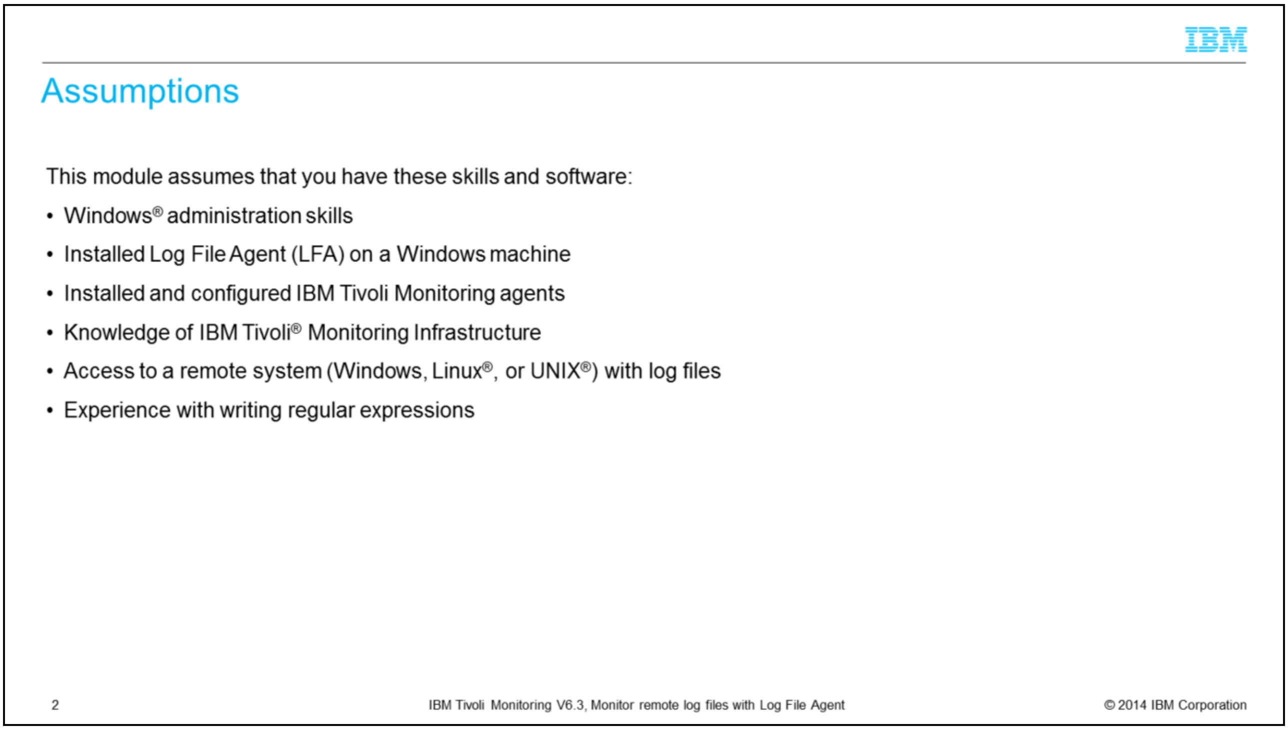
IBM Tivoli Monitoring V6.3

Monitor remote log files with Log File Agent

This module shows the steps to create a Log File Agent instance for remote monitoring. Use the remote monitoring feature in Log File Agent to monitor a log file on a remote system.

