IBM Tivoli Monitoring
Version 6.2.3

Troubleshooting Guide

GC32-9458-04

IBM Tivoli Monitoring
Version 6.2.3

Troubleshooting Guide

GC32-9458-04

Note
Before using this information and the product it supports, read the information in "Notices" on page 295.

This edition applies to version 6.2.3 of IBM Tivoli Monitoring (product number 5724-C04) and to all subsequent releases and modifications until otherwise indicated in new editions.

Contents

Chapter 1. Introduction to troubleshooting

This guide helps you to decide where to begin looking for causes when you have a problem with IBM Tivoli Monitoring. Usually, you start with a symptom, or set of symptoms, and trace them back to their cause. This process is called *troubleshooting*. Troubleshooting is not the same as problem solving, although during the process of troubleshooting, you can obtain enough information to solve a problem. Examples of situations where this can happen include:

- End-user errors
- Application programming errors
- System programming errors, such as in resource definitions

However, you might not always be able to solve a problem yourself after determining its cause. For example, a performance problem might be caused by a limitation of your hardware. If you are unable to solve a problem on your own, contact IBM® Software Support for a solution. See Chapter 2, "Collecting and reviewing troubleshooting data," on page 5 for information on what types of data to collect before contacting Support.

Sources of troubleshooting information

The primary troubleshooting feature is logging. *Logging* refers to the text messages and trace data generated by the software. Messages and trace data are sent to an output destination, such as a console screen or a file.

Typically, text messages relay information about the state and performance of a system or application. Messages also alert the system administrator to exceptional conditions when they occur. Consult the explanation and operator response associated with the displayed messages to determine the cause of the failure. See the document *IBM Tivoli® Monitoring Messages* for message information.

Trace data capture transient information about the current operating environment when a component or application fails to operate as designed. IBM Software Support personnel use the captured trace information to determine the source of an error or unexpected condition. See the Chapter 4, "Tools," on page 35 for more information about tracing.

Problem classification

The first task in troubleshooting is to determine the origin of the problem, or which component or function is experiencing a problem. To assist you in determining the origin of the problem, collect documentation at the time of the error. You might experience problems with IBM Tivoli Monitoring in the following areas:

- Installation
- Upgrading
- Configuration
- Connectivity
- Tivoli Enterprise Portal
- Tivoli Enterprise Portal Server
- Tivoli Enterprise Monitoring Server

- Tivoli Enterprise Monitoring Agent deployment
- Databases
- Tivoli Data Warehouse
- Universal Agent
- IBM Tivoli Enterprise Console®

Finding release notes

You can find release note information online by viewing IBM technotes. Technotes replace the Release Notes manual for this product. Technotes are short documents that cover a single topic. You can search the technotes collection for common problems and solutions, as well as known limitations and workarounds. Technotes are continuously updated to provide current product information.

The following two procedures describe how to view technotes and subscribe to have future technotes e-mailed to you. Alternatively, you can watch demos of these procedures at the following Web site:

http://www-306.ibm.com/software/support/sitetours.html

Viewing technotes

Perform the following actions to access technotes for this product:

1. Launch the IBM Software Support Web site: http://www.ibm.com/software/support
2. In the Products A - Z field, select the product name to open the product-specific support site.

   For this product, select **I > IBM Tivoli Monitoring**..
3. In the **Self help** field, click **Technotes**.
4. Scroll through the technotes, or you can optionally type a search term to refine the displayed data.

   For tips on refining your search, click **Search tips**.

Creating an e-mail subscription to technotes

You can subscribe to e-mail notification about product tips and newly published fixes through My support, a personalized portal that enables you to:

- Specify the products for which you want to receive notifications
- Choose from flashes, downloads, and technotes
- Receive an e-mail update in your inbox

Perform the following actions to subscribe to My support e-mails:

1. Launch an IBM support Web site such as the following site:

   http://www.ibm.com/support/us/
2. Click **My support** in the upper-right corner of the page.
3. If you have not yet registered, click **register** in the upper-right corner of the support page to create your user ID and password.
4. Sign in to **My support**.
5. On the My support page, click **Edit profile**.
6. Select a product family and continue setting your preferences to specify the information you want in your e-mails.

7. Click **Submit**.

Chapter 2. Collecting and reviewing troubleshooting data

If you have a problem that you are unable to solve using the information in this guide, gather the following information that relates to the problem and contact IBM Software Support for further assistance

Appropriate IBM Tivoli Monitoring RAS1 trace output

The reliability, availability, and serviceability (RAS) trace logs are available on the Tivoli Enterprise Monitoring Server, the Tivoli Enterprise Portal Server, and the monitoring agent. By default, the logs are stored in the installation path for IBM Tivoli Monitoring. IBM Software Support uses the information captured by trace logs to trace a problem to its source or to determine why an error occurred. The following links to sections in this document supply more information on these files:

- For information on where they are stored, see "Trace logging" on page 35.
- For information on setting the trace option for an IBM Tivoli Monitoring component, see "Setting traces" on page 42.
- For information on dynamically setting the trace settings, see "Dynamically modify trace settings for an IBM Tivoli Monitoring component" on page 53.
- For information on reading RAS1 logs, see "Reading RAS1 logs" on page 42.
- For information on the ras1log tool, see "ras1log tool" on page 59.

Snapcore files

The snapcore command gathers a core file, program, and libraries used by the program and compresses the information into a pax file. The file can then be downloaded to disk or tape, or transmitted to a remote system. The information gathered with the snapcore command allows you to identify and resolve problems with an application. To collect all the information you might need to debug and analyze the problem, you can use the snapcore command, as shown in the following steps:

1. Change to the directory where the core dump file is located:

   ```
   # ls -l
   total 84176
   -rw-r--r-- 1 root system 2704 Feb 21 09:52 core.18048.01084144
   ```

2. Run the snapcore command to collect all needed files:

   ```
   # snapcore -d /tmp/myDir core.18048.01084144
   ```

   The snapcore command gathers all information and creates a new compressed pax archive in the /tmp/*myDir* directory. If you do not specify a special directory using the -d flag, the archive will be stored in /tmp/snapcore directory. The new archive file will be named as snapcore_$pid.pax.Z:

   ```
   # ls -l /tmp/myDir
   total 5504
   -rw-r--r--     1 root system 2815081 Feb 21 09:56 snapcore_20576.pax.Z
   ```

3. To check the content of the pax archive, use the following command:

   ```
   # uncompress -c snapcore_20576.pax.Z | pax core.18048.01084144
   README
   lslpp.out
   errpt.out
   ```

```
vi
./usr/lib/libc.a
./usr/lib/libcrypt.a
./usr/lib/libcurses.a
./usr/lib/nls/loc/en_US
./usr/lib/libi18n.a
./usr/lib/libiconv.
```

Core files

If the system stops on UNIX-based systems, collect the core file from the directory where the binary file that the process belongs to is stored. For example, if the failing process is the portal server process, KfwServices, the core is created in the /opt/IBM/ITM_61/*archtype*/cq/bin/ directory.

To retrieve information about where the core file is created, use the **errpt -a** command. This command shows a summary information about the most recent crashes and also the location of the core file:

```
-------------
LABEL:          CORE_DUMP
IDENTIFIER:     A63BEB70

Date/Time:       Tue Jun 30 15:38:47 DFT 2009
Sequence Number: 1229
Machine Id:      0056536D4C00
Node Id:         nc114062
Class:           S
Type:            PERM
Resource Name:   SYSPROC

Description
SOFTWARE PROGRAM ABNORMALLY TERMINATED

Probable Causes
SOFTWARE PROGRAM

User Causes
USER GENERATED SIGNAL

        Recommended Actions
        CORRECT THEN RETRY

Failure Causes
SOFTWARE PROGRAM

        Recommended Actions
        RERUN THE APPLICATION PROGRAM
        IF PROBLEM PERSISTS THEN DO THE FOLLOWING
        CONTACT APPROPRIATE SERVICE REPRESENTATIVE

Detail Data
SIGNAL NUMBER
          11
USER'S PROCESS ID:
       32248
FILE SYSTEM SERIAL NUMBER
          10
INODE NUMBER
      655367
PROCESSOR ID
           0
CORE FILE NAME
/opt/IBM/ITM_61/aix533/cq/bin/core
```

```
PROGRAM NAME
KfwServices
STACK EXECUTION DISABLED
--------------
```

drWatson dumps and logs

If the systems stops on Windows, collect the `drwtsn32.log` and `user.dmp` files if available. The `drwtsn32.log` and `user.dmp` files are located in

`\Documents and Settings\All Users\Documents\DrWatson`

1. Enter the following command at the prompt to enable Dr. Watson as default debugger:

   `drwtsn32 –i`
2. Enter the following command at the prompt to open the Dr. Watson configuration window:

   `drwtsn32`
3. Set the **Crash dump Type** to **FULL**.
4. Remove the check from the **Dump Symbol Table** box.
5. Place a check in the **Dump all Thread Contexts** box.
6. Place a check in the **Create Crash Dump File** box.

KxxCMA.RAS files

`KxxCMA.RAS` files are created on Windows systems, usually under the `c:\windows\system32` directory, to gather information about IBM Tivoli Monitoring process crashes. For example, for the Monitoring Agent for Windows OS, this file would be called `KNTCMA.RAS`. These files contain symptom dump information similar to the `drWatson.log`, but are generated by the IBM Tivoli Monitoring infrastructure.

Other important information

Other important information includes the following:

- Monitored application file as specified on the SOURCE FILE statement, if applicable.
- Description of the operation scenario that led to the problem.
- Incorrect output, such as Tivoli Enterprise Portal screencaptures or a description of what you observed, if applicable.
- Log files - collect these from failing systems. You can collect all logs or logs of a certain type such as, RAS trace logs or message logs.
- Messages and other information displayed on the screen.
- Application information - this would be for the application you are monitoring, such as DB2® or SAP. This information would include the version number and patch level and a sample application data file if you are monitoring a file.
- Operating system version number and patch level.
- Version number of the following members of the monitoring environment:
  - IBM Tivoli Monitoring. Also provide the patch level, if available.
  - Monitoring Agent version number .
  - Tivoli Enterprise Portal. Select **About Tivoli Enterprise Portal ...** from the Help menu.

Note: The version number of the Tivoli Enterprise Portal and the Tivoli Enterprise Portal server must always be synchronized.

Chapter 3. Solving common problems

The following sections give troubleshooting instructions for the most common problems encountered by customers using the IBM Tivoli Monitoring product or the components of Tivoli Management Services.

Note: Use the trace settings indicated in these troubleshooting instructions only while you are trying to diagnose a specific problem. To avoid generating excessive trace data, go back to the default trace settings as soon as the problem is solved.

About the tools

This section describes several tools that are available to help you with troubleshooting.

ITMSUPER Tools

Use the ITMSUPER Tools to learn about the health of your managed systems, situations, and environment configuration. The ITMSUPER Tools are included in the IBM Support Assistant (ISA), a free local software serviceability workbench that helps you resolve questions and problems with IBM software products. To install the ISA software, go to http://www.ibm.com/software/support/isa.

Log Analyzer tool

The Log Analyzer tool helps you perform detailed problem diagnosis on situations and events. For more information see "Log and Trace Analyzer Tool" on page 60.

A detailed explanation of where to find the monitoring server logs, portal server logs, and any other logs mentioned in this chapter can be found in "Trace logging" on page 35, Table 22 on page 35.

pdcollect tool

The pdcollect tool collects the most commonly used information from a system. It gathers log files, configuration information, version information, and other data. You can also use this tool to manage the size of trace data repositories.

For more information see "pdcollect tool" on page 59.

IBM Support Assistant

The IBM Support Assistant is a free, stand-alone application that you can install on any workstation. You can then enhance the application by installing product-specific plug-in modules for the IBM products you use.

For more information see Appendix C, “Support information,” on page 287.

I am trying to find out what software is supported

The following information lists the resources available to determine what software is supported.

IBM Tivoli Monitoring Installation and Setup Guide

The *IBM Tivoli Monitoring Installation and Setup Guide* provides specific information about the supported software for IBM Tivoli Monitoring. Use the "Hardware and software requirements" section in Chapter 3 of the *Installation and Setup Guide* to find information on supported software.

To find the "Hardware and software requirements" section of the *Installation and Setup Guide* go to the Tivoli Monitoring and OMEGAMON® XE Information Center at http://publib.boulder.ibm.com/infocenter/tivihelp/v15r1/index.jsp. In the left navigation panel select **IBM Tivoli Monitoring**, expand the version of the software you are using, for example, **Version 6.2.2**, then expand **Installing and Configuring**. Then navigate through the following levels: **Planning your installation** > **Preparing for installation** > **Hardware and software requirements**.

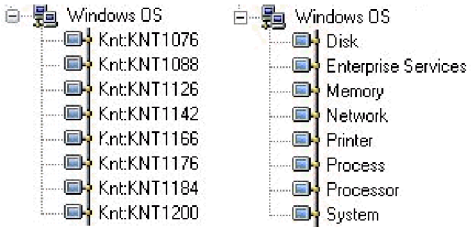
Tivoli Platform and Database Support Matrix

The Tivoli Platform and Database Support Matrix provides platform and database support information for most Tivoli products. The matrix can be found at http://www.ibm.com/software/sysmgmt/products/support/Tivoli_Supported_Platforms.html.

Workspaces are missing or views are empty

The following problems might occur:

- The workspaces return no data.
- There are no child Navigator items under the agent node in the Navigator view. See Table 1 on page 13.
- The Navigator items are labeled with internal names such as `Knt:KNT1076` instead of the correct names (such as Disk). See Table 1 on page 13.



- You receive message `KFWITM217E: Request error: SQL1_CreateRequest failed, rc=209`. See Table 1 on page 13.
- You receive message `KFWITM220E: Request failed during execution`. See Table 3 on page 14.

Note: For workspaces related to historical data refer to "Historical data is missing or incorrect" on page 22.

Preliminary diagnostics:

1. Refresh the Navigator (**View** > **Refresh**).
2. Verify that the monitoring agent has been started. Restart if needed.
3. Verify that the monitoring agent configuration is correct.
4. If your data is missing in an Oracle Agent workspace see Table 21 on page 32. (Similar problems might exist for other monitoring agents.)
5. Check that application support has been added. See Table 1 on page 13.

The following tables include possible causes and corresponding solutions for the problems described in this section.

