

You also need to provide the complete path, not the relative path, to the configuration and format files. The configuration and format files must be created before you configure the agent. These files are explained later in the presentation.

Depending on where you want to send events, select either the "Send EIF Events to OMNIbus" or "Send ITM Events" option. If you want to monitor syslogs, choose Yes for the option "Automatically initialize UNIX syslog".

Beginning with V6.2.3 Fix Pack 2, Log File Agent has an auto-discovery directory to which many pairs of configuration and format files can be added. Log File Agent checks this directory periodically for any changes to these files and starts monitoring the new log sources that are specified in the configuration files. In Tivoli Enterprise Portal, these log sources appear as sub nodes under the instance.

The remaining configuration options are related to Tivoli Enterprise Monitoring Server communication. Your answers to these questions are based on your environment setup.

\_\_\_\_

	IBM
Creating the configuration file	
<ul> <li>File extension is .conf</li> </ul>	
<ul> <li>Specifies the log sources</li> </ul>	
<ul> <li>Contains configuration options and filters</li> </ul>	
Is read by the agent when it starts and monitored for changes every 60 seconds thereafter	
<ul> <li>The only required parameter is the log being monitored, which is specified as follows: LogSources=/var/log/application.log</li> </ul>	
<ul> <li>Other common parameters:</li> <li>NumEventsToCatchUp</li> <li>UnmatchedLog</li> </ul>	
6 Configure log file agent on UNIX and Linux	© 2014 IBM Corporation

Tivoli Log File Agent uses a configuration file that specifies the log sources. It also contains configuration options and filters. The configuration file is read by the agent when it starts and is monitored for changes to its timestamp every 60 seconds thereafter.

The only required parameter is the path to the log being monitored.

An optional parameter is NumEventsToCatchUp, which specifies the event in the log that the agent starts with. A value of 0 makes the log start with the next event. This is the default value. When set to -1, the agent saves its place in the file that is being monitored. It saves its place so that, when the agent is stopped and later restarted, it can process any events that were written to the log while it was stopped.

If set to a positive integer *n* the agent starts with the *n*th event from the most current event in the log. Note that for text files, only values 0 and -1 apply.

Another optional parameter is UnmatchLog. This parameter specifies a file in which to log discarded events that cannot be parsed into an event class by the agent.

The User's Guide has a description of all the parameters that can be included in the configuration file.

		IBM
Creating the format file		
<ul> <li>File extension is .fmt</li> <li>The format file specifies the regular ex</li> <li>Example of a format file:</li> </ul>	pression that is used to parse the events in the log fi	ile
REGEX REExample Error: (.*) msg		
<ul> <li>Snippet from an example log file:</li> </ul>		
Error: disk failure Error: out of memory WARNING: incorrect login		
7	Configure log file agent on UNIX and Linux	© 2014 IBM Corporation

The format file specifies the regular expression that is used to parse the events in the log file.

Shown here is an example of a format file and a snippet from the log that it reads. This format file generates an event for each line that begins with "Error:" and ignores the line that begins with "Warning:". So the regular expression begins with the string "Error:" and then includes a sub expression. The sub expression is denoted by parentheses and it is the input text for the "msg" slot.

	IBM
Start Log File Agent	
<ul> <li>Once configured, start the agent with this command: \$CANDLEHOME/bin/itmcmd agent -o <instance name=""> start lo</instance></li> </ul>	
8 Configure log file agent on UNIX and Linux	© 2014 IBM Corporation

Once configured, start the agent with the command shown here.

		IBM
Summary		
Now that you completed this module, you	can perform these tasks:	
<ul> <li>View data that is obtained by log file age</li> </ul>	ent on Tivoli Enterprise Portal	
Use the data to monitor the logs		
9	Configure log file agent on UNIX and Linux	© 2014 IBM Corporation

Now that you completed this module, you can view data that is obtained by the log file agent on Tivoli Enterprise Portal. And you can use the data to monitor the logs.

## 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" at http://www.ibm.com/legal/copytrade.shtml

Linux is a registered trademark of Linus Torvalds 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 FOM 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.

10

Configure log file agent on UNIX and Linux

© 2014 IBM Corporation