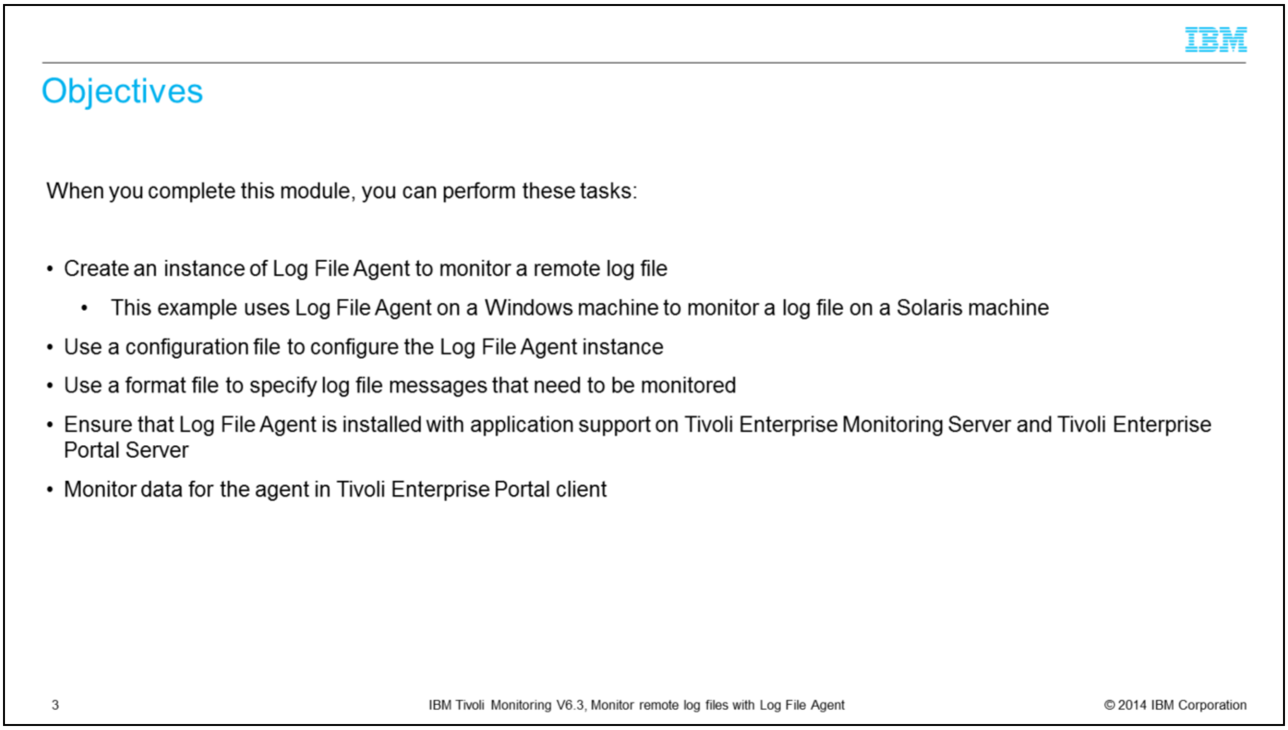


Assumptions

This module assumes that you have these skills and software:

- Windows® administration skills
- Installed Log File Agent (LFA) on a Windows machine
- Installed and configured IBM Tivoli Monitoring agents
- Knowledge of IBM Tivoli® Monitoring Infrastructure
- Access to a remote system (Windows, Linux®, or UNIX®) with log files
- Experience with writing regular expressions

This module assumes that you have Windows administration skills. Log File Agent version 6.3 must be installed on a Windows system. You need to have experience with the installation and configuration of IBM Tivoli Monitoring agents and be familiar with IBM Tivoli Monitoring Infrastructure. Technical skills with writing regular expressions are beneficial.



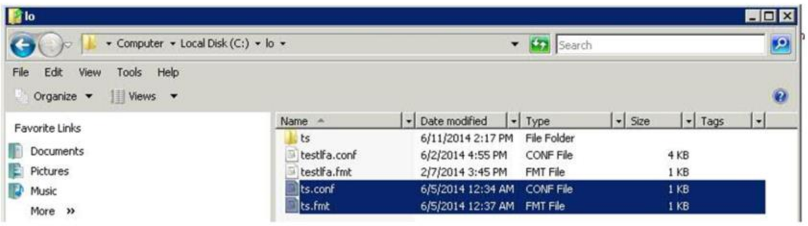
Objectives

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

- Create an instance of Log File Agent to monitor a remote log file
  - This example uses Log File Agent on a Windows machine to monitor a log file on a Solaris machine
- Use a configuration file to configure the Log File Agent instance
- Use a format file to specify log file messages that need to be monitored
- Ensure that Log File Agent is installed with application support on Tivoli Enterprise Monitoring Server and Tivoli Enterprise Portal Server
- Monitor data for the agent in Tivoli Enterprise Portal client

When you complete this module, you can create a new instance of Log File Agent that can be used to monitor a log file on a remote system. You will learn how to define configuration and format files in order to set up remote log file monitoring. You will configure the instance, add application support, and start monitoring the data for the agent in the Tivoli Enterprise Portal client.

Configuration file and format file

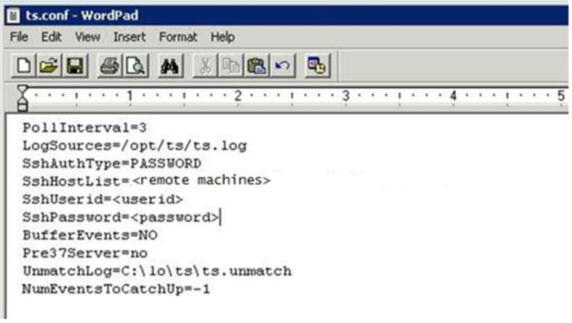


Name	Date modified	Type	Size	Tags
ts	6/11/2014 2:17 PM	File Folder		
testlfa.conf	6/2/2014 4:55 PM	CONF File	4 KB	
testlfa.fmt	2/7/2014 3:45 PM	FMT File	1 KB	
ts.conf	6/5/2014 12:34 AM	CONF File	1 KB	
ts.fmt	6/5/2014 12:37 AM	FMT File	1 KB	

- Log File Agent uses a configuration file that contains configuration options and filters
  - This example uses the configuration file **ts.conf**
- Log File Agent uses a regular expression that is specified in the format file to look up messages in the log files
  - This example uses format file **ts.fmt**

The configuration and format files are two important files that are required by any Log File Agent instance. In this example, these files reside in C:\lo.

Configuration file



```
PollInterval=3
LogSources=/opt/ts/ts.log
SshAuthType=PASSWORD
SshHostList=<remote machines>
SshUserid=<userid>
SshPassword=<password>
BufferEvents=NO
Pre37Server=no
UnmatchLog=C:\lo\ts\ts.unmatch
NumEventsToCatchUp=-1
```

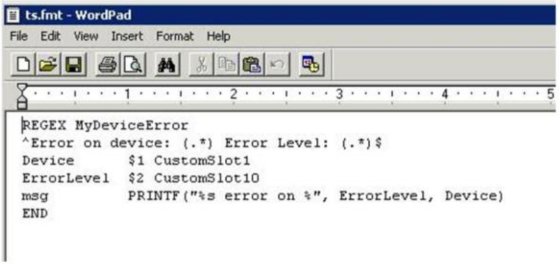
- **C:\lo\ts.conf** contains the configuration values for the Log File Agent instance
- For remote log file monitoring, the SshAuthType parameter determines which other configuration parameters need to be specified
  - A value of either PASSWORD or PUBLICKEY needs to be specified
  - In this example, PASSWORD was specified
- The LogSources parameter specifies the log files to be monitored on the remote machine

The configuration file can be located in a different directory.