Table 1. Correcting application support problems

Lack of application support, or application support level mismatch among components (monitoring server, portal server, desktop and Java Web Start clients, and monitoring agents).
Diagnostic and corrective actions
1. Check application support on the monitoring server, portal server, and portal client: • On Windows: Run the **kincinfo.exe -i** command in the *%CANDLE_HOME\InstallITM* directory to show what is installed. • On Linux or UNIX: Run the **./cinfo –i** command in the *$CANDLEHOME/bin* directory to show what is installed. • For a monitoring server on z/OS®: Look in the &*rhilev*.&*rte*.RKANDATV data set (where &*rhilev* is the high-level qualifier and &*rte* is the mid-level qualifier of the libraries for the runtime environment where the monitoring server is configured) for files named K*pp*CAT and K*pp*ATR (where *pp* is the two-character product or component code). 2. You can also run the TEMS Servers Analysis tool provided by ITMSUPER against the hub monitoring server to ensure that application support is installed consistently throughout your environment. 3. If application support is missing, add the appropriate application support to the portal server and monitoring server for the monitoring agents. If the desktop or Java Web Start client is being used, application support must also be installed on the portal client. For more information and instructions on installing application support see "Configuring application support for non-base monitoring agents" in the *IBM Tivoli Monitoring Installation and Setup Guide*. For instructions on installing application support on a monitoring server on z/OS, see *Configuring the Tivoli Enterprise Monitoring Server on z/OS*.

Table 2. Correcting monitoring server problems

• Monitoring server is not started. • Connectivity has been lost between the portal server and monitoring server, or between the monitoring server and monitoring agent.
Diagnostic and corrective actions
1. If you are an administrator, restart the monitoring server. Otherwise, notify an administrator and wait for the monitoring server to be restarted. 2. Running the following ITMSUPER tools might also provide more information: • Topology tool • Connectivity tool • TEMS Server Analysis tool • TEPS Analysis tool 3. Check the portal server logs for messages indicating communication failures to the monitoring server. Check the monitoring server logs for messages indicating communication failures to the remote monitoring servers or to monitoring agents. 4. Correct the communication failures indicated in the logs.

Table 3. Correcting monitoring agent problems

• The monitoring agent is running but no data is being returned. • The monitoring agent log contains an error message similar to `Endpoint unresponsive`.
Diagnostic and corrective actions
Note: For monitoring agents on z/OS, see each product's *Problem Determination Guide* or the *IBM Tivoli Monitoring Troubleshooting Guide*. 1. Verify that the agent is connected. Check the monitoring server log for messages similar to `Remote node <SYS:MQIRA> is ON-LINE` 2. If the agent is online, check to see whether subnodes are online in the agent log. For example: `KMQMI171I Node JSG1:SYS:MQESA is online` 3. If subnodes are online, are workspaces showing correct titles? **No**: Verify that application support has been installed correctly and `buildpresentation.bat` ran correctly. **Yes**: Go to the next step. 4. If workspaces contains titles, is there a column heading? **No**: Verify that application support has been installed correctly and `buildpresentation.bat` ran correctly. **Yes**: Go to the next step. 5. If there is only a column heading with no data, turn on `(UNIT:KRA ALL)` in the agent and verify that rows are being returned when the workspaces are displayed.

Status of a monitoring agent is mismatched between the portal client and tacmd command

This problem involves a discrepancy or mismatch between a monitoring agent's status as shown in the portal client and as returned by a tacmd command. For example:

- A monitoring agent shows as offline in the portal client and online in the results of a tacmd command.
- A monitoring agent shows as online in the portal client and offline in the results of a tacmd command.

Preliminary diagnostics:

1. Verify the state of the monitoring agent in Manage Tivoli Monitoring Services.
2. Compare the status of the node in the physical Navigator view with the status reported in the Managed System Status workspace. If the status in the physical Navigator view agrees with the status shown in the Managed System Status workspace, then the problem is at the monitoring agent. See Table 4.
3. To determine whether the problem is in the portal server or monitoring server, set the following trace in the portal server:

   ```
   ERROR (UNIT:ctcmw IN ER)
   ```

   Then examine the portal server log for the following statement:

   ```
   Node Status event received (managed system name)
   ```

   If the trace shows that the last node status record received for the managed system matches the status shown in the portal client, then the problem is located in the monitoring server. See Table 5 on page 16.

   If the trace shows that the last node status record received for the managed system indicated the correct status, then the problem is located in the portal server. Run the portal server trace, collect logs, and call IBM Software Support.

The following tables include possible causes and corresponding solutions for the problems described in this section.

Table 4. Correcting monitoring agent problems

Monitoring agent has been started, but the Navigator has not been refreshed in the portal client.
Diagnostic and corrective actions
1. Open the Managed System Status workspace and click **Refresh**. 2. Make sure the monitoring agent is connected to the correct monitoring server. 3. Check the status of the monitoring server the monitoring agent is connected to. (Proceed to Table 5 on page 16.)

Table 5. Correcting monitoring server problems

• Remote monitoring server has shut down. • Loss of connectivity between the monitoring agent and the remote monitoring server to which it reports, or between that remote monitoring server and the hub monitoring server. • You receive the following message in the monitoring server log: – `KDS9151E: The heartbeat from remote TEMS` *`variable`* `was not received at its scheduled time and the remote TEMS has been marked offline.`
Diagnostic and corrective actions
1. Check the Managed System Status workspace in the portal client. 2. If the monitoring agent is connected through a remote monitoring server, confirm that the remote monitoring server is connected to the hub monitoring server. 3. If the remote monitoring server is not running and you are an administrator, restart it. Otherwise, notify an administrator and wait for the remote monitoring server to be restarted. 4. Running the following ITMSUPER tools might also provide more information: • Topology tool • Connectivity tool • Agent Response Time tool • TEMS Server Analysis tool 5. Correct the connectivity failures identified.

Tivoli Enterprise Portal Server does not start or stops responding

The following problems might occur:

- Portal client logon fails. See "Tivoli Enterprise Portal logon fails" on page 20.
- The portal server stops responding during normal operation of the portal client.
- You receive message `KFWITM091E: View not available at this time`.
- You receive message `KFWITM010I: Tivoli Enterprise  Portal Server not ready`.
- You receive message `KFWITM402E: Communication with the Tivoli Enterprise Poratl Server could not be established`.
- You find a similar text string to `KFWDBVER, version not found` when trying to start the portal server. See Table 6 on page 18.

Preliminary diagnostics:

1. Refer to the *IBM Tivoli Monitoring Messages* reference guide for more information about any messages received. Operator responses and general information are provided for each message.
2. Allow the portal client enough time to establish a connection with the portal server.
3. Is DB2 running?
   Yes: See step 4.
   No: See Table 8 on page 19.
4. Collect the portal server log or the operations log and look for the following text strings:
   - `KFWDBVER, version not found` see Table 6 on page 18.
   - `TEPS database not found`, see Table 6 on page 18
   - `user ID or password invalid`, see Table 7 on page 18.
   - `DB2 instance not started`, see Table 8 on page 19.
5. Run the TEPS Analysis ITMSUPER tool.

The following tables include possible causes and corresponding solutions for the problems described in this section.

Table 6. Correcting database problems - 1 of 3

• Portal server database is not found or is missing. • Missing table. • Version of portal server does not match version record in database.
Diagnostic and corrective actions
1. Reconfigure the portal server. On Windows: Open Manage Tivoli Monitoring Services, right-click the portal server, and select **Reconfigure**. If the problem still persists, go on to the next step. On Linux or UNIX: • GUI interface Open Manage Tivoli Monitoring Services, right-click the portal server, and select **Reconfigure**. • Command-line interface Run the **./itmcmd config -A cq** command 2. On Windows: Run one of the following commands and set the correct password in the window that is displayed: • For an SQL database `cnpsdatasource.exe` • For an DB2 database `db2datasource.exe` Then run the `buildpresentation.bat` script.

Table 7. Correcting database problems - 2 of 3

Portal server database user password is out of sync. • User ID does not match operating system's logon user ID. • Password does not match operating system's password. • Registry does not have the correct password.
Diagnostic and corrective actions
Reconfigure the portal server. On Windows: Run the **tacmd configureportalserver** command. If the problem persists, see the steps in the following row. On UNIX and Linux: Reconfigure the portal server through the command line or user interface.
You might also need to check the following to make sure that the user ID and password are correct and in sync. On Windows: 1. Make sure your portal client user ID is identical with the logon user ID of your system. – Right-click My Computer and select **Manage**. – Select "Local Users and Groups." – Select **Users**. – Right-click your user ID and select **Properties** to change your password settings. For db2admin, set the password to never expire. 2. Use the correct capitalization for your user ID and password.

Table 7. Correcting database problems - 2 of 3 (continued)

3. Check the DB2 UDB database and make sure the db2admin user ID and password match those of the db2admin local account. – Go to **Control Panel** > **Administrative Tools** > **Services**. – Right-click **DB2 - DB2** and select **Properties**. Select the **Log On** tab and make sure the db2admin user ID and password match the db2admin UDB account. – To check the DB2 user ID and password for the database and data source: Go to **Control Panel** > **Administrative Tools** > **Data Sources (ODBC)** At the **System DSN** tab, select TEPS2 and click **Configure**. Enter your user ID and password. For example: `db2admin` for database and `CNPS` for data source. Click on **Connect** to test the connection to UDB database. – On the **Advanced Settings** tab, verify that the DATABASE name is correct.

Table 8. Correcting database problems - 3 of 3

DB2 instance is not started.
Diagnostic and corrective actions
1. Check the status of the instance in the DB2 Control Panel. 2. Recycle the portal server and resolve any issues reported. 3. Ensure the user ID and password are correct. See Table 7 on page 18 for more information.

Tivoli Enterprise Portal logon fails

The following problems might occur:

- You cannot log on to the portal client.
- You receive one or more of the following error messages:
  - `KFWITM392E: Internal error occurred during logon.`
  - `KFWITM009I: The Tivoli Enterprise Portal Server is still being initialized and is not ready for communications.`
  - `KFWITM010I: Tivoli Enterprise Portal Server not ready.`
  - `KFWITM395E: User ID has been locked or disabled.`
  - `KFWITM396E: User ID has been locked or disabled by Tivoli Enterprise Portal Server.`

Preliminary diagnostics:

- Refer to the *IBM Tivoli Monitoring Messages* reference guide for operator responses.
- Look in the portal server or portal client logs for more information concerning the message.

See "Cannot log in to the Tivoli Enterprise Portal" on page 116 for more symptoms and corrective actions.

Tivoli Enterprise Portal does not respond

During normal operation of the portal client, the client stops running or stops responding.

Preliminary diagnostics:

1. Verify that the monitoring server is started.
2. If you have selected a workspace that is retrieving large amounts of data, wait for the data to be returned. If the workspace returns empty see "Workspaces are missing or views are empty" on page 12.
3. On Windows:
   - Check the Windows Task Manager.
   - Run the **kincinfo.exe** command in the `%CANDLE_HOME\InstallITM` directory:
     - **kincinfo.exe -r** to show running processes.
     - **kincinfo.exe -i** to show what is installed.
4. On Linux or UNIX, run the **cinfo** command in `$CANDLEHOME/bin` directory:
   - **./cinfo -r** to show running processes.
   - **./cinfo –i** to show what is installed.
5. If your portal client stops responding while in an Oracle Agent workspace see Table 21 on page 32. Your problem might be related to a high CPU usage problem. Similar problems might exist for other monitoring agents.
6. Running the following ITMSUPER tools might also provide more information:
   - Stressed Resources tool
   - Connectivity tool
   - Topology tool

The following tables include possible causes and corresponding solutions for the problems described in this section.

Table 9. Correcting storage or memory problems

Specific problem that leads to lack of storage or memory.
Diagnostic and corrective actions
• Reconfigure the Java Control Panel. See "Tivoli Enterprise Portal has high memory usage and poor response time" on page 138.

Table 10. Correcting configuration problems

Incorrect configuration.
Diagnostic and corrective actions
• Disable DirectDraw. See "DirectDraw thread loops infinitely causing poor Tivoli Enterprise Portal performance" on page 139.

Historical data is missing or incorrect

The following problems might occur:

- Workspace is missing historical data.
- Workspace graphs or tables contain short-term but not long-term historical data. (By default, long-term historical data is older than 24 hours.)
- Summarized historical data is not displayed.
- You suspect that the values returned for historical data are incorrect.

Preliminary diagnostics:

1. Verify component connectivity through the Self-Monitoring Topology workspace.

   To open this workspace right-click the Enterprise Navigator item, and then select **Workspace** > **Self-Monitoring Topology**.

   You can also use the workspaces assigned to the Warehouse Proxy and Summarization and Pruning Agent in the physical Navigator view.
2. Verify the configuration of historical data by using the portal client or by issuing the following tacmd commands:

   tacmd histlistproduct

   tacmd histlistattributegroups

   tacmd histviewattributegroup

   tacmd histConfigureGroups

   tacmd histViewAttributeGroup

   tacmd histUnconfigureGroups

   tacmd histStartCollection

   tacmd histStopCollection

The following tables include possible causes and corresponding solutions for the problems described in this section.

Table 11. Correcting Warehouse Proxy connection problems

<table>
<tr><td colspan="2">There is a connection problem to the Warehouse Proxy agent.</td></tr>
<tr><td colspan="2">Possible causes</td></tr>
<tr><td colspan="2">Short-term historical data is stored at the location of the
monitoring agent (see left column below)
-or-
monitoring server (see right column below)
and that component cannot connect to the Warehouse Proxy agent.</td></tr>
<tr><td colspan="2">Diagnostic actions</td></tr>
<tr><td colspan="2">• Make sure the Warehouse Proxy agent is running.
• Look for export failures to the Warehouse Proxy agent in either the monitoring agent RAS1 log or monitoring server RAS1 log. Depending on where the error is found see the coordinating column below.</td></tr>
<tr><td>Monitoring agent:
1. Verify that the correct socket connection is being used.
2. Verify that the monitoring agent is connected to the Warehouse Proxy agent.</td><td>Monitoring server:
1. Verify that the connection between the monitoring server and Warehouse Proxy agent is not being stopped by a firewall.
2. Verify that the correct port is being used for each component.</td></tr>
</table>

Table 11. Correcting Warehouse Proxy connection problems (continued)

Corrective actions	
Store the collected data at the location of the monitoring server to ensure a stable connection.	Consider using a high port number for the monitoring server. See the *IBM Tivoli Monitoring Deployment Guide* for more information on the COUNT and SKIP options for port number allocation.

Table 12. Correcting Warehouse Proxy agent problems - 1 of 2

Monitoring agent or monitoring server is connected to the Warehouse Proxy agent but cannot send data.
Diagnostic actions
Review the current `CTIRA_NCSLISTEN` and `KHD_QUEUE_LENGTH` settings in the Warehouse configuration file.
Corrective actions
Set `CTIRA_NCSLISTEN` equal to at least 20 times the value of `KHD_EXPORT_THREADS`. Increase `KHD_QUEUE_LENGTH` equal to a value greater than the number of agents being handled by that Warehouse Proxy agent.

Table 13. Correcting Warehouse Proxy agent problems - 2 of 2

• Warehouse Proxy agent is unable to send data to the Tivoli Data Warehouse database. • Expired or incorrect database password. • The Warehouse Proxy agent has lost connectivity to the warehouse database.
Diagnostic actions
1. Verify component connectivity through the Self-Monitoring Topology workspace. To open this workspace right-click the Enterprise Navigator item, and then select **Workspace** > **Self-Monitoring Topology**. 2. Verify that the warehouse database password and user ID are correct and have not expired. 3. Look at the Warehouse Proxy agent RAS1 logs for export resource availability timeout. The Warehouse Proxy agent might be unable to export because it is too busy.
Corrective actions
Update the configuration parameters. See "Tivoli Data Warehouse environment variables" on page 280 for a list of warehouse proxy environment variables.

