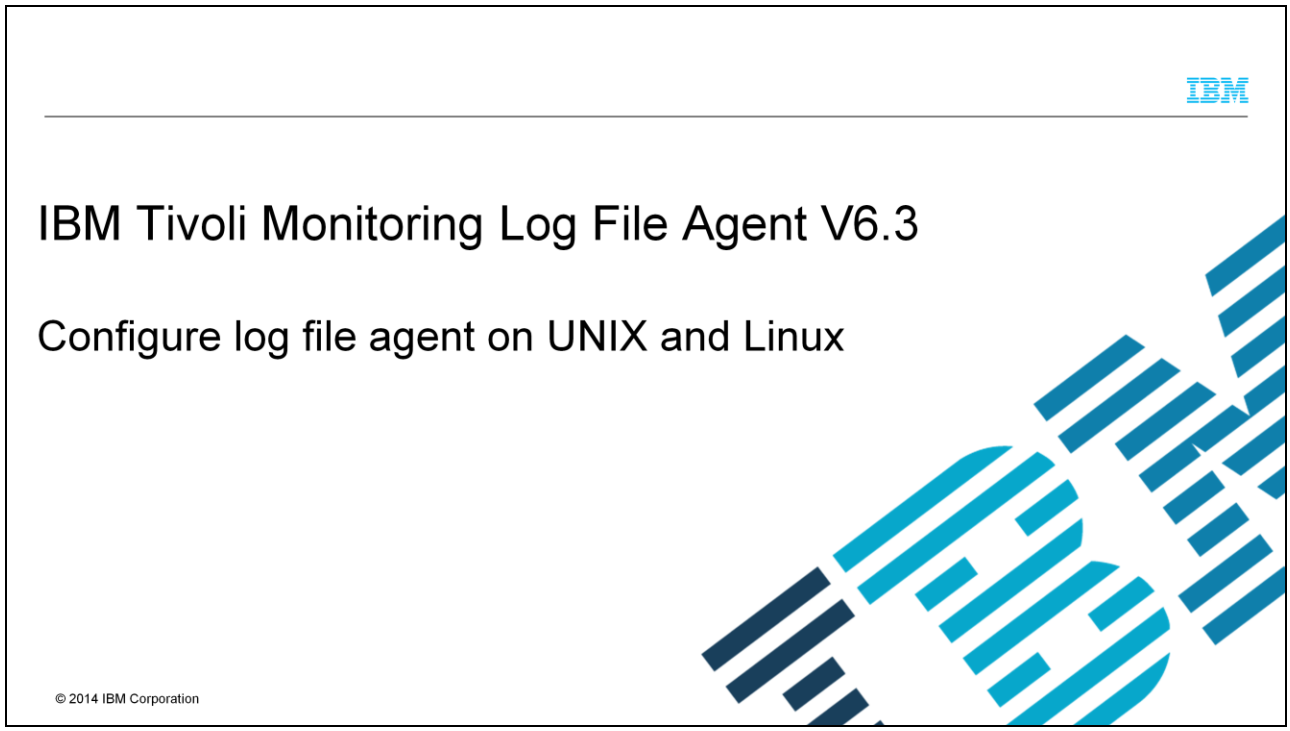

In this module, you learn the main steps in the configuration of log file agent on UNIX® and Linux®.

Assumptions

- Before you proceed, you must have these prerequisites in place:
  - Basic administration skills on UNIX and Linux
  - Knowledge of Tivoli® Monitoring
  - A Tivoli Monitoring environment that includes Tivoli Monitoring Enterprise Server, Tivoli Monitoring Portal Server, a Portal desktop, and Log File Agent
  - Knowledge of regular expressions

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

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.