The value for the SshHostList parameter is a list of remote machines. All of the other parameters in the configuration file can have only one value, which is applied to all of the remote machines specified in the SshHostList parameter.

In this example, the remote machine that is being monitored is a Solaris machine. The SshUserid and SshPassword parameters need to be provided in order to log onto that machine.

Format file



```
REGEX MyDeviceError
^Error on device: (.*) Error Level: (.*)$
Device      $1 CustomSlot1
ErrorLevel  $2 CustomSlot10
msg         PRINTF("%s error on %", ErrorLevel, Device)
END
```

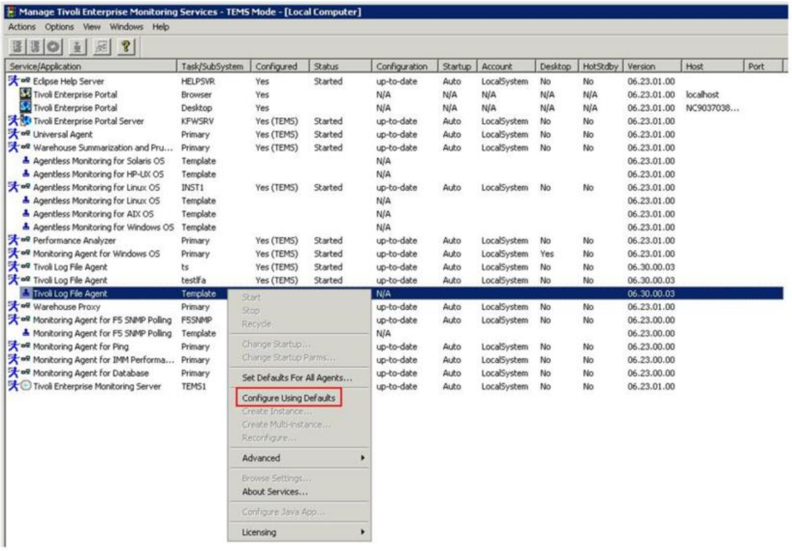
- The **C:\lo\ts.fmt** file contains the regular expression that is used as a look-up for messages in log files
- Format files can define multiple attribute groups with multiple regular expressions
- Regular expression-filtering support is provided by the International Components for Unicode (ICU) libraries
  - For more information, see: http://userguide.icu-project.org/strings/regexp

The format file can exist in a different directory.

The regular expression syntax that you use to create patterns to match log file messages and events is specified in the format file. Regular expression-filtering support is provided by the International Components for Unicode libraries to check whether the attribute value that is examined matches the specified pattern. For more information about using regular expressions, see the URL on this slide.

Configuration (1 of 4)

- Go to the Manage Tivoli Enterprise Monitoring Services window
- Right click Tivoli Log File Agent template
- Choose "Configure Using Defaults"

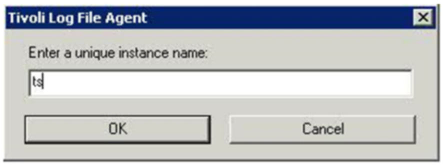


Manage Tivoli Enterprise Monitoring Services - TEMS Mode - [Local Computer]

Service/Application	Task/SubSystem	Configured	Status	Configuration	Startup	Account	Desktop	HotStdby	Version	Host	Port
Eclipse Help Server	HELPSVR	Yes	Started	up-to-date	Auto	LocalSystem	No	No	06.23.01.00		
Tivoli Enterprise Portal	Browser	Yes		N/A	N/A	N/A	N/A	N/A	06.23.01.00	localhost	
Tivoli Enterprise Portal	Desktop	Yes		N/A	N/A	N/A	N/A	N/A	06.23.01.00	NC9037038...	
Tivoli Enterprise Portal Server	KFWSRV	Yes (TEMS)	Started	up-to-date	Auto	LocalSystem	No	No	06.23.01.00		
Universal Agent	Primary	Yes (TEMS)	Started	up-to-date	Auto	LocalSystem	No	No	06.23.01.00		
Warehouse Summarization and Pru...	Primary	Yes (TEMS)	Started	up-to-date	Auto	LocalSystem	No	No	06.23.01.00		
Agentless Monitoring for Solaris OS	Template			N/A					06.23.01.00		
Agentless Monitoring for HP-UX OS	Template			N/A					06.23.01.00		
Agentless Monitoring for Linux OS	INST1	Yes (TEMS)	Started	up-to-date	Auto	LocalSystem	No	No	06.23.01.00		
Agentless Monitoring for Linux OS	Template			N/A					06.23.01.00		
Agentless Monitoring for AIX OS	Template			N/A					06.23.01.00		
Agentless Monitoring for Windows OS	Template			N/A					06.23.01.00		
Performance Analyzer	Primary	Yes (TEMS)	Started	up-to-date	Auto	LocalSystem	No	No	06.23.01.00		
Monitoring Agent for Windows OS	Primary	Yes (TEMS)	Started	up-to-date	Auto	LocalSystem	Yes	No	06.23.01.00		
Tivoli Log File Agent	ts	Yes (TEMS)	Started	up-to-date	Auto	LocalSystem	No	No	06.30.00.03		
Tivoli Log File Agent	testlfa	Yes (TEMS)	Started	up-to-date	Auto	LocalSystem	No	No	06.30.00.03		
Tivoli Log File Agent	Template			N/A					06.30.00.03		
Warehouse Proxy	Primary			up-to-date	Auto	LocalSystem	No	No	06.23.01.00		
Monitoring Agent for F5 SNMP Polling	F5SNMP			up-to-date	Auto	LocalSystem	No	No	06.23.00.00		
Monitoring Agent for F5 SNMP Polling	Template			N/A					06.23.00.00		
Monitoring Agent for Ping	Primary			up-to-date	Auto	LocalSystem	No	No	06.23.00.00		
Monitoring Agent for IMM Performa...	Primary			up-to-date	Auto	LocalSystem	No	No	06.23.00.00		
Monitoring Agent for Database	Primary			up-to-date	Auto	LocalSystem	No	No	06.23.00.00		
Tivoli Enterprise Monitoring Server	TEMS1			up-to-date	Auto	LocalSystem	No	No	06.23.01.00		

You can configure the Log File Agent instance in the Manage Tivoli Enterprise Monitoring Services window. Right click the Log File Agent template and choose "Configure Using Defaults".