Table 14. Correcting Summarization and Pruning Agent problems

• Summarization and Pruning Agent yields unexpected values. • Unanticipated attribute behavior leads to unexpected data.
Diagnostic actions
1. Look at a workspace view that shows real-time data and compare it with the unexpected data. 2. The *Tivoli Management Services Warehouse and Reporting* IBM Redbooks® publication discusses aggregation methods used by the Summarization and Pruning Agent. This Redbook might help you understand how data is aggregated for various data types.
Corrective actions
Review documentation for the monitoring agents that are generating the unexpected values to clarify the expected types of values for the attributes in question.

Table 15. Correcting persistent data store for z/OS problems

Incorrect configuration of the persistent data store for z/OS agents.
Diagnostic and corrective actions

1. Is historical data configured to be collected at the agent or the monitoring server? (If the agent is configured in the address space of the monitoring server, then historical data can be collected only at the monitoring server.)
If at the monitoring server, see "2."
If at the agent, see "3."
 	
2. Check the RKPDLOG output of the monitoring server to verify that the persistent data store is configured correctly. For example:
`2008/07/28 08:45:41 KPDIFIL: Status of files assigned to group GENHIST:`
`2008/07/28 08:45:41 ----------------------------------------------------`
`2008/07/28 08:45:41 &philev.RGENHIS3          Status = Active`
`2008/07/28 08:45:41 &philev.RGENHIS2          Status = Offline`
`2008/07/28 08:45:41 &philev.RGENHIS1          Status = Offline`
`2008/07/28 08:45:41 ----------------------------------------------------`
`2008/07/28 08:45:41 KPDIFIL: End of group GENHIST status.`
 	
See "4" on page 25 for various error codes to look for in the RKPDLOG.
 	
3. Check the RKPDLOG of the agent to verify that the persistent data store is configured correctly at the agent. For example:
If KM5AGENT (this agent runs in the monitoring server), check the RKPDLOG of the monitoring server:
`2008/07/28 08:48:27 KPDIFIL: Status of files assigned to group PLEXDATA:`
`2008/07/28 08:48:27 ----------------------------------------------------`
`2008/07/28 08:48:27 &philev.RKM5PLX3          Status = Active`
`2008/07/28 08:48:27 &philev.RKM5PLX2          Status = Empty`
`2008/07/28 08:48:27 &philev.RKM5PLX1          Status = Partially Full`
`2008/07/28 08:48:27 ----------------------------------------------------`
If the MQ agent is running in its own address space check its RKPDLOG:
`2008/07/28 08:44:18 Response: &philev.RMQSGRP3      1700     83     14  5000 Active   Write`
`2008/07/28 08:44:18 Response: &philev.RMQSGRP2      1700     25      0  5000 Empty    Read Access`
`2008/07/28 08:44:18 Response: &philev.RMQSGRP1      1700     25      0  5000 Empty    Read Access`
`2008/07/28 08:44:18 Response: &philev.RKMQPDS3     23327     31      0  4000 Empty    Read Access`
`2008/07/28 08:44:18 Response: &philev.RKMQPDS2     23327   6598    143  4000 Partial  Read Access`
`2008/07/28 08:44:18 Response: &philev.RKMQPDS1     23327   3523    105  4000 Active   Write`
 	
See "4" on page 25 for various error codes to look for in the RKPDLOG.

Table 15. Correcting persistent data store for z/OS problems (continued)

4. The following are examples of persistent data store error codes found in the RKPDLOG:
   - **Error code 25804**:

     Indicates that an attempt was made to read slot 0 of the GENHIST dataset. This is a protected record and the persistent data store will not allow the slot to be read. One possible cause is a problem with DELETE processing. The warehouse code, which is the only code that attempts to use the delete logic, might be generating bad condition.

     Run the **RECOVERY** command which will save the data and rebuild the indexes so that the data is once again usable.
   - **Error code 3205**:

     The last 3 digits represent the error and the beginning digits represent the persistent data store function that was being called. The 205 indicates the error **RowExceedsFileFormat**.

     This error is generated if the row you attempt to insert is larger than what will fit in a block allocated to the persistent data store data set. The actual maximum length is about 100 bytes smaller than the block size. Therefore, if you allocate a block size of 1000 (Window=1) and attempt to write a row greater then 900, you receive this message. The persistent data store cannot span a data row across multiple blocks. One other possibility is that either the API calls to the persistent data store to do the insert are specifying an invalid row length or the lengths of all the columns put together for the insert exceed the buffer length.
   - **Error code 35404**:

     This code has many causes. One possibility is that a PARMA parameter intended for the agent processing is mistakenly set to the monitoring server and interpreted as a column name. This might be due to obsolete SQL saved in the monitoring server database. In most cases you can ignore this error. Set monitoring server traces to (`UNIT:kdssqprs input,error`).

     The `UNIT:kdssqprs input,error` trace returns large amounts of data. Turn the trace off as soon as you finish troubleshooting.
   - **KFAPERR : error code 14209**:

     Persistent data store Filename is Not Available messages in the RKLVLOG of an agent or monitoring server on z/OS: Error 8 trying to set up table <table-name>, KRAIRA000, Starting UADVISOR_K*pp*_table-name, where *pp* is the two-character component or product code and table-name is the application table name.
5. Verify that the files are not being used by another task.
6. Verify that the files are initialized correctly and that the K*pp*PDICT is inserted into the persistent data store files.
7. Verify that the maintenance procedure is correctly processing the persistent data store files.

For further information about the persistent data store, see *OMEGAMON XE and Tivoli Management Services on z/OS: Common Planning and Configuration Guide*.

A situation does not raise when expected

You are working in the portal client or Tivoli Enterprise Console and know that conditions exist that should have raised a situation, but the situation has not been raised.

Preliminary diagnostics:

1. Verify that the monitoring agent has started.
2. Verify whether the situation is associated with a node in the Tivoli Enterprise Portal Navigator.
3. Confirm the situation is raised in the event console.
4. Verify that maintenance has not been run against situations. One possible tacmd command that could have been run is the **tacmd maintAgent**. If maintenance has been run, wait for the situation to restart.
5. Click on any workspace where the data should be, and verify that data is arriving.
6. Running the following ITMSUPER tools might also provide more information:
   - Situation Test tool
   - Exceptions Analysis tool
   - Distributions Analysis tool

The following tables include possible causes and corresponding solutions for the problems described in this section.

Table 16. Correcting situation-specific problems

• The situation is distributed to an incorrect managed system. • The situation is not associated with a node in the Navigator. • The situation is formulated incorrectly.
Diagnostic and corrective actions

1. Verify that the situation was started by checking one of the following log files for text strings based on the specific situation:
– Agent operations log
For example:
`106111012573100OKRAIRA000 Starting FireOnWednesday <7340776,3145895> for KPX.LOCALTIME`
– Monitoring server log
For example:
`11/13/06 15:07:21 KO41046 Monitoring for enterprise situation FireOnWednesday started.`
Did the situation start?
Yes: See step "4" on page 28.
No: See step "2" on page 27.

Table 16. Correcting situation-specific problems (continued)

2. Is the situation distributed to the agent and is the agent online?

Look for a text string similar to this one in the monitoring server log:

```
KO41047 Situation CheckIfSituationCreated distribution Primary:KATE:NT added.
```

Yes: See step "4" on page 28.

No: Use (`UNIT:kpxreqds all`) to trace the distribution at the monitoring server for a situation.

The following example is taken from a monitoring server log:

```
(4558D8CC.0033-1114:kpxreqds.cpp,621,"DetermineTargets") Active RAS1
  Classes: EVERYT EVERYE EVERYU
(4558D8CC.0034-1114:kpxreqds.cpp,661,"determineTargetsFromNodelist") Active RAS1
  Classes: EVERYT EVERYE EVERYU
(4558D8CC.0035-1114:kpxreqds.cpp,661,"determineTargetsFromNodelist") Entry
(4558D8CC.0036-1114:kpxreqds.cpp,669,"determineTargetsFromNodelist") Exit
(4558D8CC.0037-1114:kpxreqds.cpp,821,"determineTargetsFromAccessList") Active RAS1
  Classes: EVERYT EVERYE EVERYU
(4558D8CC.0038-1114:kpxreqds.cpp,821,"determineTargetsFromAccessList") Entry
(4558D8CC.0039-1114:kpxreqds.cpp,837,"determineTargetsFromAccessList")
  Calling KFA_GetAccessListNodes for NT_Paging_File_Critical, 5140
(4558D8CC.003A-1114:kpxreqds.cpp,852,"determineTargetsFromAccessList") Node #0 Primary:KATE:NT
(4558D8CC.003B-1114:kpxreqds.cpp,891,"determineTargetsFromAccessList")
  Deleting NodeRecEntry: #0, node_entries @0x1B63B90, next @0xNULL, ptr_next @0xNULL
(4558D8CC.003C-1114:kpxreqds.cpp,898,"determineTargetsFromAccessList") Exit
```

3. Did the agent return data?

On the monitoring server set this trace level (`UNIT:kpxrpcrq ERROR STATE`) to show the number of rows returned by each agent.

```
(3A933B00.24A827C0-154:kpxrpcrq.cpp,547,"IRA_NCS_Sample")
  Rcvd 1 rows sz 448 tbl *.NTLOGINFO req NT_Log_Space_Low <4294706777,761> node <Primary:NODE1:NT
```

Yes: See step "5" on page 28.

No: Is the situation authored correctly? At the agent, trace (`UNIT:kdsfilt all`)

Yes: The problem might be related to the monitoring agent. See the Troubleshooting appendix of the distributed agent's User's Guide or the Troubleshooting Guide of the z/OS monitoring agent.

No: See step "4" on page 28.

Table 16. Correcting situation-specific problems (continued)

4. Look in the log of the monitoring server to which the agent is attached. Search for the situation name and look for any errors logged.

– Catalog errors (message return codes 202 and 209). Ensure the application support is installed at the monitoring server.

– Message KO41046 is missing – situation failed to lodge message:

```
KO41039    Error in request MCS_Sit. Status= 1133. Reason= 1133.
KO41039    Error in request MCS_Sit. Status= 1131. Reason= 1131.
(4558E8EF.0079-11A4:ko4sitma.cpp,782,"IBInterface::lodge") error: Lodge <1131>
(4558E8EF.007A-11A4:ko4ibstr.cpp,659,"IBStream::op_ls_req") IB Err: 1131
(4558E8EF.007B-11A4:ko4sit.cpp,658,"Situation::slice") Sit MCS_Sit: Unable to lodge - giving up.
KO48156    Not able to start monitoring for situation MCS_Sit.
```

– SITMON/IB Lodge errors

- Attribute file is incorrect (wrong version) or missing and the RULE could not be created.
- A value of 1133 or 1203 leads to a value of 1131.
- A value of 1145 generally means that the referenced situation either has been deleted or has not been distributed correctly.

```
#define ERR_LODGEERROR          1131   // Bad lodge request
#define ERR_NOATTRIBUTE         1133   // No attribute found
#define ERR_DUPLICATEINSERT     1144   // Duplicate record exists
#define ERR_INVALIDSITNAME      1145   // Invalid sitname supplied
#define ERR_RULESYNTAX          1203   // Generic rule syntax error
```

5. Did SITMON receive the data?

Monitoring server trace (UNIT:ko4async ERROR STATE FLOW) (UNIT:ko4tobje ALL) (UNIT:ko4sitma ALL)

Yes: Does the situation apply to the Enterprise?

For example: *ENTERPRISE in the MSG2 message of the monitoring server message log when the situation was created?

```
11/08/06 16:18:49 KO46256 Situation definition CheckIfSituationCreated created by *ENTERPRISE.
```

Only Enterprise situations show up in the portal client user interface. A non-Enterprise situation does not show up in the portal client user interface, even if the situation is raised. The distinction between Enterprise and non-Enterprise situations is seen in the following monitoring server log examples:

- Enterprise situation `KO41046 Monitoring for enterprise situation MS_Offline started.`
- Non-Enterprise situation `KO41036 Monitoring for situation Weekday started.`

  Yes: See step "6."

  No: Reconfigure the situation to include the Enterprise flag setting.

No: Use the Monitoring server trace (UNIT:kdsruc1 ERROR STATE) (UNIT:kfaadloc all) to see where the data is getting filtered out.

This trace generates a large amount of data. Turn the trace off as soon as you finish troubleshooting.

6. Is there a MSG2 message indicating the situation raised?

Yes: Contact IBM Software Support. See Chapter 2, "Collecting and reviewing troubleshooting data," on page 5 for information on what types of data to collect before contacting Support.

Table 17. Correcting application support problems

Lack of application support, or application support level mismatch among components (monitoring server, portal server, and monitoring agents).
Diagnostic and corrective actions
See Table 1 on page 13 for instructions on updating application support.

A reflex automation script does not run when it should

An action that should have occurred after a situation raised, did not occur.

Preliminary diagnostics:

If the situation did not raise see "A situation does not raise when expected" on page 26.

Table 18. Correcting format and variable problems

• The situation or script is not formulated correctly. • Authentication or environment variable problems. (Begin at step "3.")
Diagnostic and corrective actions
1. Does the system command run correctly from a command line? **Yes**: Go on to the next step. **No**: Verify that the command typed in is correct. 2. Is the length of the command within the limit for your operating system? **Yes**: Go on to the next step. **No**: The command cannot be executed on this platform. You might be able to write a wrapper script to issue the command. 3. Are the required user type and environment variables correct? **Yes**: Go on to the next step. **No**: Include the **set** command in the shell script or batch script and redirect the output to a file. Review the file afterwards to show which variables are being used. 4. Collect the monitoring agent operations log, which shows whether reflex automation occurred. A monitoring server message log also confirms what error occurred. 5. Correct the identified problem.

High CPU usage on a distributed system

The following problems might occur:

- Performance degrades or availability is lost because of high processing in an application or a computer.
- No data is returned in the portal client and the collector log contains the text string `Open Probe pipe error`. See Table 21 on page 32.
- Situations alert you frequently about a managed system cycling between online and offline. See Table 20 on page 31.

Preliminary diagnostics:

1. Determine whether an IBM Tivoli Monitoring component is the root cause. Another application or process running on the system might be causing high CPU usage.

   On Windows:
   Use the tools and data provided by Task Manager to identify the process causing high CPU usage. In the **Processes** tab you can reorder the processes by CPU usage. An example of a process name is `kntcma.exe` for the Windows OS agent.