Configuring Log File Agent – process steps

1. Log in to the UNIX/Linux system
2. Run $CANDLEHOME/bin/cinfo -i and ensure that Log File Agent is installed

Log File Agent →

```
jr      Tivoli Enterprise-supplied JRE
         aix523  Version: 07.04.02.00
         aix526  Version: 07.04.02.00
         tpj     Version: 07.05.00.00

kf      IBM Eclipse Help Server
         aix533  Version: 06.30.02.00

lo      Tivoli Log File Agent
         aix526  Version: 06.30.00.00
         tms     Version: 06.30.00.00
         tps     Version: 06.30.00.00
         tpw     Version: 06.30.00.00

lz      Monitoring Agent for Linux OS
         tms     Version: 06.30.02.00
         tps     Version: 06.30.02.00
         tpw     Version: 06.30.02.00
```


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 **$CANDLEHOME/bin/itmcmd config -A lo** command

```
[tapsaix637:root:/opt/IBM/ITM/bin:] ./itmcmd config -A lo
Agent configuration started...
Enter instance name (default is: ): inst2
Edit "Tivoli Log File Agent" settings? [ 1=Yes, 2=No ] (default is: 1):
Edit 'Log File Adapter Configuration' settings? [ 1=Yes, 2=No ] (default is: 1):
Conf file (default is: /opt/IBM/ITM/config/int2.conf):
Format File (default is: /opt/IBM/ITM/config/int2.fmt):
Send EIF Events to OMNIbus [ 1=Yes, 2=No ] (default is: 2): 2
Send ITM Events [ 1=Yes, 2=No ] (default is: 1): 1
Automatically initialize UNIX syslog [ 1=Yes, 2=No, 3=Use .conf file value ] (default is: 2): 2
Edit 'Log File Adapter Global Settings' settings? [ 1=Yes, 2=No ] (default is: 1): 1
Process Priority Class [ 1=A, 2=B, 3=C, 4=D, 5=E, 6=F, 7=Use .conf file value ] (default is: 7):
Process maximum CPU percentage (default is: 100):
Configuration file autodiscovery directory (default is: ${CANDLE_HOME}/config/lo):

Will this agent connect to a TEMS? [1=YES, 2=NO] (Default is: 2): 1

Network Protocol [ip, sna, ip.pipe, ip.spipe, ip6, ip6.pipe or ip6.spipe] (Default is: none):
************************************************
KCIIN0530W 8-( Value entered is not allowed )-8
************************************************

Network Protocol [ip, sna, ip.pipe, ip.spipe, ip6, ip6.pipe or ip6.spipe] (Default is: none): ip.pipe

     Now choose the next protocol from one of these:
     - ip
     - sna
     - ip.spipe
     - ip6
     - ip6.pipe
     - ip6.spipe
     - 0 for none
Network Protocol 2 (Default is: 0):
TEMS Host Name for IPv4 (Default is: tapsaix637):
IP.PIPE Port Number (Default is: 1918):
Enter name of KDC_PARTITION (Default is: null):

Configure connection for a secondary TEMS? [1=YES, 2=NO] (Default is: 2):
Enter Optional Primary Network Name or 0 for "none" (Default is: 0):
Agent configuration completed...
As a reminder, you should restart appropriate instance(s) for new configuration settings to take effect.
[tapsaix637:root:/opt/IBM/ITM/bin:]
```

5 Configure log file agent on UNIX and Linux

Configuring Log File Agent requires several parameters. Log File Agent is an instance-based 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.

Creating the configuration file

- File extension is .conf
- Specifies the log sources
- Contains configuration options and filters
- Is read by the agent when it starts and monitored for changes every 60 seconds thereafter
- The only required parameter is the log being monitored, which is specified as follows:
  LogSources=/var/log/application.log
- Other common parameters:
  - NumEventsToCatchUp
  - UnmatchedLog

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.

Creating the format file

- File extension is .fmt
- The format file specifies the regular expression that is used to parse the events in the log file
- Example of a format file:

```
REGEX REExample
Error: (.*)
msg
```

- Snippet from an example log file:

```
Error: disk failure
Error: out of memory
WARNING: incorrect login
```


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.

Start Log File Agent

- Once configured, start the agent with this command:
  $CANDLEHOME/bin/itmcmd agent -o <instance name> start lo

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

Summary

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

- View data that is obtained by log file agent on Tivoli Enterprise Portal
- Use the data to monitor the logs

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