Configuration (2 of 4): Tivoli Log File Agent instance name



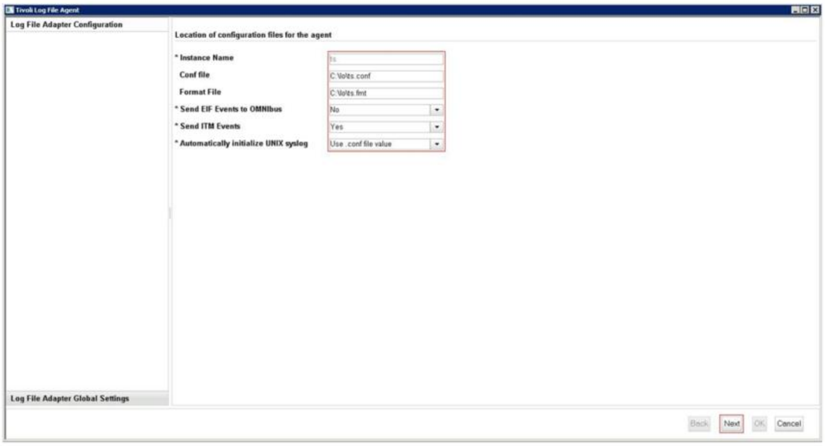
Enter a unique instance name: ts

- Enter a unique instance name
  - For example: ts
- Instance names cannot be reused
  - The instance name acts as a unique identifier for the monitored log file
- Certain keywords and special characters are not allowed for the instance name
- Click "OK"

Enter a unique instance name and click OK.

Configuration (3 of 4): Log File Adapter Configuration

- Enter the valid values for each field
- Click “Next”


Tivoli Log File Agent
Log File Adapter Configuration
Log File Adapter Global Settings
Back
Next
OK
Cancel

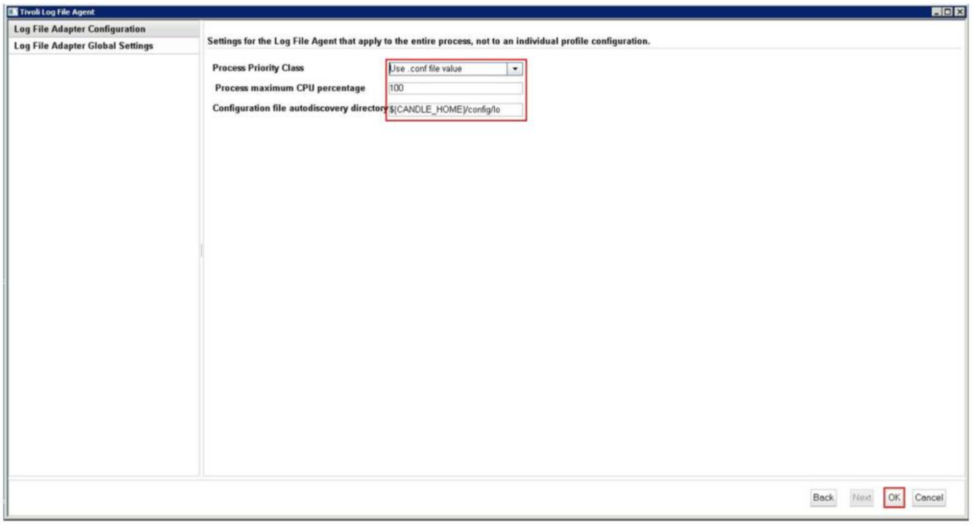
Location of configuration files for the agent

* Instance Name: ts
Conf file: C:\lo\ts.conf
Format File: C:\lo\ts.fmt
* Send EIF Events to OMNIbus: No
* Send ITM Events: Yes
* Automatically initialize UNIX syslog: Use .conf file value

Enter the locations of the configuration file and the format file. The other log file adapter configuration parameters are pre-populated. You can change the entries per your requirements. Then click Next.

Configuration (4 of 4): Log File Adapter Global Settings

- Enter the appropriate value for each field
- Choose “OK”



Tivoli Log File Agent
Log File Adapter Configuration
Log File Adapter Global Settings

Settings for the Log File Agent that apply to the entire process, not to an individual profile configuration.