   On UNIX and Linux:
   Use the **top** command to display processes using high CPU. For UNIX, you can also use the **ps auxww** command.
2. Verify the following:
   - Is historical data collection enabled?
   - Is the database undergoing a backup?
3. Is the situation writing a lot of Windows event logs?
   Yes: Disable all event log monitoring situations.
4. Select each of the workspaces in turn, to see which one is consuming high CPU.
5. Running the following ITMSUPER tools might also provide more information:
   - Stressed Resources tool
   - Connectivity tool
   - Situations tool
6. When the computer where the monitoring agent is running has multiple Network Interface Cards (NICs), the agent might not be bound to the Primary NIC and therefore might not be able to establish connectivity with the monitoring server. High CPU usage can result from the agent's frequent attempts to connect.

   To correct this you might need to set the environment variable `KDEB_INTERFACELIST='!*'` or `KDEB_INTERFACELIST=`*`IP_address`*, where *IP_address* is the address of the NIC. Make the changes in the associated agent `*ENV` configuration file for Windows, or the `*.ini` configuration file for UNIX or Linux.

The following tables include possible causes and corresponding solutions for the problems described in this section.

Table 19. Correcting situation problems

A situation is causing the high CPU usage problem.
Diagnostic actions
1. Run the Situation Test ITMSUPER tool. 2. Find out which situations have been deployed to the monitoring agent. On Windows: Open the agent-specific `.lg0` file found in the *`install_dir\TMAITM6\logs`* directory to view a list of situations started for that agent. On UNIX and Linux: Open the agent-specific `.lg0` file found in *`install_dir/logs`* directory. 3. Examine the situation definition and formula. 4. Does the situation contain any wildcard * characters against UTF8 columns? **Yes**: See corrective actions below. 5. Switch between situations to see which one is causing the high CPU.
Corrective actions
• Change the formulation of any situations that are causing excessive processing. • For situations with wildcard * characters: Rewrite the situation using the SCAN strcscan function instead of the character-by-character pattern-matching function LIKE. For example, situations with this simple `LIKE"*/process"` pattern can be rewritten as `SCAN "/process"`. -OR- Rewrite the situation using non-UTF8 columns. For example, `*IF *LIKE NT_System.User_Name_U *EQ '*group'` can be rewritten as `*IF *LIKE NT_System.User_Name *EQ '*group'` where `User_Name` is a non-UTF8 column and `User_Name_U` is the corresponding UTF8 column. -OR- Rewrite the situation combining predicates with an `OR`. For example, `*IF *LIKE NT_System.User_Name_U *EQ 'group*'` can be rewritten as `*IF ( ( *VALUE NT_System.User_Name_U *EQ 'groupA' ) *OR ( *VALUE NT_System.User_Name_U *EQ 'groupB' ) *OR ( *VALUE NT_System.User_Name_U *EQ 'groupC' ) )`

Table 20. Correcting firewall problems

• A firewall interference problem. • Communication layer cannot establish communication with the monitoring server
Diagnostic actions
• Check connectivity between monitoring agent and monitoring server. • Use the **ping** command to verify whether communication exists between the monitoring server and agents. Ping from the monitoring agent system to the monitoring server, and then from the monitoring server system to the monitoring agent. Use the IP address of the host name specified during agent configuration. If the communication is broken and you see high CPU proceed to the corrective actions. • Turn on the RAS1 trace log to verify whether the monitoring agent has made a connection to the monitoring server. See "Setting traces" on page 42 for more information.
Corrective actions
If you still have high CPU usage issues even after ensuring proper connectivity across firewalls, open a problem report with IBM Software Support. For more information refer to the *IBM Tivoli Monitoring Installation and Setup Guide*.

Table 21. Correcting Oracle DB Agent problems

Oracle DB Agent cursor performance problem. • Oracle Agent does not return any data to the portal client. • Oracle Agent consumes high CPU on the system.
Diagnostic actions

1. Collect the detail traces of collector and RAS1 log.
Refer to "Enabling detailed tracing in the collector trace log " and "Setting RAS trace parameters" in Appendix E. Problem determination, in the *IBM Tivoli Monitoring for Databases: Oracle Agent User's Guide*.
2. Identify the SQL query that caused the high CPU usage issues from the collector logs.
You can identify the SQL query that caused the high CPU usage issue from Tivoli Monitoring Oracle Agent logs or the Oracle tools. Use the following procedure to identify the problematic cursors from Tivoli Monitoring Oracle Agent logs:
– Open the collector logs and find `CFE1645` messages. The messages show the return time of each cursors. For example: `CFE1645T (165929) Time = 2008/06/06 16:59:29, collected records in 6 seconds`.
– The default timeout value of Tivoli Monitoring Oracle Agent is 45 seconds. If it takes more than 45 seconds, it might cause a timeout problem and `Open Probe pipe error` will be reported in the collector log.
`CFE1645T (170246) Time = 2008/06/06 17:02:46, collected records in 203 seconds`
– When a timeout happens, review the previous cursor that executed before this message. For example:
`PDR3000T (170002) Deleting (1) rows for cursor DB6`
`RPF0300T (170002) Doing prep_l_fet for cursor DB6`
`ORU0085I (170002) ----------`
`ORU0090I (170002) Starting new SQL query.`
`ORU0095I (170002) <SELECT /*+RULE*/ COUNT(*) EXTENTS FROM SYS.DBA_EXTENTS >`
`ORU0085I (170002) ----------`
`CAT1610I (170213) Dump of row 1`
`UPX0100T 000: 20202020 20202020 20202032 34313135 * 24115*`
The previous cursor (DB6) took about 2 minutes and 11 seconds to return data causing the performance problem.
Were you able to identify and SQL query?
Yes: See Corrective action "1."

Corrective actions
Note: The following corrective actions are available only for products that include the 6.2.0-TIV-ITM_ORA-LA0001 limited availability fix, and higher.
1. Disable the problematic cursors by setting an environment variable. On Windows: `COLL_DISABLE_CURSORS` On UNIX and Linux: `db_extparms`

Table 21. Correcting Oracle DB Agent problems (continued)

Set the environment variables as follows:

– On Windows:
  - Launch Manage Tivoli Enterprise Monitoring Services.
  - Right-click the row that contains the name of the monitoring agent whose environment variables you want to set.
  - Select **Advanced** > **Edit Variables** in the pop-up menu.
  - If the agent is running, accept the prompt to stop the agent.
  - The list window is displayed. When only the default settings are in effect, no variables are displayed. The variables are listed after you override them.
  - Override the variable settings as follows:
    a. Click **Add**.
    b. Select the **COLL_DISABLE_CURSORS** in the Variable pull-down menu. If it is not there, you can add it.
    c. Type a value in the **Value** field.
    d. Select **OK** twice.
    e. Restart the agent.

– On UNIX and Linux:

  Use a text editor to enter a new value for the `db_extparms` variables in the *hostname_or_instance_name.cfg* file in the *install_dir/config* directory.

The cursors that are listed below take longer to return data and consume excessive system resources in some customer environments:
DB3, DB6, KF1, KF4, STATLTRN, TS1, TS3, TS5, and TS6.

Each comma-delimited, no white space, value represents a change to the SQL cursor that is executed during data gathering operations within the agent. The values are the SQL cursor name. For example, setting the **Extended Parameters** field to `DB3,TS1` means that the `DB3` and `TS1` SQL cursor is enabled for `Set FREEBYTES to zero`, `Set TSNEXTS to zero`, and `Set MAXEXTTS to zero`. The SQL cursor name is not case sensitive.

2. Recycle the Monitoring Agent for Oracle to recognize these changes to the `Extended Parameters` value.

Using the name of the SQL cursor, you can look in the *korcoll.ctl* file for the SQL modification that is done when the SQL cursor is enabled. The *korcoll.ctl* file is located in the following locations:

On Windows: *%CANDLE_HOME%\TMAITM6*

On UNIX and Linux: *$CANDLEHOME/misc*

When these cursors are enabled, the Monitoring Agent for Oracle displays default attribute values of these cursors in the Tivoli Enterprise Portal, meaning, the Monitoring Agent for Oracle no longer monitors the attributes of the enabled cursors.

Table 21. Correcting Oracle DB Agent problems (continued)

An example of an SQL cursor is displayed below:

```
SQL cursor: DB3 - ARCHIVE LOG DISPLAY
   SQL:
       SELECT  TABLESPACE_NAME   UTSNAME,
          SUM(BYTES)        FREEBYTES
       FROM    SYS.DBA_FREE_SPACE
       GROUP BY TABLESPACE_NAME;

   Enabled: Set FREEBYTES to zero

   Navigation Tree : Databases->Database Summary
     Workspace: Oracle_Database/Database Summary->Database Summary(Bar Chart View)
                Oracle_Database/Database Summary->Database Summary(Table View)
                  Column : DB Percent Free Space = 0
                           System TS Percent Free = 0

   Navigation Tree : Databases->Enterprise Database Summary
     Workspace: Oracle_Statistics_Enterprise/Databases Global->Database Summary(Bar Chart View)
                Oracle_Statistics_Enterprise/Databases Global->Database Summary(Table View)
                  Column : System TS Percent Free = 0

   Situation: Oracle_DB_PctFree_Space_Low = always true
              Oracle_SystemTS_PctFree_Critica = always true
              Oracle_SystemTS_PctFree_Warning = always false
```

For more information on the cursors refer to the *Oracle Agent 6.2.0-TIV-ITM_ORA-LA0001 README* or a higher version of the *README*.

Chapter 4. Tools

IBM Tivoli Monitoring provides several tools; some include functionality for diagnosing problems. The primary diagnostic tool of IBM Tivoli Monitoring is logging. *Logging* refers to the text messages and trace data generated by the software. Messages and trace data are sent to an output destination, such as a console screen or a file.

Trace logging

Trace logs capture information about the operating environment when component software fails to operate as intended. The principal log type is the reliability, availability, and serviceability (RAS) trace log. RAS logs are in the English language only. The RAS trace log mechanism is available on the Tivoli Enterprise Monitoring Server, the Tivoli Enterprise Portal Server, and the monitoring agent. By default, the logs are stored in the installation path for IBM Tivoli Monitoring. IBM Software Support uses the information captured by trace logs to trace a problem to its source or to determine why an error occurred. The default configuration for tracing, such as whether tracing is enabled or disabled and trace level, depends on the source of the tracing. You can choose how many files to keep when the log rolls. If you cannot find the log files you need, restart the system and try again. This section includes instructions for configuring trace logging.

Table 22 lists the location of the log files directories.

Table 22. Location of log files on the Tivoli Enterprise Monitoring Server

Component	Windows	UNIX-based systems
Tivoli Enterprise Portal Server	*install_dir*\logs	*install_dir*/logs/ hostname_PC_*timestamp*.log where: *install_dir* Specifies the directory where Tivoli Enterprise Portal Server was installed. *hostname* Specifies the name of the system hosting the product. *PC* Specifies the product code. cq for the Tivoli Enterprise Portal Server. *timestamp* A decimal representation of the time at which the process was started.
Tivoli Enterprise Portal browser client	C:\Documents and Settings\ Administrator\ Application Data\ Java\Deployment\ log\plugin142.trace	None.

Table 22. Location of log files on the Tivoli Enterprise Monitoring Server (continued)

Component	Windows	UNIX-based systems
Tivoli Enterprise Portal desktop client	*install_dir*\CNP\kcjerror.log *install_dir*\CNP\kcjras1.log When launched via Java Web Start: %USERPROFILE%\Application Data\IBM\Java\Deployment\log\javawsnnnnn.trace where 'nnnnn' is a unique, randomly generated numeric suffix to support generational logs (for example, the last generated log will not be overlayed by the most current execution of Tivoli Enterprise Portal using Java Web Start. This is in contrast to the Tivoli Enterprise Portal Browser client, which has a fixed name and is overlayed with each execution cycle.	*install_dir*/logs/hostname_PC_*timestamp*.log where: *install_dir* Specifies the directory where Tivoli Enterprise Portal Server was installed. *hostname* Specifies the name of the system hosting the product. *PC* Specifies the product code. cq for the Tivoli Enterprise Portal Server. *timestamp* A decimal representation of the time at which the process was started. When launched via Java Web Start: ${user.home}/.java/deployment/log/javawsnnnnn.trace where 'nnnnn' is a unique, randomly generated numeric suffix to support generational logs (for example, the last generated log will not be overlayed by the most current execution of Tivoli Enterprise Portal using Java Web Start. This is in contrast to the Tivoli Enterprise Portal Browser client, which has a fixed name and is overlayed with each execution cycle.
Tivoli Enterprise Monitoring Server	*install_dir*\logs*hostname_PC_HEXtimestamp-nn*.log where: *install_dir* Specifies the directory where Tivoli Enterprise Monitoring Server was installed. *PC* Specifies the product code. ms for Tivoli Enterprise Monitoring Server *HEXtimestamp* A hexadecimal representation of the time at which the process was started. *nn* Represents the circular sequence in which logs are rotated. Ranges from 1-5, by default, though the first is always retained, since it includes configuration parameters.	*install_dir*/logs/*hostname_PC_timestamp*.log where: *install_dir* Specifies the directory where Tivoli Enterprise Portal Server was installed. *hostname* Specifies the name of the system hosting the product. *PC* Specifies the product code. cq for the Tivoli Enterprise Portal Server. *timestamp* A decimal representation of the time at which the process was started.

Table 22. Location of log files on the Tivoli Enterprise Monitoring Server (continued)

Component	Windows	UNIX-based systems
Monitoring agents	*install_dir*\tmaitm6\logs*hostname_PC_HEXtimestamp-nn*.log where: *install_dir* Specifies the directory where monitoring agent was installed. *PC* Specifies the product codes, for example, um for Universal Agent or nt for Windows. *HEXtimestamp* A hexadecimal representation of the time at which the process was started. *nn* Represents the circular sequence in which logs are rotated. Ranges from 1-5, by default, though the first is always retained, since it includes configuration parameters.	*install_dir*/logs/*hostname_PC_timestamp*.log where: *install_dir* Specifies the directory where Tivoli Enterprise Portal Server was installed. *hostname* Specifies the name of the system hosting the product. *PC* Specifies the product code. cq for the Tivoli Enterprise Portal Server. *timestamp* A decimal representation of the time at which the process was started.
IBM Tivoli Warehouse Proxy agent	*install_dir*\logs*hostname_PC_timestamp*.log where *PC* Specifies the product code. hd is the product code for the IBM Tivoli Warehouse Proxy agent	Not supported.
IBM Tivoli Summarization and Pruning agent	The Summarization and Pruning Agent uses C-based RAS1 tracing, Java-based RAS1 tracing and Java-based internal tracing. By default, Summarization and Pruning Agent trace data is written to a file in the logs subdirectory.	
	install_dir\logs*hostname_PC_HEXtimestamp-nn*.log *install_dir*\logs*hos tname_PC_ras1java_HEXtimestamp-nn*.log *install_dir*\logs*hostname_PC_java_HEXtimestamp-nn*.log	*install_dir*/logs/*hostname_PC_HEXtimestamp-nn*.log *install_dir*/logs/*hostname_PC_ras1java_HEXtimestamp-nn*.log *install_dir*/logs/*hostname_PC_java_HEXtimestamp-nn*.log
	where: *install_dir* Specifies the directory where monitoring agent was installed. *PC* Specifies the product codes, for example, sy for IBM Tivoli Summarization and Pruning agent. *HEXtimestamp* A hexadecimal representation of the time at which the process was started. *nn* Represents the circular sequence in which logs are rotated. Ranges from 1-5, by default, though the first is always retained, since it includes configuration parameters.	

Table 22. Location of log files on the Tivoli Enterprise Monitoring Server (continued)

Component	Windows	UNIX-based systems
IBM Tivoli Enterprise Console Event Forwarder	*install_dir*\logs*hostname_PC_HEXtimestamp-nn*.log where: *install_dir* Specifies the directory where Tivoli Enterprise Monitoring Server was installed. *PC* Specifies the product code. ms for Tivoli Enterprise Monitoring Server *HEXtimestamp* A hexadecimal representation of the time at which the process was started. *nn* Represents the circular sequence in which logs are rotated. Ranges from 1-5, by default, though the first is always retained, since it includes configuration parameters.	*install_dir*/logs/*hostname_PC_timestamp*.log install_dir/logs/hostname_PC_HEXtimestamp-nn.log where: *install_dir* Specifies the directory where Tivoli Enterprise Portal Server was installed. *hostname* Specifies the name of the system hosting the product. *PC* Specifies the product code. cq for the Tivoli Enterprise Portal Server. *timestamp* A decimal representation of the time at which the process was started.
IBM Tivoli Enterprise Console Situation Update Forwarder	c:\tmp\itmsynch\logs\synch_trace.log c:\tmp\itmsynch\logs\synch_msg.log	/tmp/itmsynch/logs/synch_trace.log tmp/itmsynch/logs/synch_msg.log
	Note: IBM Tivoli Enterprise Console Situation Update Forwarder logs are created on the IBM Tivoli Enterprise Console server.	

The log files are managed as follows:

- On Windows, the log file name includes a time stamp in hexadecimal format. By default, the logs are stored in the installation path for IBM Tivoli Monitoring. The following is an example of a log file name that includes the time stamp in hexadecimal format:

  ibm-kpmn803v01_cq_472649ef-01.log
- On UNIX-based systems, the log file name includes a time stamp. The UNIX-based systems RAS1 log files are stored in the /logs directory. The following is an example of a log files name that includes the time stamp:

  f50pa2b_ux_1112097194.log
- On Linux systems using the Firefox browser:

  candle_home/.java/deployment/log

Note: When you communicate with IBM Software Support, you must capture and send the RAS1 log that matches any problem occurrence that you report.

Installation log files

The following table lists and describes the log files created during installations.

Table 23. Installation log files

Windows	UNIX-based systems
• `ITM_HOME\InstallITM\Abort<Product_name><date_timestamp>.log` This log is created if an abort occurs for either a first time install or a modification of previous installation of IBM Tivoli Monitoring. • `ITM_HOME\InstallITM\<Product_name>_<timestamp>.log` This log is created during a normal clean installation. • `ITM_HOME\InstallITM\MOD_<Product_name>timestamp.log` This log is created if you modify an existing product specified with the PC, or when adding or deleting components. where: *Product_name* Specifies the product name. `IBM Tivoli Monitoring 20050923 1815.log` is the log file name for the IBM Tivoli Monitoring installation CD. *timestamp* A decimal representation of the time at which the process was started.	`$CANDLEHOME/logs/candle_ installation.log`

You can find a log for uninstallation on Windows in the root directory where the product was installed:

`Uninstall<PC><date_timestamp>.log`

Windows installer and configuration logs

You can obtain details about the GUI and silent installation (or upgrade) process through logging and tracing information. You can set the degree of logging and tracing to one of the following levels:

- DEBUG_MIN
- DEBUG_MID
- DEBUG_MAX

By default, logging and tracing is set to DEBUG_MIN. Higher levels give you more detailed information about the installation process. This can be useful for investigating any problems or errors that occur.

Level name	What is logged or traced
DEBUG_MIN	Most important method entries, exits and trace messages are traced
DEBUG_MID	Most of the method entries, exits and trace messages are traced
DEBUG_MAX	All of the method entries, exits and trace messages are traced

You can set the level of logging and tracing by using the **/z** flag when you execute the `setup.exe` file in the CLI.

- For GUI installation use one of the following commands:
  - `setup.exe /zDEBUG_MAX`
  - `setup.exe /zDEBUG_MID`
  - `setup.exe /zDEBUG_MIN`

- For silent installation use one of the following commands:
  - `start /wait setup /z"DEBUG_MAX/sfC:\temp\SILENT_SERVER.txt" /s /f2"C:\temp\silent_setup.log"`
  - `start /wait setup /z"DEBUG_MID/sfC:\temp\SILENT_SERVER.txt" /s /f2"C:\temp\silent_setup.log"`
  - `start /wait setup /z"DEBUG_MIN/sfC:\temp\SILENT_SERVER.txt" /s /f2"C:\temp\silent_setup.log"`

UNIX installer and configuration logs

For tracing and logging java code (that is run on UNIX systems), this mechanism enables problem debugging. Two sets of information are created – logs and traces. Logs (*.log) are globalized and traces (*.trc) are in English. They contain entry and exit parameters of method and stack traces for exceptions. The amount of information traced depends on the level of tracing set.

Level name	What is logged or traced
LOG_ERR	Only exceptions and errors are logged and traced
LOG_INFO	Also log messages are logged and traced - DEFAULT
DEBUG_MIN	Also most important method entries, exits and trace messages are traced
DEBUG_MID	Most of the method entries, exits and trace messages are traced
DEBUG_MAX	All of the method entries, exits and trace messages are traced

The level can be set in configuration files or by exporting an environment variable called TRACE_LEVEL with one of the values mentioned above. Configuration of RAS settings is stored in the following files:

- CH/config/ITMInstallRAS.properties (for installation)
- CH/config/ITMConfigRAS.properties (for configuration)

Callpoints are the only component that is handled differently, their logs and traces always go to the directory CH/InstallITM/plugin/executionEvents. The default location for installation is CH/logs/itm_install.log(.trc) and for configuration it is CH/logs/itm_config.log(.trc).

To gather all the needed logs and environment information in case of an error, use the pdcollect tool described in “pdcollect tool” on page 59.

Component	Location	File name
Install logs/traces	CH/logs	candle_installation.log itm_install.log (.trc)
Config logs/traces	CH/logs	itm_config.log (.trc)
Logs for component startup	CH/logs	pc.env (lists env variables passed to the agent) hostname_pc_ID.log

Component	Location	File name
Callpoint logs/traces	CH/InstallITM/plugin/ executionEvents /logs/timestamp/ install(config)/ plugin_type/pc	callpoint.trc (.log) *.stderr *.stdout

Upgrading from Tivoli Distributed Monitoring log file

All upgrade actions performed by the IBM Tivoli Monitoring Upgrade Toolkit are recorded in a central log with an associated user ID and a time stamp. Upgrade actions taken outside of the Upgrade Toolkit are not recorded in the log. The detailed results from running the Upgrade Toolkit are recorded in a log file.

Table 24. Upgrading from Tivoli Distributed Monitoring log file

Windows	UNIX-based systems
$DBDIR/AMX/logs/log_*tool*_ *timestamp*.log	*$DBDIR*/AMX/logs/log_*tool*_ *timestamp*.log

where:

$DBDIR
The Tivoli Management Environment Framework environment variable that specifies the directory where the Object Repository (odb.bdb) is located.

tool Specifies the IBM Tivoli Monitoring Upgrade Toolkit tool: witmscantmr, witmassess, or witmupgrade.

timestamp
Specifies a time stamp that includes data and time of execution.

For example: `log_witmscantmr_20050721_15_30_15.log`

The log file name displays when the Upgrade Toolkit tool completes the upgrade operation. Each time a Upgrade Toolkit tool runs, its generates a new log file that is never reused by any tool. The contents of the log file conform to the Tivoli Message Standard XML logging format. The following example is an excerpt from an Upgrade Toolkit tool log file:

```
<Message Id="AMXUT2504I" Severity="INFO">
<Time Millis="1121977824199"> 2005.07.21 15:30:24.199 CST </Time>
<Server Format="IP">YFELDMA1.austin.ibm.com</Server>
<ProductId>AMXAMX</ProductId>
<Component>ScanTMR</Component>
</Component>1</ProductInstance>
<LogText><![CDATA[AMXUT2504I The software is creating a new baseline file
C:\PROGRA~1\Tivoli\db\YFELDMA1.db\AMX\shared\analyze\scans\
1889259234.xml.]];
</LogText>
<TranslationInfo Type="JAVA"
Catalog="com.ibm.opmt.utils.messages.MigrationManager_
msgs"
MsgKey="AMXUT2504I"><Param>
<![CDATA[C:\PROGRA~1\Tivoli\db\YFELDMA1.db\AMX\shared\analyze\scans\
1889259234.xml]];
</Parm></TranslationInfo>
<Principal></Principal>
</Message>
```

Reading RAS1 logs

This section provides an example of the Universal Agent RAS1 trace logs. By default, the Universal Agent RAS1 trace log lists the following details about the health of an ODBC data provider application:

- Whether the ODBC tables come online during startup.
- Whether the ODBC table data is collected.
- Errors with the ODBC-related status messages, including informational messages about when each ODBC connection completes.
- Errors that occur during ODBC data provider data retrieval, including errors in the ODBC driver code.
- Independent Software Vendor (ISV) API errors. (The Universal Agent makes API calls to the ISV ODBC driver to implement the connections and SQL select statements.)

The following RAS1 log excerpt lists ODBC status messages using default tracing:

```
KUMP_ProcessStartUpConfig") Loading metafile
<f:\candle\cma\metafiles\TIVOLI_DATA_WAREHOUSE.mdl>
from startup config file
f:\candle\CMA\WORK\KUMPCNFG_INST1
"DCHserver::dp_register") Application TIVOLI_DATA_WAREHOUSE
successfully registered"KUMP_ProcessStartUpConfig")
1 application metafile(s) processed from startup
config
file f:\candle\CMA\WORK\KUMPCNFG_INST1
"KUMP_StartDataProvider") Starting ODBC Data Provider...
"KUMP_WaitODBCsourceReadyForMonitor")
Reusing connection handle for ODBC source
TIVOLI_DATA_WAREHOUSE table <syscharsets>
"KUMP_ODBCserver") Successfully connected to ODBC source
TIVOLI_DATA_WAREHOUSE table <syscharsets>
"KUMP_WaitODBCsourceReadyForMonitor") Reusing connection handle
for ODBC source TIVOLI_DATA_WAREHOUSE table <syscomments>
```

The `Reusing connection handle` messages indicates the ODBC provider is reusing resource to conserve memory. The ODBC data provider allocates a connection for each metafile with multiple attribute groups that connect to the same data source using the same user ID and password combination. Each SQL Select statement that is run for the various attribute groups shares the same connection handle.

The following is an excerpt from later in the same log:

```
userDataList::calculateChecksum") Initial creation of catalog/attribute tables for
applName <Tivoli_Data_Warehouse>
"KUMP_ODBCserver") ODBC source <Tivoli_Data_Warehouse> table <syscharsets> is now
online to the data provider
"KUMP_ODBCserver") ODBC source <Tivoli_Data_Warehouse> table <syscacheobjects>
is now online to the data provider
"KUMP_ODBCserver") ODBC source <Tivoli_Data_Warehouse> table <syscomments>
is now online to the data provider"
```

Setting traces

When you encounter an error with IBM Tivoli Monitoring that requires contacting IBM Software Support, you might be asked to submit a copy of the error log. The error log is part of the trace diagnostic tool in Tivoli Enterprise Portal. It is set to log errors, and you can set other parameters for collecting specific details. Always backup the files before altering them.

Setting the trace option for the Tivoli Enterprise Portal client trace

A log file is created automatically the first time you start Tivoli Enterprise Portal, and is named `install_dir\cnp\logs\kcjras1.log`. This log file contains all of the RAS1 tracing for the Tivoli Enterprise Portal client. Whenever you start a new work session, the log file is purged and rewritten for the current work session. If you want to preserve the log file from the last work session, you must rename it or copy it to another directory before starting Tivoli Enterprise Portal again. The `kcj.log` file contains errors generated by the Sun Java™ libraries used in the Tivoli Enterprise Portal client.

To set the trace options:

1. Always backup the files before altering them.
2. From the Tivoli Enterprise Portal menu, select **File** > **Trace Options**.
3. Select a trace class from the list or as instructed by IBM Software Support (such as UNIT:Workspace ALL):

   ALL provides data for all classes. Use the setting temporarily, because it generates large amounts of data.

   ERROR logs internal error conditions. This setting provides the minimum level of tracing, with little resource overhead, and ensures that program failures will be caught and detailed.

   NONE turns off the error log so no data is collected.
4. Click **OK** to close the window and turn on logging.

Setting the trace option for the Tivoli Enterprise Portal Server trace

You must set the trace options for the Tivoli Enterprise Portal Server through Manage Tivoli Enterprise Monitoring Services. Before you set the trace options for the Tivoli Enterprise Portal Server, determine the trace string. The trace string specifies the trace setting. Set trace options for the Tivoli Enterprise Portal Server when you start the Tivoli Enterprise Portal Server. The log file continues to grow until you either turn off the trace or recycle the Tivoli Enterprise Portal Server. Always backup the files before altering them.

On Windows systems:

1. Always backup the files before altering them.
2. On the computer where the Tivoli Enterprise Portal Server is installed, click **Start** > **Programs** > **IBM Tivoli Monitoring** > **Manage Tivoli Enterprise Monitoring Services.**
3. Right-click the Tivoli Enterprise Portal Server service.
4. Select **Advanced** > **Edit Trace Parms** to display the **Trace Parameters** window.
5. Select the RAS1 filters. The default setting is ERROR
6. Accept the defaults for the rest of the fields.
7. Click **OK** to set the new trace options.
8. Click **Yes** to recycle the service.

On UNIX systems:

1. Always backup the files before altering them.
2. Set the following variable in the `$CANDLEHOME/config/cq.ini`:

   `KBB_RAS1=ERROR (UNIT:`*`filter trace_level`*`)`

where *filter* is the component you want to trace and *trace_level* is the level of tracing you want.

3. Recycle the Tivoli Enterprise Portal Server by "restarting" or "stop" and then "start".

Setting the trace option for the Tivoli Enterprise Monitoring Server trace

On Windows systems:

1. Always backup the files before altering them.
2. On the computer where the Tivoli Enterprise Monitoring Server is installed, select **Start** > **Programs** > **Tivoli Monitoring Services** > **Manage Tivoli Enterprise Monitoring Services**.
3. Right-click the Tivoli Enterprise Monitoring Server service.
4. Select **Advanced** > **Edit Trace Parms** to display the **Trace Parameters** window.
5. Select the RAS1 filters. RAS1 is the unit trace for the Tivoli Enterprise Monitoring Server. The default setting is ERROR.