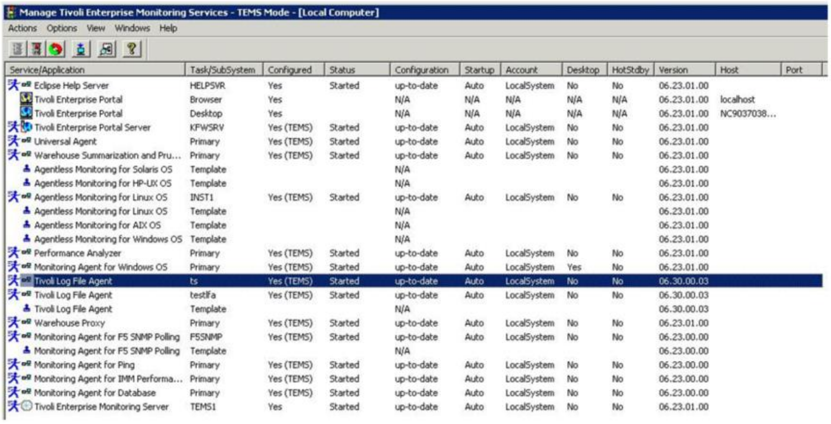
Process Priority Class: Use .conf file value

Process maximum CPU percentage: 100

Configuration file autodiscovery directory: $(CANDLE_HOME)/config/lo

Enter the log file adapter global settings parameters per your requirements. Then click OK.

Agent started



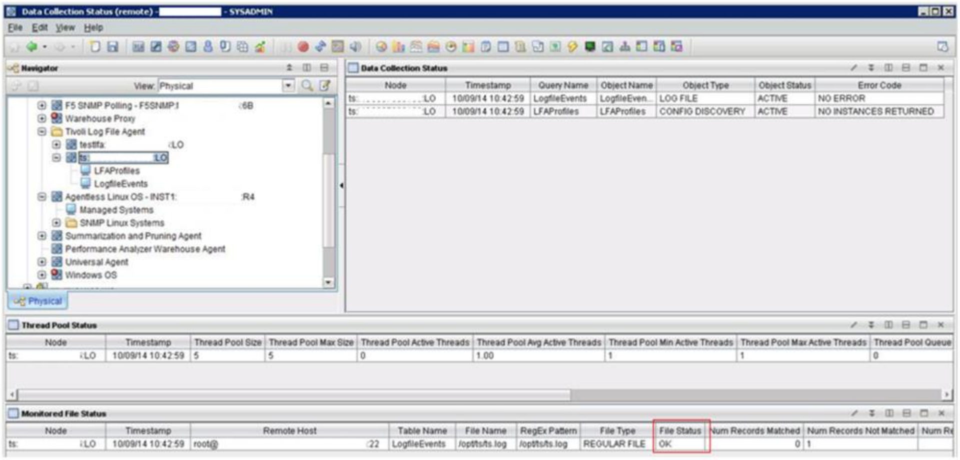
Manage Tivoli Enterprise Monitoring Services - TEMS Mode - [Local Computer]

Service/Application	Task/SubSystem	Configured	Status	Configuration	Startup	Account	Desktop	HotStdby	Version	Host	Port
Eclipse Help Server	HELPSVR	Yes	Started	up-to-date	Auto	LocalSystem	No	No	06.23.01.00		
Tivoli Enterprise Portal	Browser	Yes		N/A	N/A	N/A	N/A	N/A	06.23.01.00	localhost	
Tivoli Enterprise Portal	Desktop	Yes		N/A	N/A	N/A	N/A	N/A	06.23.01.00	NC9037038...	
Tivoli Enterprise Portal Server	KFWSRV	Yes (TEMS)	Started	up-to-date	Auto	LocalSystem	No	No	06.23.01.00		
Universal Agent	Primary	Yes (TEMS)	Started	up-to-date	Auto	LocalSystem	No	No	06.23.01.00		
Warehouse Summarization and Pru...	Primary	Yes (TEMS)	Started	up-to-date	Auto	LocalSystem	No	No	06.23.01.00		
Agentless Monitoring for Solaris OS	Template			N/A					06.23.01.00		
Agentless Monitoring for HP-UX OS	Template			N/A					06.23.01.00		
Agentless Monitoring for Linux OS	INST1	Yes (TEMS)	Started	up-to-date	Auto	LocalSystem	No	No	06.23.01.00		
Agentless Monitoring for Linux OS	Template			N/A					06.23.01.00		
Agentless Monitoring for AIX OS	Template			N/A					06.23.01.00		
Agentless Monitoring for Windows OS	Template			N/A					06.23.01.00		
Performance Analyzer	Primary	Yes (TEMS)	Started	up-to-date	Auto	LocalSystem	No	No	06.23.01.00		
Monitoring Agent for Windows OS	Primary	Yes (TEMS)	Started	up-to-date	Auto	LocalSystem	Yes	No	06.23.01.00		
Tivoli Log File Agent	ts	Yes (TEMS)	Started	up-to-date	Auto	LocalSystem	No	No	06.30.00.03		
Tivoli Log File Agent	testlfa	Yes (TEMS)	Started	up-to-date	Auto	LocalSystem	No	No	06.30.00.03		
Tivoli Log File Agent	Template			N/A					06.30.00.03		
Warehouse Proxy	Primary	Yes (TEMS)	Started	up-to-date	Auto	LocalSystem	No	No	06.23.01.00		
Monitoring Agent for F5 SNMP Polling	F5SNMP	Yes (TEMS)	Started	up-to-date	Auto	LocalSystem	No	No	06.23.00.00		
Monitoring Agent for F5 SNMP Polling	Template			N/A					06.23.00.00		
Monitoring Agent for Ping	Primary	Yes (TEMS)	Started	up-to-date	Auto	LocalSystem	No	No	06.23.00.00		
Monitoring Agent for IMM Performa...	Primary	Yes (TEMS)	Started	up-to-date	Auto	LocalSystem	No	No	06.23.00.00		
Monitoring Agent for Database	Primary	Yes (TEMS)	Started	up-to-date	Auto	LocalSystem	No	No	06.23.00.00		
Tivoli Enterprise Monitoring Server	TEMS1	Yes	Started	up-to-date	Auto	LocalSystem	No	No	06.23.01.00		

- The Log File Agent instance “ts” configuration is complete
- The Manage Tivoli Enterprise Monitoring Services window shows the Log File Agent instance “ts” as Started

Once the configuration of the Log File Agent instance is complete, the instance will have a status of “Started” in the Manage Tivoli Enterprise Monitoring Services window.