   Note: There must be a space between each UNIT trace setting. For example, ERROR (UNIT:kdy all) (UNIT:kfaprpst all).
6. Accept the defaults for the rest of the fields.
7. Click **OK** to set the new trace options.
8. Click **Yes** to recycle the service.

On UNIX systems:

1. Always backup the files before altering them.
2. Set the following variable in the `ms.ini` file in the `%CANDLEHOME/config` directory:

   `KBB_RAS1=ERROR (UNIT:`*`filter trace_level`*`)`

   where *filter* is the component you want to trace and *trace_level* is the level of tracing you want. The following example traces everything in the Deploy component:

   `KBB_RAS1=ERROR (UNIT:KDY ALL)`

   Note: There must be a space between each UNIT trace setting. For example:

   `KBB_RAS1=ERROR (UNIT:KDY ALL) (UNIT:KFAPRPST ALL)`
3. Set the following variable in `$CANDLEHOME/bin/tacmd` to trace the command line interface of the Tivoli Enterprise Monitoring Server:

   `KBB_RAS1=ERROR (UNIT:`*`filter trace_level`*`)`
4. Regenerate the *`host_name`*`_ms_`*`TEMS_NAME`*`.config` file by running the ./itmcmd config -S [-h install_dir] [-a arch] -t tems_name command.
5. Recycle the Tivoli Enterprise Monitoring Server by "restarting" or "stop" and then "start". The command syntax for starting and stopping the monitoring server is ./itmcmd server [-h install_dir] [-l] [-n] start|stop tems_name.

For information on how to set trace levels dynamically, see “Dynamically modify trace settings for an IBM Tivoli Monitoring component” on page 53.

Setting the trace option for the Agent Deploy tool

On Windows systems:

1. On the computer where the Tivoli Enterprise Monitoring Server is installed, select **Start** > **Programs** > **Tivoli Monitoring Services** > **Manage Tivoli Enterprise Monitoring Services**.
2. Right-click the Tivoli Enterprise Monitoring Server service.
3. Select **Advanced** > **Edit Trace Parms** to display the **Trace Parameters** window.
4. Type **(UNIT:kdy all)** in the **Enter RAS1 Filters** field.
5. Accept the defaults for the rest of the fields.
6. Click **OK** to set the new trace options.
7. Click **Yes** to recycle the service.

On Linux systems, set the following variable in `$CANDLEHOME/config/lz.ini`:

```
KBB_RAS1=ERROR(UNIT:kdy ALL)(UNIT:kdd ALL)
```

On UNIX systems other than Linux:

1. Set the following variable in `$CANDLEHOME/config/ux.ini`:

   ```
   KBB_RAS1=ERROR (UNIT:kdy ALL) (UNIT:kdd ALL)
   ```
2. Recycle the OS Agent on that endpoint.

Setting any monitoring agent's trace option for SNMP alerts

When troubleshooting SNMP Alerts for any agent, set the following trace:

```
ERROR (UNIT:KRA ALL)
```

If the agent is configured to use SNMPv3 Encryption when emitting the SNMP alerts, set (COMP:SNMP ALL) so that the trace setting would be the following:

```
ERROR (UNIT:KRA ALL) (COMP:SNMP ALL)
```

Use (COMP:SNMP ALL) when you are focusing on SNMP traps. If you are focusing on an agent communication error or crash, then use:

```
KBB_RAS1=(UNIT:KRA ALL) (UNIT:s_ ALL)
```

The (UNIT:s_ ALL) trace level includes tracing of system calls during SNMP processing.

Setting the trace option for the IBM Tivoli Universal Agent

Use the IBM Tivoli Universal Agent trace facility to diagnose problems with the Universal Agent. The Universal Agent uses RAS1 tracing. By default, Universal Agent trace data is written to a file in the logs subdirectory. The default RAS1 trace level is ERROR for all Universal Agent components and modules. On Windows, Tivoli Monitoring Services overwrites the `kumras1.log` each time the Universal Agent starts and there is no method for archiving previous RAS1 log files. Therefore, you must obtain the RAS1 log that matches the problem occurrence before contacting IBM Software Support. You can set tracing options for individual Universal Agent components and modules in the `KUMENV` file on Windows or the `um.ini` file on UNIX-based systems.

RAS1 supports pattern matching. For example, (UNIT:kums options) traces all SNMP data provider modules because they all begin with `kums`. Detailed RAS1 tracing can degrade Universal Agent performance due to high CPU usage and I/O overhead. Therefore, set the Universal Agent RAS1 tracing to `KBB_RAS1=ERROR` after problem diagnosis. If a module produces excessive error messages and fills the RAS1 log, set (`UNIT:modulename None`) to suppress the module until you resolve the errors. If you discover an old Windows RAS1 log file, the KBB_RAS1 environment

was erased or commented out in the KUMENV file, add KBB_RAS1=ERROR to the install_dir\logs\hostname_um_timestamp.log to reactivate Universal Agent RAS1 tracing.

Set the IBM Tivoli Universal Agent trace from Manage Tivoli Enterprise Monitoring Services:

1. Right-click the Universal Agent.
2. Select **Advanced** > **Edit Trace Parms**.
3. Select the RAS1 filters. The default setting is ERROR
4. Accept the defaults for the rest of the fields.
5. Click **OK** to set the new trace options.
6. Click **Yes** to recycle the service.

Setting the trace option for the Warehouse Proxy agent

1. On Windows systems, on the computer where the Tivoli Enterprise Monitoring Server is installed, select **Start** > **Programs** > **Tivoli Monitoring Services** > **Manage Tivoli Enterprise Monitoring Services**.
2. Right-click **Warehouse Proxy**.
3. Select **Advanced** > **Edit Trace Parms**.
4. Select the RAS1 filters. The default setting is ERROR.
5. Accept the defaults for the rest of the fields.
6. Click **OK** to set the new trace options.
7. Click **Yes** to recycle the service.

Using the Warehouse Proxy Agent user interface: You can edit the handler configuration file $CANDLEHOME%\Config\ITMConfigRAS.properties for UNIX systems and the %CANDLEHOME%\Config\ITMConfigRAS.properties file for Windows systems, and set the handler99 as the configuration handler and set the debug tracing to the maximum DEBUG_MAX as shown below:

```
Handler99.name=config
Handler99.scope=*
Handler99.scopeName=Config
Handler99.logFile=../logs/config.log
Handler99.traceFile=../logs/config.trc
Handler99.level=DEBUG_MAX
Handler99.onConsoleToo=true
Handler99.maxFiles=10
Handler99.maxFileSize=8192
```

Then you need to create a file called kKHDconfig.sysprops.cfg under the directory $CANDLEHOME\TMAITM6 for UNIX systems, and %CANDLEHOME%\TMAITM6 for Windows systems, containing a link to the handler configuration file as shown below:

```
DInstallRASConfig="ITMConfigRAS.properties"
```

When the Warehouse Proxy Agent configuration panel is executed, tracing appears in the $CANDLEHOME/logs/config.trc file for UNIX systems, and %CANDLEHOME%/logs/config.trc for Windows systems, as described by the handler configuration file.

To trace the 2way translator, set the trace level to (UNIT: KDY ALL) (UNIT: KHD_XA ALL) in the Warehouse Proxy Agent environment file for KBB_RAS1.

Setting the trace option for the Summarization and Pruning Agent

Use the IBM Tivoli Universal Agent trace facility to diagnose problems with the Summarization and Pruning Agent. See "Setting the trace option for the IBM Tivoli Universal Agent" on page 45. The Summarization and Pruning Agent uses C-based RAS1 tracing, Java-based RAS1 tracing and Java-based internal tracing. By default, Summarization and Pruning Agent trace data is written to a file in the logs subdirectory. The default RAS1 trace level is ERROR for all Summarization and Pruning Agent components and modules.

The following trace options are available for the IBM Tivoli Summarization and Pruning Agent:

KBB_RAS1=ERROR
Trace general errors. KBB_RAS1=ERROR Affects the content of the C-based RAS1 tracing (`hostname_sy_HEXtimestamp-nn.log`).

KBB_RAS1=ERROR (UNIT:ksz ALL)
Trace agent startup. Affects the content of the C-based RAS1 tracing (`hostname_sy_HEXtimestamp-nn.log`).

KBB_RAS1=ERROR (COMP:com.tivoli.twh.ksy ALL)
Minimum level trace for summarization. Affects the content of the Java-based RAS1 tracing (`hostname_sy_ras1java_timestamp-nn.log`).

KBB_RAS1=ERROR (UNIT:ksy1 ALL)
Medium level trace for summarization. Affects the content of the Java-based internal tracing (`hostname_sy_java_timestamp-n.log`)

KBB_RAS1=ERROR (UNIT:ksy2 ALL)
Connection level trace for summarization. Affects the content of the Java-based internal tracing (`hostname_sy_java_timestamp-n.log`)

KBB_RAS1=ERROR (UNIT:ksy3 ALL)
Statement level trace for summarization. Affects the content of the Java-based internal tracing (`hostname_sy_java_timestamp-n.log`).

KBB_RAS1=ERROR (UNIT:ksy4 ALL)
ResultSet level trace for summarization. Affects the content of the Java-based internal tracing (`hostname_sy_java_timestamp-n.log`).

KBB_RAS1=ERROR (UNIT:ksy5 ALL)
Column value level trace for summarization. Affects the content of the Java-based internal tracing (`hostname_sy_java_timestamp-n.log`).

KBB_RAS1=ERROR (UNIT:ksysql ALL)
Traces every SQL statement being executed. Affects the content of the Java-based internal tracing (`hostname_sy_java_timestamp-n.log`).

KBB_RAS1=ERROR (UNIT:ksysql1 ALL)
Same as (UNIT:ksysql ALL) but also includes all the parameter values used in the parameterized statements.

Notes:

1. The following settings: (UNIT:ksy3 ALL) or (UNIT:ksy4 ALL) or (UNIT:ksy5 ALL) produce a high volume of trace output.
2. By default, the Java-based internal trace (`hostname_sy_java_timestamp-n.log`) wraps at 5 files, and each file contains 300000 lines. To change the defaults, use the following settings in the `KSYENV` (Windows) or `sy.ini` (UNIX) files:

```
KSZ_JAVA_ARGS=-Dibm.tdw.maxNumberDetailTraceFiles=<A>
-Dibm.tdw.maxLinesForDetailTraceFile=<B>
```

where:

<A> Specifies the maximum number of Java-based internal trace files that can exist at any one time for a single launch

<B> Specifies the maximum number of lines per Java-based internal trace file.

Using the Summarization and Pruning Agent user interface: You can edit the handler configuration file `$CANDLEHOME%\Config\ITMConfigRAS.properties` for UNIX systems and the `%CANDLEHOME%\Config\ITMConfigRAS.properties` file for Windows systems, and set the handler99 as the configuration handler and set the debug tracing to the maximum DEBUG_MAX as shown below:

```
Handler99.name=config
Handler99.scope=*
Handler99.scopeName=Config
Handler99.logFile=../logs/config.log
Handler99.traceFile=../logs/config.trc
Handler99.level=DEBUG_MAX
Handler99.onConsoleToo=true
Handler99.maxFiles=10
Handler99.maxFileSize=8192
```

Then you need to create a file called `kKSYconfig.sysprops.cfg` under the directory $CANDLEHOME\TMAITM6 for UNIX systems, and %CANDLEHOME%\TMAITM6 for Windows systems, containing a link to the handler configuration file as shown below:

```
DInstallRASConfig="ITMConfigRAS.properties"
```

When the Summarization and Pruning Agent configuration panel is executed, tracing appears in the `$CANDLEHOME/logs/config.trc` file for UNIX systems, and `%CANDLEHOME%/logs/config.trc` for Windows systems, as described by the handler configuration file.

To trace the 2way translator, set the trace level to (UNIT: KDY ALL) (UNIT: KHD_XA ALL) in the Summarization and Pruning Agent environment file for KBB_RAS1.

Setting the trace option for the tacmd commands

For Windows systems, manually edit the KUIENV file in the `CANDLEHOME` directory with the standard KBB_RAS1 statement to include the following:

```
KBB_RAS1=ERROR(UNIT:ksh all) (UNIT:kui all)
```

.

On UNIX systems, manually edit the `$CANDLEHOME/bin/tacmd` shell script to add a line like the following example:

```
KBB_RAS1=ERROR(UNIT:ksh all) (UNIT:kui all)
```

In order to debug KT1 as well, edit the line to be like the following example:

```
KBB_RAS1=ERROR(UNIT:ksh all) (UNIT:kui all) (UNIT:kt1 all)
```

Setting the trace option for the IBM Tivoli Monitoring upgrade toolkit

Table 25. Setting the trace option for the IBM Tivoli Monitoring upgrade toolkit

Trace option	Instructions
Endpoint tracing	Run the following command to setting log_threshold=3 or higher on an endpoint and enable endpoint tracing: `wep ep set_config log_threshold=3` Traces are written to `lcfd.log` on the endpoint in `$LCF_DATDIR`.
Tracing in a test environment.	A Boolean value of TRUE or FALSE default. The default is FALSE. Run the following command from a Tivoli Management Environment command prompt to enable tracing:`idlcall oid _set_debug TRUE` where: *oid* Specifies the object ID of the Upgrade Manager object. Run the **wlookup** Framework command to locate the Upgrade Manager object ID in the Tivoli Management Environment: `wlookup -a | grep Upgrade` **Note:** Setting the trace value to TRUE sets all Upgrade Toolkit tools to TRUE, affecting all users running Upgrade Toolkit tools. A trace file named `trace_tool_timestamp.log` is created in the *$DBDIR*`/AMX/trace/` directory in XML format, with tool being 'witmscantmr', 'witmassess', and 'witmupgrade', and *timestamp* a time stamp that includes data and time of execution. Each record in this log contains a time stamp and message. Additionally, these tools inherit Framework FFTC mechanisms such as **wtrace** and **odstat** for transaction and method stack traces. See the Tivoli management Framework documentation for more information about the commands.
OS Agent tracing	OS Agent tracing is enabled at a minimum level by default. Agent tracing levels can be adjusted with agent specific settings. Logs are stored in *install_dir*`\installITM\` on Windows agents or *install_dir*`/logs/` on UNIX-based systems agents. These logs follow the RAS1 log format.

Setting the trace option for the IBM Tivoli Monitoring event forwarding

If your monitoring environment is configured for the IBM Tivoli Monitoring event forwarding, you can forward situation events to the IBM Tivoli Enterprise Console, and view events on the event server through the Tivoli Enterprise Portal. If you want to forward situation events to and view updates from IBM Tivoli Enterprise Console in the Tivoli Enterprise Portal, you can set the trace for the event forwarder on the Tivoli Enterprise Monitoring Server.

Use the IBM Tivoli Monitoring event forwarding trace facility to diagnose problems with the IBM Tivoli Monitoring event forwarding. The IBM Tivoli Monitoring event forwarding trace facility uses RAS1 tracing. The IBM Tivoli Monitoring event forwarding is set during installation. The acceptable values include:

- STATE
- DETAIL
- ALL

The default trace value is STATE. If you change the trace level, you must restart the Tivoli Enterprise Monitoring Server for the change to take effect.

Use the following instructions to set the trace levels:

On Windows:

1. From Manage Tivoli Enterprise Monitoring Services, right-click the **Tivoli Enterprise Monitoring Server**.
2. Click **Advanced** > **Edit trace parms**.
3. Under **Enter RAS1 Filter** add **UNIT:kfaot** *trc_class*

   where:

   trc_class
   Specifies STATE, DETAIL or ALL which produces increasingly more trace information.
4. The default log file location is `C:\IBM\ITM\CMS\logs\KMSRAS1.LOG`, change if necessary.
5. Click **OK** to set the trace.
6. Recycle the Tivoli Enterprise Monitoring Server for the trace to take effect.

On UNIX-based systems:

1. Edit *install_dir*`/config/`*hostname*`_ms_`*Tivoli_Enterprise_Monitoring_Server_ID*`.config`

   where:

   install_dir
   Specifies the install directory of Tivoli Enterprise Monitoring Server.

   hostname
   Specifies the host name value supplied during install.
2. Add `(UNIT:kfaot` *trc_class*`)` to the line `KBB_RAS1='ERROR'`

   where:

   trc_class
   Specifies one of the following levels of trace detail:
   - STATE - minimum detail.
   - DETAIL - medium detail.
   - ALL - maximum detail.

   For example, `'KBB_RAS1='ERROR (UNIT:kfaot STATE)'`
3. Save the file.
4. Recycle Tivoli Enterprise Monitoring Server for the trace to take effect.
5. The Tivoli Enterprise Monitoring Server log can be found in *install_dir*`/logs/`*hostname*`_ms_nnnnnnn.log` where is a time stamp. There might be multiple files with different time stamps in the logs directory.

Setting the trace option for the IBM Tivoli Enterprise Console Situation Update Forwarder

If your monitoring environment is configured for the IBM Tivoli Enterprise Console, you can forward situation events to the Tivoli Enterprise Console event server. You can also view events on the event server through the Tivoli Enterprise Portal. If you want to forward situation events to and view updates from IBM Tivoli Enterprise Console in the Tivoli Enterprise Portal, you can set the trace for the Situation Update Forwarder on the IBM Tivoli Enterprise Console event server. The default trace setting is low. You can edit the trace setting using the **sitconfig** command.

```
$BINDIR/TME/TEC/OM_TEC/bin/sitconfig.sh update
fileName=configuration_file_name logLevel=trace_level
```

where:

configuration_file_name
: The file name of the actively loaded configuration file as indicated by the `situpdate.properties` file.

trace_level
: Specifies the level of trace as **low**, **med**, or **verbose**.

Use the IBM Tivoli Enterprise Console Situation Update Forwarder trace facility to diagnose problems with the IBM Tivoli Enterprise Console Situation Update Forwarder. The trace for the IBM Tivoli Enterprise Console Situation Update Forwarder is set during installation. The acceptable values include:

- low
- med
- verbose

The default trace value is low. If you change the trace level after the Situation Update Forwarder is started, you must restart the Situation Update Forwarder for the change to take effect. There are two trace files:

synch_trace.log
: is always created.

synch_msg.log
: is created if an error occurs while running the Situation Update Forwarder.

Run the following command to set the trace levels:

```
$BINDIR/TME/TEC/OM_TEC/bin/sitconfig.sh update
fileName=configuration_file_name logLevel=trace_level
```

where:

configuration_file_name
: The file name of the actively loaded configuration file as indicated by the `situpdate.properties` file.

trace_level
: Specifies the level of trace as **low**, **med**, or **verbose**.

Setting up RAS1 tracing on z/OS systems

This syntax is used to specify a RAS1 trace in the `KppENV` file (where pp is the product code: HL for the OMEGAMON z/OS Management Console or DS for the Tivoli Enterprise Monitoring Server). After you add this command to the `KppENV` file, you must stop and restart the address space for the command to take effect. After that, it remains in effect for the life of the address space. To end the trace, you must edit the `KppENV` file again to reset the trace level, and stop and restart the address space.

The basic syntax of the RAS1 trace command is:

```
KBB_RAS1= global_class (COMP: component_type)
(ENTRY: entry_point) (UNIT: unit_name, class)
```

where:

global_class
: Indicates the level of tracing that you want. This is a global setting that

applies to all RAS1 filters in the process. If you set this global class by itself, it is global in scope and the trace cannot filter on any of the other keywords. Separate combined classes with a space. The following values are possible. Valid abbreviations are in parentheses.

ERROR (ER):
returns severe error messages only (this is the default for most applications).

STATE (ST):
records the condition or current setting of flags and variables in the process. If state tracing is enabled, you can see the current state of particular variables or flags as the process is running.

FLOW (FL):
causes a message to be generated at an entry or exit point of a function.

DETAIL (DE):
produces a detailed level of tracing.

INPUT (IN):
records data created by a particular API, function, or process.

ALL: causes all available messages to be recorded. This setting combines all the other forms of tracing.

COMP
Indicates that the trace includes a component type. The COMP keyword is used to trace groups of routines related by function (or component). Use this keyword only at the explicit request of an IBM Software Support representative.

component_type
Identifies a component type. An IBM Software Support representative can tell you what value to specify.

ENTRY
Narrows a filtering routine to specify a specific ENTRY POINT. Since multiple entry points for a single routine are rare, use this keyword only at the explicit request of an IBM Software Support representative.

entry_point
Represents the name of the entry point. An IBM Software Support representative can tell you what value to specify.

UNIT Indicates that the trace is to look for a match between the compilation unit dispatched and the fully or partially qualified compilation unit specified on the RAS1 statement. A match results in a trace entry.

unit_name
Represents the name of the compilation unit. In most instances, this name defines the component that is being traced. The value is likely to be the three-character component identifier for the monitoring agent (KHL for OMEGAMON z/OS Management Console).

class One of the same values specified for *global_class* but, because of its position inside the parentheses, narrowed in scope to apply only to the *unit_name* specified.

Note: The default setting for monitoring agents on z/OS is KBB_RAS1=ERROR, meaning that only error tracing is enabled. You can specify any combination

of UNIT, COMP, and ENTRY keywords. No keyword is required. However, the RAS1 value you set with the global class applies to all components.

For more information on setting RAS1 tracing on z/OS system, see your individual monitoring agent's user's guide.

Dynamically modify trace settings for an IBM Tivoli Monitoring component

You can access the Tivoli Enterprise Monitoring Server, Tivoli Enterprise Portal Server, almost all of the agents, and other IBM Tivoli Monitoring components from this utility.

This method of modifying trace settings on an IBM Tivoli Monitoring component is the most efficient method since it allows you to do so without restarting the component. Settings take effect immediately. Modifications made this way are not persistent.

Note: When the component is restarted the trace settings are read again from the `.env` file. Dynamically modifying these settings does not change the settings in the `.env` files. In order to modify these trace settings permanently, modify them in the `.env` files.

How to turn tracing on:

In order to use this utility you need to know a local log-on credential for the system.

This method uses the IBM Tivoli Monitoring Service Console. The Service Console is accessed using a web browser. Access the utility by using the following link:

`http://`*`hostname`*`:1920`

where *hostname* is the hostname or IP address of the system where the IBM Tivoli Monitoring component is running. The utility then appears with information about the components that are currently running on this system.

For example, the component Tivoli Enterprise Portal Server shows as cnp, the Monitoring Agent for Windows OS shows as nt, and the Tivoli Enterprise Monitoring Server shows as ms.

Select the link below the component for which you want to modify the trace settings. In the previous view if you want to modify tracing for the Tivoli Enterprise Monitoring Server, you select the "IBM Tivoli Monitoring Service Console" link under the Service Point: system. balayne_ms.

When you select one of the links, you will be prompted for a user ID and password to access the system. This is any valid user that has access to the system.

Typing **?** displays a list of the supported commands.

The command for modifying the trace settings is **ras1**.

If you type `ras1` in the field at the bottom of the screen, you will then see the help for this command.

The **set** option (ras1 set) turns on the tracing, but does not affect existing tracing.

An example would be **ras1 set (UNIT:xxx ALL) (UNIT:yyy Detail)**. This command will enable full tracing for the *xxx* class of the component and low-level detailed tracing on the *yyy* class of the component.

The **ras1 list** command lists what tracing is set as default. It is best to do an initial list in order to track what changes you have made to the tracing settings.

The following list describes the options of tracing available:

ALL - Provides all trace levels. Shown as ALL when using the **ras1 list** command.

Flow - Provides control flow data describing function entry and exit. Shown as Fl when using the **ras1 list** command.

ERROR - Logs internal error conditions. Shown as ER when using the **ras1 list** command. The output also shows as EVERYE+EVERYU+ER.

Other settings which provide component specific information are:

Detail - Shown as Det when using the **ras1 list** command.

INPUT - Shown as IN when using the **ras1 list** command.

Metrics - Shown as ME when using the **ras1 list** command.

OUTPUT - Shown as OUT when using the **ras1 list** command.

State - Shown as ST when using the **ras1 list** command.

Setting trace to ALL includes every trace point defined for the component. This might result in a large amount of trace. If you have been given a more specific setting, use it. ALL can sometimes be necessary when isolating a problem. It is the equivalent of setting "Error Detail Flow State Input Output Metrics".

The **ras1 units** command is used to determine the list of UNITs and COMPs available in an IBM Tivoli Monitoring component. The first column is the list of available UNIT values, the last column lists the corresponding COMP values.

Turning on (COMP:KDH ALL) will turn ALL level tracing on for all of the files where KDH is listed in the right hand column (highlighted below).

The following is a subset of the results for the Monitoring for Windows agent:

```
kbbcre1.c, 400, May 29 2007, 12:54:43, 1.1, *
kbbcrn1.c, 400, May 29 2007, 12:54:42, 1.1, *
kdhb1de.c, 400, May 29 2007, 12:59:34, 1.1, KDH
kdh0med.c, 400, May 29 2007, 12:59:24, 1.1, KDH
kdhsrej.c, 400, May 29 2007, 13:00:06, 1.5, KDH
kdhb1fh.c, 400, May 29 2007, 12:59:33, 1.1, KDH
kdhb1oe.c, 400, May 29 2007, 12:59:38, 1.2, KDH
kdhs1ns.c, 400, May 29 2007, 13:00:08, 1.3, KDH
kbbacdl.c, 400, May 29 2007, 12:54:27, 1.2, ACF1
kbbaclc.c, 400, May 29 2007, 12:54:27, 1.4, ACF1
kbbac1i.c, 400, May 29 2007, 12:54:28, 1.11, ACF1
kdhsfcn.c, 400, May 29 2007, 13:00:11, 1.1, KDH
kdhserq.c, 400, May 29 2007, 12:59:53, 1.1, KDH
kdhb1pr.c, 400, May 29 2007, 12:59:39, 1.1, KDH
kdhsgnh.c, 400, May 29 2007, 12:59:49, 1.1, KDH
kdh0uts.c, 400, May 29 2007, 12:59:23, 1.1, KDH
```

```
kdhsrsp.c, 400, May 29 2007, 13:00:13, 1.2, KDH
kdhs1rp.c, 400, May 29 2007, 13:00:12, 1.1, KDH
kdhscsv.c, 400, May 29 2007, 12:59:58, 1.9, KDH
kdebbac.c, 400, May 29 2007, 12:56:50, 1.10, KDE
```

The UNIT value matches any unit that starts with the specified value. For example, (UNIT:kra FLOW) prints the FLOW traces for all files which match kra*.

How to turn tracing back off:

The option for turning the tracing off is **ANY**. For example you would use the following command to turn off tracing for the kbbcrcd class of the Windows OS agent:

```
ras1 set (UNIT:kbbcrcd ANY)
```

Using the IBM Tivoli Monitoring Service Console

The IBM Tivoli Monitoring Service Console enables you to read logs and turn on traces for remote product diagnostics and configuration. The IBM Tivoli Monitoring Service Console is uniquely identified by its service point name. All IBM Tivoli Monitoring Service Consoles for a host are linked and presented on the IBM Tivoli Monitoring Service Index for that host. Point a browser to the HTTP port 1920 on a specific host (for example, http://goby:1920) to launch the IBM Tivoli Monitoring Service Index. You can also launch the Service console can also be launched with the https protocol by connecting via the https protocol and port 3661. You can perform operations on a specific IBM Tivoli Monitoring process by selecting the IBM Tivoli Monitoring Service Console associated with a service point name.

The IBM Tivoli Monitoring Service Index has links to service consoles for the components installed on the computers. Now, when you go to the Service Index, you will also see links to the Agent Service Interface. Use the Agent Service Interface to get reports for an installed agent, whether it is a Tivoli Enterprise Monitoring Agent or Tivoli System Monitoring Agent. After logging into the local operating system, you can choose reports of agent information, private situations, private history, and attribute descriptions and current values. You can also make a service interface request using provided XML elements.

Starting the IBM Tivoli Monitoring Service Console

Use the following procedure to start the IBM Tivoli Monitoring Service Console.

1. Start Internet Explorer V5 or higher.
2. In the **Address** field, type the URL for the Tivoli Enterprise Portal browser client installed on your Web server.

   The URL for the Tivoli Monitoring Services Web server is

   ```
   http://hostname:1920
   ```

   hostname
   Specifies the computer where the Tivoli Enterprise Portal Server was installed. If the IBM Tivoli Monitoring Service Console is not displayed, a system administrator might have blocked access to it. See "Blocking access to the IBM Tivoli Monitoring Service Console" on page 56.
3. Click the IBM Tivoli Monitoring Service Console link associated with the desired process (service point name).
4. When the log in window opens, click **OK**.

In secure environments, you need a valid user ID and password to proceed. Upon successful login, the IBM Tivoli Monitoring Service Console opens with three areas:

- Header
- Command Results
- Command Field

You can now issue IBM Tivoli Monitoring Service Console commands in the command input area. For a list available commands, type a question mark (?) and click **Submit**.

The IBM Tivoli Monitoring Service Console performs user authentication using the native OS security facility. If you use the IBM Tivoli Monitoring Service Console on z/OS systems, your user ID and password are checked by the z/OS security facility (RACF/SAF). If you use the IBM Tivoli Monitoring Service Console on Windows systems, then you must pass the Windows workstation user ID and password prompt. This is the rule except for instances of a NULL or blank password. The IBM Tivoli Monitoring Service Console never accepts a NULL or BLANK password.

A password is always required to access the service console. Blank passwords, even if correct, cannot access to the service console. Even if a user ID is allowed to log in to the operating system without a password, access to the service console is denied. Create a password for the user ID that is being used to log in to the service console.