Agent registration OK



Data Collection Status (remote) - [redacted] - SYSADMIN

- F5 SNMP Polling - F5SNMP1 :6B
- Warehouse Proxy
- Tivoli Log File Agent
  - testlfa: :LO
  - ts: LO
    - LFAProfiles
    - LogfileEvents
- Agentless Linux OS - INST1: :R4
  - Managed Systems
  - SNMP Linux Systems
- Summarization and Pruning Agent
- Performance Analyzer Warehouse Agent
- Universal Agent
- Windows OS

Data Collection Status

Node	Timestamp	Query Name	Object Name	Object Type	Object Status	Error Code
ts: LO	10/09/14 10:42:59	LogfileEvents	LogfileEven...	LOG FILE	ACTIVE	NO ERROR
ts: LO	10/09/14 10:42:59	LFAProfiles	LFAProfiles	CONFIG DISCOVERY	ACTIVE	NO INSTANCES RETURNED

Thread Pool Status

Node	Timestamp	Thread Pool Size	Thread Pool Max Size	Thread Pool Active Threads	Thread Pool Avg Active Threads	Thread Pool Min Active Threads	Thread Pool Max Active Threads	Thread Pool Queue
ts: :LO	10/09/14 10:42:59	5	5	0	1.00	1	1	0

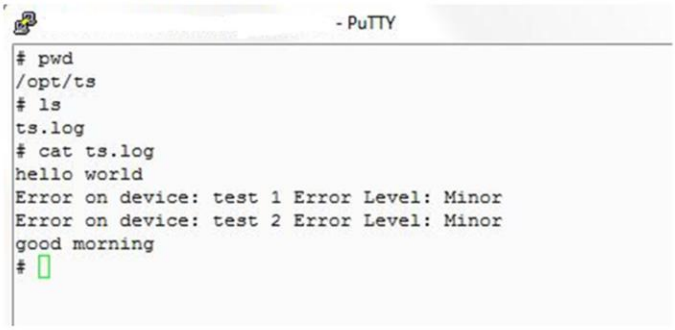
Monitored File Status

Node	Timestamp	Remote Host	Table Name	File Name	RegEx Pattern	File Type	File Status	Num Records Matched	Num Records Not Matched	Num Re
ts: :LO	10/09/14 10:42:59	root@ :22	LogfileEvents	/opt/ts/ts.log	/opt/ts/ts.log	REGULAR FILE	OK	0	1	

- The new Log File Agent instance ts is registered in the Tivoli Enterprise Portal Client
- The corresponding workspaces and attribute groups are added

Ensure that there are no errors in Tivoli Enterprise Portal, once the agent is registered. The correct value for the File Status column is OK. If there are any errors in this column, rectify the agent configuration.

Test entries in the remote log file



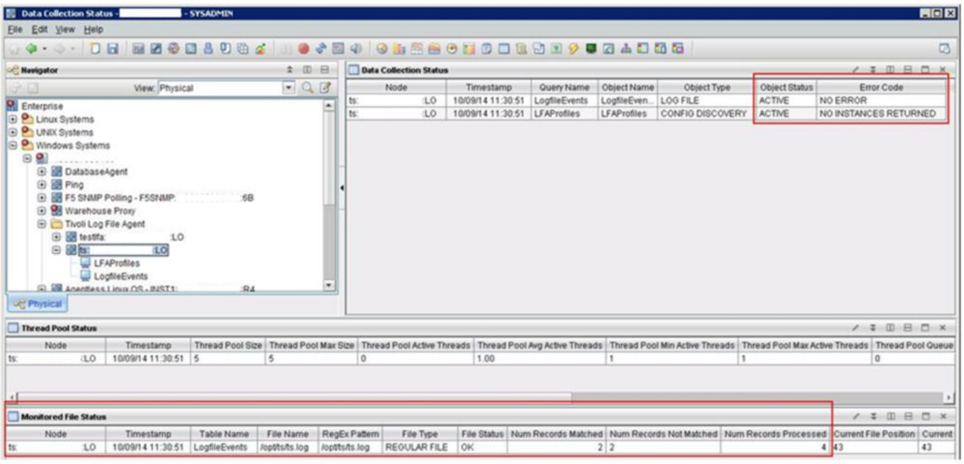
- PuTTY

```
# pwd
/opt/ts
# ls
ts.log
# cat ts.log
hello world
Error on device: test 1 Error Level: Minor
Error on device: test 2 Error Level: Minor
good morning
# 
```

- Shown above are the test entries in “/opt/ts/ts.log” on the remote machine
- These entries are compared against the regular expression that is specified in the format file
  - If the entries match, they are displayed in the Tivoli Enterprise Portal client
  - Otherwise, they are captured in the UnmatchLog file, if specified in the configuration file

Here, four sample entries are made in the remote log file. These entries are monitored by the Log File Agent instance that was configured earlier in this module.

Test output in the portal



Data Collection Status

Node	Timestamp	Query Name	Object Name	Object Type	Object Status	Error Code
ts: :LO	10/09/14 11:30:51	LogfileEvents	LogfileEven...	LOG FILE	ACTIVE	NO ERROR
ts: :LO	10/09/14 11:30:51	LFAProfiles	LFAProfiles	CONFIG DISCOVERY	ACTIVE	NO INSTANCES RETURNED

Thread Pool Status

Node	Timestamp	Thread Pool Size	Thread Pool Max Size	Thread Pool Active Threads	Thread Pool Avg Active Threads	Thread Pool Min Active Threads	Thread Pool Max Active Threads	Thread Pool Queue
ts: :LO	10/09/14 11:30:51	5	5	0	1.00	1	1	0

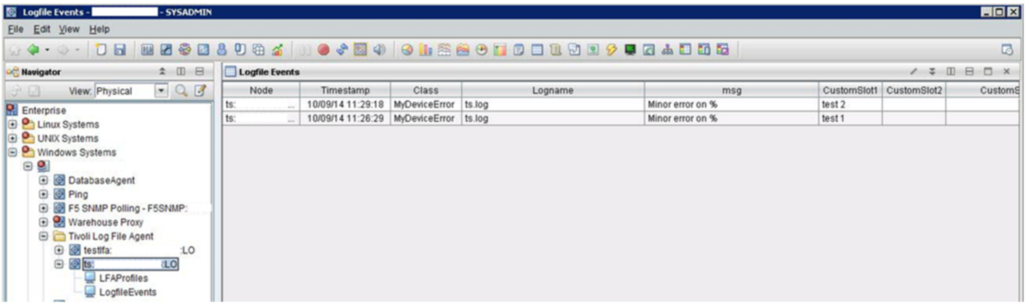
Monitored File Status

Node	Timestamp	Table Name	File Name	RegEx Pattern	File Type	File Status	Num Records Matched	Num Records Not Matched	Num Records Processed	Current File Position	Current
ts: :LO	10/09/14 11:30:51	LogfileEvents	/opt/ts/ts.log	/opt/ts/ts.log	REGULAR FILE	OK	2	2	4	43	43

- Num Records Processed = 4, with Matched = 2 and Not Matched = 2
- No errors are recorded and the file name that is being monitored is specified

Of the four records, two are reported as matched and two as unmatched entries. Ensure that no other entries are displaying any errors.

Test matched entries

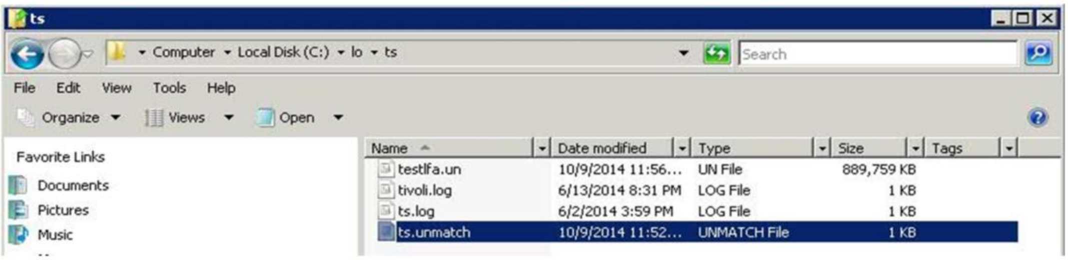


Node	Timestamp	Class	Logname	msg	CustomSlot1	CustomSlot2	CustomS
ts: ...	10/09/14 11:29:18	MyDeviceError	ts.log	Minor error on %	test 2		
ts: ...	10/09/14 11:26:29	MyDeviceError	ts.log	Minor error on %	test 1		

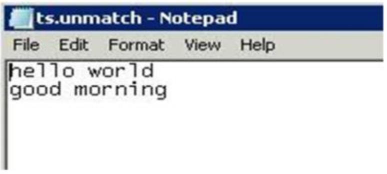
- Matched records are displayed in the Logfile Events workspace
- The column attributes are specified in the format file

The matched entries are shown in the Logfile Events workspace. The values in each column are specified by the regular expression in the format file.

Test unmatched entries



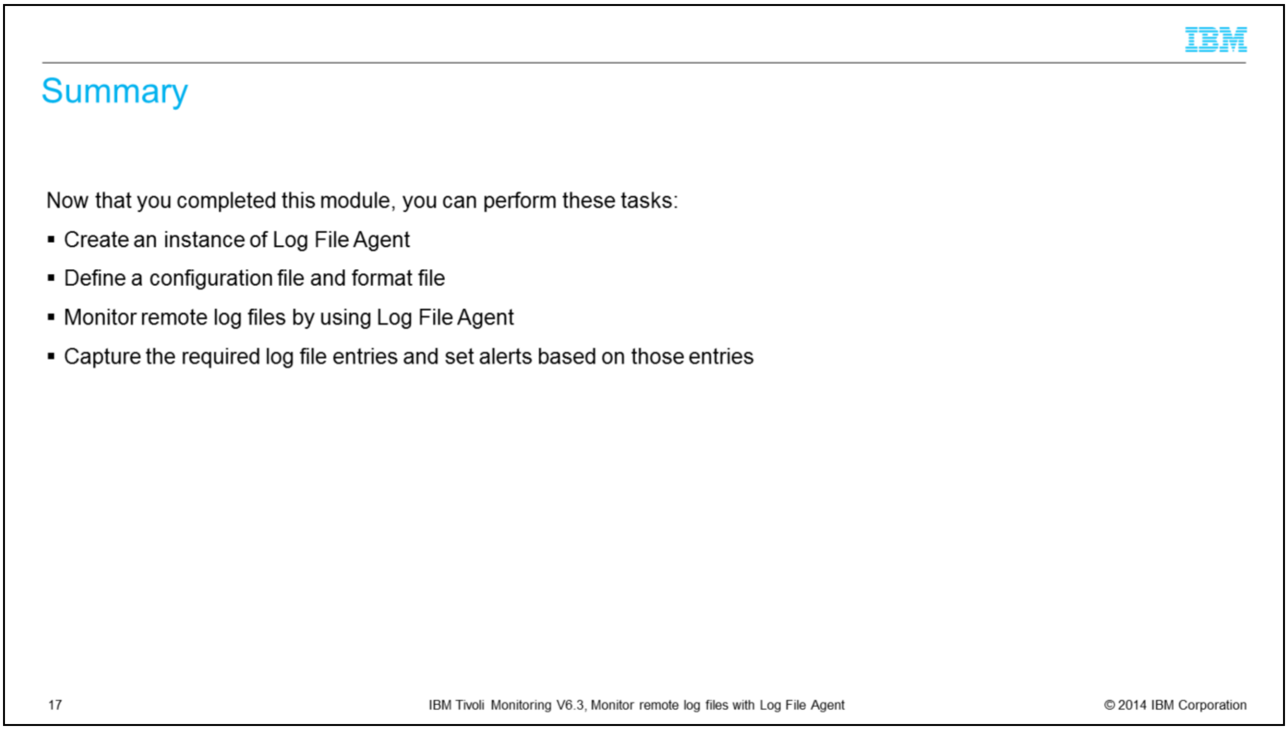
Name	Date modified	Type	Size	Tags
testlfa.un	10/9/2014 11:56...	UN File	889,759 KB	
tivoli.log	6/13/2014 8:31 PM	LOG File	1 KB	
ts.log	6/2/2014 3:59 PM	LOG File	1 KB	
ts.unmatch	10/9/2014 11:52...	UNMATCH File	1 KB	



```
hello world
good morning
```

- Unmatched records are captured in the unmatch file, if specified in the configuration file
- The two unmatched entries are shown in the ts.unmatch file

Log file entries that do not match are captured in the unmatch log file. Recording unmatched entries is not mandatory. If these entries are not needed, they can be ignored.

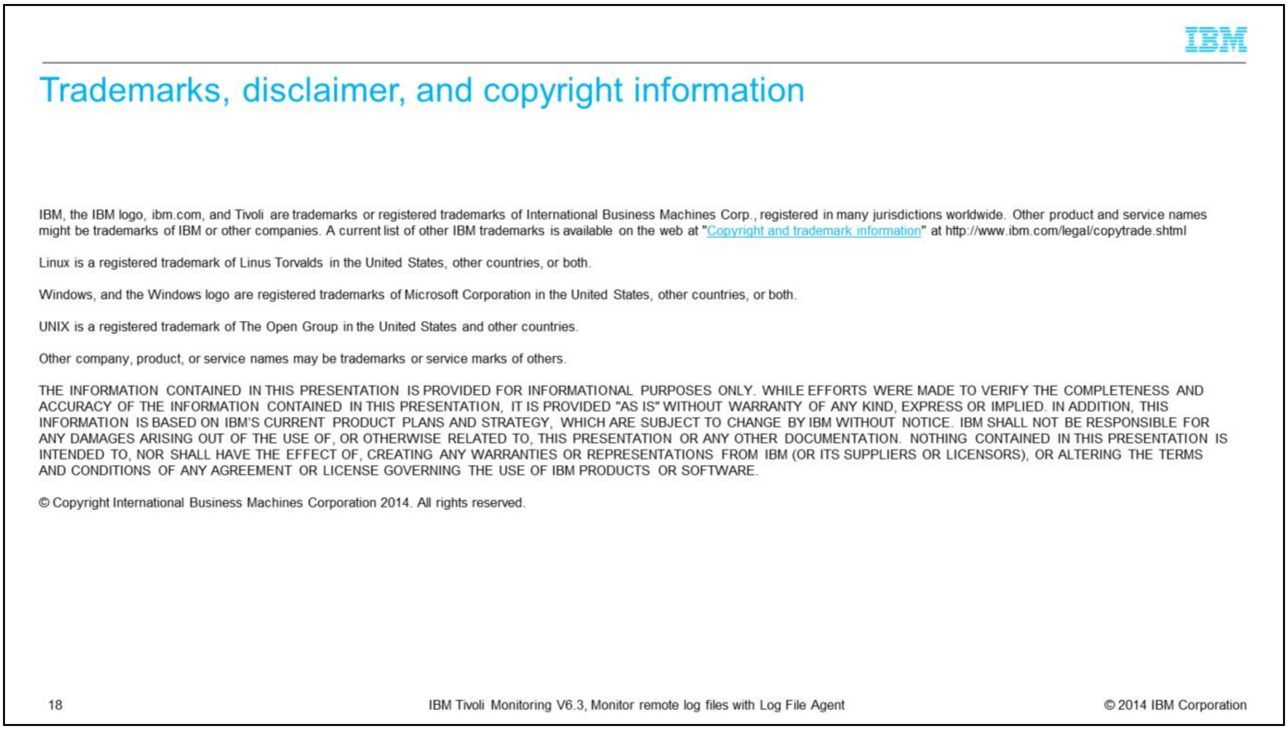


Summary

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

- Create an instance of Log File Agent
- Define a configuration file and format file
- Monitor remote log files by using Log File Agent
- Capture the required log file entries and set alerts based on those entries

Now that you completed this module, you can create a new Log File Agent instance that can be used to monitor remote log files. You can define the configuration and format files. And you can capture the required log file entries and set alerts based on those entries.



Trademarks, disclaimer, and copyright information

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.