Blocking access to the IBM Tivoli Monitoring Service Console

The Tivoli Monitoring Services integral Web server is installed automatically with the Tivoli Enterprise Portal Server and enables users to access the IBM Tivoli Monitoring Technology Service Console. You can prevent users from accessing the IBM Tivoli Monitoring Technology Service Console that is available through the integral Web server (http://*computer_name*:1920). To block access to the IBM Tivoli Monitoring Technology Service Console, disable the integral Web server. However, if you disable the integral Web server, you must install a third party Web server on the Tivoli Enterprise Portal Server computer to access the images and style sheets for the graphic view and edit the application parameters at every desktop client.

1. From the Windows desktop select **Start** > **Run** >
2. Type `regedit`.
3. Open the Tivoli Enterprise Portal Server Environment folder:

   `HKEY_LOCAL_computer\SOFTWARE\Tivoli Monitoring Services\KFW\Tivoli Enterprise Portal Server\KFWSRV\`**`Environment`**
4. Locate the `KDC_FAMILIES` in the right frame and add a space and type the following at the end of the line: `http_server:n`

   Example:

   ```
   IP PORT:1918 SNA use:n IP.PIPE use:n http_server:n
   ```
5. Install a third party Web server on each computer where you installed the Tivoli Enterprise Portal desktop client:
   a. From the Windows desktop select **Start** > **Programs** > **Tivoli Monitoring Services** > **Manage Tivoli Enterprise Monitoring Services**.
   b. Right-click **Tivoli Enterprise Portal desktop** and select **Reconfigure** from the menu.
   c. In the list of parameters that opens, double-click **cnp.http.url.DataBus** to open the **Edit Tivoli Enterprise Portal Parm** window.

d. Type the URL to the external Web server and to the `cnps.ior` file in the `candle\cnb` directory.

   For example, if the Web server name is **myWeb.hostname.com** and its document root was configured to be `\candle\cnb`, the value to type is:

   http://myWeb.hostname.com/cnps.ior

e. Check **In Use** and click **OK**.

Displaying tasks in the command prompt

The Tivoli Enterprise Portal Server has an option to display the tasks at the command prompt. This is used primarily with IBM Software Support for gathering diagnostic information.

1. From your Windows desktop, select **Start** > **Programs** > **Tivoli Monitoring Services** > **Manage Tivoli Enterprise Monitoring Services**.
2. Right-click **Tivoli Enterprise Monitoring Server**, then select **Change Startup** from the menu.
3. Check **Allow Service to Interact with Desktop**.

KfwSQLClient utility

This utility provides an optional cleanup step if any of the portal server-generated workspace queries must be deleted. A sample scenario where this might be necessary is if you initially create a metafile application called DISKMONITOR for the Tivoli Universal Agent that has five attribute groups in it. Assume that you subsequently remove two of the attribute groups, which results in a new application version suffix. You then decide to run **um_cleanup** to reset the DISKMONITOR version back to 00. After completing the cleanup process, the Navigator tree still shows workspaces for each of the five original attribute groups, even though the metafile contains only three attribute groups.

This mismatch is caused by the fact that the portal server saves workspace queries in the KFWQUERY table of the portal server database, which is not updated by the `um_cleanup` script. Therefore, the original 00 version of the queries, which knows about the five original attribute groups, is still being used when you view the DISKMONITOR00 application.

If you determine that you need to delete one or more portal server-generated queries for your Tivoli Universal Agent applications, there is a Tivoli Universal Agent-provided script called `um_cnpsCleanup.bat`, which is installed on Windows computers, that demonstrates how to perform the delete. The script is very short and uses only the following command:

```
kfwsqlclient /d TEPS2 /e "delete from kfwquery where id like 'zkum.%%';"
```

For a Windows-based portal server, this command is entered from the \IBM\ITM\CNPS directory. The command assumes that the portal server database is using the default data source name of TEPS2, but you can change it if you have configured a different data source name.

On Linux and UNIX systems, this command should be invoked using the **itmcmd execute** command, for example:

```
itmcmd execute cq "KfwSQLClient -f myqueries.sql"
```

Note that this command deletes all portal server-generated Universal Agent queries, which always begin with zkum. To confirm that portal server-generated

Tivoli Universal Agent queries have been deleted, or to see which queries are currently defined, run the following select command against the KFWQUERY table:

```
kfwsqlclient /d TEPS2 /e "select id, name from kfwquery where id like 'zkum.%%';"
```

Clearing the JAR cache

If you encounter problems, IBM Software Support might instruct you to uninstall and to clear the JAR cache.

1. If Tivoli Enterprise Portal is running, exit by closing the browser window.
2. Start the Java Plug-in.

   Additional Information: You can find the Java Plug-in in **Start** > **Settings** > **Control Panel**. To start it, double-click the Java Plug-in icon. Your Windows desktop might have a shortcut to the Java Plug-in (1.4.2).
3. In the Java Plug-in Control Panel window, select the **Cache** tab and click **Clear JAR Cache**.
4. When a message indicates the JAR cache is cleared, click **OK**.

   If you want to start Tivoli Enterprise Portal browser mode again, restart Internet Explorer and type the URL for Tivoli Enterprise Portal. The Java Extension Installation progress bar shows as each Java archive file is downloaded. Upon completion, the logon window opens and prompt you to enter a user ID.

Using the UAGENT application

The UAGENT application is a diagnostic tool to help solve problems you might experience with the IBM Tivoli Universal Agent. Every Universal Agent data provider automatically activates an application called UAGENT, which includes the DPLOG and ACTION workspaces.

DPLOG

The DPLOG is a pure event table in that it maintains only the most recent 100 rows, unless overridden by the KUMA_MAX_EVENT_ENTRIES environment variable. The DPLOG contains informational and error messages about the status of a data provider that indicate:

- If a metafile was validated successfully.
- If a metafile failed validation (which means the application will not come online).
- If a data source was available at startup
- Which console ports and socket listening ports were used or unavailable.
- When monitoring started and stopped for a data source.
- When monitoring switched from one file to another.
- When an API or socket client program connected and disconnected.

The DPLOG also records other actions including metafile refreshes. The two most common Universal Agent problem symptoms are:

- One or more managed systems do not come online.
- The managed systems are online but the workspaces are empty.

Use the UAGENT application workspaces as one of the first tools to diagnose a Universal Agent problem. You might find the solutions for both problems in the

appropriate DPLOG. The ODBC data provider also includes a DPLOG message indicating when monitoring started for every attribute group listed in every ODBC metafile.

ACTION workspace

Whenever a Take Action command is issued or a Reflex Action fires, an entry is added to the ACTION workspace. The Action table is keyed and ActionID is the Key attribute. The Action table rows have a time-to-live value of 30 minutes. Unlike the DPLOG which is data provider-specific, the ACTION table is shared by all data providers. If you run multiple data providers, the ACTION workspace under every UAGENT application contains the same rows.

The Action_Result can indicate what happened to a particular Take Action command. For example, if Universal Agent reflex actions fire faster than one per second, the ACTION workspace temporarily stops recording the results. Recording resumes after several minutes if the action rate slows down.

pdcollect tool

Use the pdcollect tool to collect the most commonly used information from a system. Technicians in IBM Software Support use this information to investigate a problem. The pdcollect tool is used to gather log files, configuration information, version information, and other information to help solve a problem. You can also use the tool to manage the size of trace data repositories.

The pdcollect tool is run from the **tacmd pdcollect** command. To use this tool, you must install the User Interface Extension. When you install or upgrade the Tivoli Enterprise Portal Server, the Tivoli Enterprise Services User Interface Extensions software is automatically installed in the same directory. The portal server extensions are required for some products that use the Tivoli Enterprise Portal (for example, IBM Tivoli Composite Application Manager for Service Oriented Architecture). For more information about this command, see the *IBM Tivoli Monitoring Command Reference*.

ras1log tool

This is a tool that converts the time stamps contained in trace logs into readable values. This tool can be found in the *itm_install*/bin directory on both Windows and UNIX systems. The following lists how the help appears:

```
usage: ras1log [-l|u] logfile ...
        -l for local time
        -u for UTC time
```

logfile can be either a file name or '-' for stdin (default).

You can either pass the tool a file name or you can filter a file through it to obtain a readable log. You do not need to specify any arguments.

The following examples work on Windows systems:

```
ras1log <balayne_ms_46c071a6-01.log
ras1log <balayne_ms_46c071a6-01.log | grep GetEnv
ras1log <balayne_ms_46c071a6-01.log > tems_log
```

The first example sends the result to the screen, the second sends the result to grep to find all of the lines with the text 'GetEnv' in them, which are then printed on the screen, and the third sends the result to a file named `tems_log`.

By default this tool converts the timestamps to UTC time. When using the -l option, it writes local time instead.

Log and Trace Analyzer Tool

With the Log and Trace Analyzer, you can gather system and performance data from local and remote systems. The data can be used for troubleshooting should a less than optimal system event occur.

You can use the Log and Trace Analyzer to create resource sets. Resource sets are sets of definitions that contain the path locations of the logs that you need to examine and the levels of information that they contain. You can keep customized definitions to reuse. The definitions provide the same set of instructions about where to find a log, and what kind of information to gather from the log, saving time during subsequent log imports.

The Log and Trace Analyzer also makes it possible for you to download and store symptom database catalogs to your local system. These catalogs provide detailed diagnostic solutions to a variety of scenarios, which can give direction to your troubleshooting tasks.

To download the Log and Trace Analyzer, complete the following steps:

1. If you do not have the IBM Support Assistant (ISA) installed, go to the ISA Web site at www.ibm.com/software/support/isa/ to download the software. Instructions for downloading and installing the ISA are on the ISA Web site.
2. Using the ISA built-in Updater component, download and install the ISA plug-in for IBM Tivoli Monitoring from the IBM Web site at www.ibm.com/software/support/isa/. Instructions for downloading and installing the ISA plug-in are on the ISA Web site.
3. Using the ISA built-in Updater component, download and install the plug-in for Log and Trace Analyzer from the IBM Web site at www.ibm.com/software/support/isa/. The Log and Trace Analyzer plug-in is included in the list of plug-ins for Common Component Tools.
4. After installation of the Log and Trace Analyzer is complete, start the ISA.
5. From the list of tasks, click **Tools**.
6. From the list of products, click **IBM Tivoli Monitoring**.
7. From the list of tools for IBM Tivoli Monitoring, click **Log and Trace Analyzer**. The Log and Trace Analyzer should start working.

To import the IBM Tivoli Monitoring log files to the Log and Trace Analyzer, complete the following steps:

1. Copy the relevant log files from the Monitoring servers to the system where you installed the IBM Support Assistant workbench. Put the log files for each server in a unique directory. For example, `c:\ITM\logs\serverXXX\...`
2. Import the IBM Tivoli Monitoring log files. The Log and Trace Analyzer organizes related log files into log sets. Log sets can be used to import and analyze a set of related log files. This facility is used to organize and import your IBM Tivoli Monitoring log files. Log set definitions provide information to the Log and Trace Analyzer specifying where log and trace data reside and what kind of data to gather from local and remote systems. The Log and Trace

Analyzer allows you to import pre-defined log sets that contain the necessary path information required for retrieving log files on demand.

3. Use one of the following procedures:
   - Create the initial IBM Tivoli Monitoring log set:
     a. Click **File -> Import Log File**.
     b. Create a new log set.
     c. Type the name for the log set. For example, you could type the following text: `IBM Tivoli Monitoring Log files for server xxxx`
     d. Click **Add**.
     e. In the Name Filter window, to limit the list of log files to the IBM Tivoli Monitoring log files, type `Discovery`.
     f. Select the type of log file you are adding to the log set.
     g. Type the name of the log file on your local system. Ensure the type of log file matches the log file you specified.
     h. Enter the correct version of the IBM Tivoli Monitoring product that corresponds to the log file. Refer to the Log and Trace Analyzer online help for additional options.
     i. To add the log file to the log set, click **OK**.

     For every log file you want to include in the log set, repeat step e. Best practice: The first time you create the log set, you save time later by including every log file you want to include in the log set.
   - Reuse an existing IBM Tivoli Monitoring log set:
     a. Select **File -> Import Log File**.
     b. Select an existing Log Set Definition from the drop-down list of defined log sets.
     c. If necessary, change the contents of the log set definition. You can add, edit, or remove from the list of log files in the log set.
     d. To indicate the file should be imported to the log set, select the checkbox next to the log file.
     e. To import the log files, click **Finish**.

     You can create and reuse as many log sets as you need. For example, when importing log files from multiple servers, you need more than one log set.

Using the Log and Trace Analyzer, you can correlate multiple IBM Tivoli Monitoring log files into a single view. The IBM Tivoli Monitoring log files can be combined in a single view, ordered by time stamp, to correlate the operation of the IBM Tivoli Monitoring components. There are two ways to correlate log files:

- Simple – To correlate all imported log file, complete the following steps:
  1. In the Log and Trace Analyzer navigation tree view, right-click **Logs**.
  2. Click **View All Logs**.
- Advanced – To correlate a set of log files by creating a custom correlation, complete the following steps:
  1. In the Log and Trace Analyzer navigation tree view, right-click **Correlations**.
  2. Click **New -> Log Correlation**.
  3. In the window that is displayed, type the name for the correlation.
  4. Add the log files that you want to include for the correlation.
  5. Click **Finish**.
  6. Refresh the navigation tree view.

7. In the navigation tree view, right-click the correlation name you typed and click **Open With -> Log View**.

After you create a view of the logs, you can organize the log data to isolate problems. The following list identifies some of the ways that you can organize the data:

- Sort log records: For example, you can sort by time, component, and server name.
- Highlight log records: For example, you can highlight all error events in red or show all events from a specific component in blue. Highlighting is similar to filtering, but instead of eliminating data from a view, you can highlight the relevant information within the full list of events.
- Filtering log records: You can narrow the scope of a problem and the data shown based on filter criteria. Examples of filter criteria include time stamps, severity, component, and server.
- Finding log records: You can search for specific information in a log file. For example, you can search to see events related to interaction with a specific server or user.

For more information about how to organize the data, in the Log and Trace Analyzer online help, search for the “Analyzing log files” topic. “Filtering, Sorting, Finding, and Highlighting” is a subheading in this topic.

In addition, there are some other topics in the online help that you might find useful:

- When trying to correlate log files from multiple servers, the time clocks on those servers can be out-of-sync. This synchronization problem could be something simple, like different time zones, or more subtle, such as a clock being a few milliseconds off from another server's clock. The Log and Trace Analyzer imbeds a function to synchronize the time between multiple log files by allowing you to adjust the time stamps in a log file. For more information, refer to the topic titled "Synchronizing time of log records for distributed applications" in the Log and Trace Analyzer online help.
- You can use symptom catalogs to quickly recognize known problems. The Log and Trace Analyzer provides a log analysis capability that allows it to recognize known problems that are defined in a knowledge database, called the 'symptom catalog'. IBM provides a symptom catalog for known problems with several products, including IBM Tivoli Monitoring. It also provides a way for you to capture and define your own symptom information. For more information, refer to the topic titled “Synchronizing time of log records for distributed applications" in the Log and Trace Analyzer online help.

Backspace Check utility

On UNIX systems, if you have incorrectly configured the backspace key, you will see the following:

- When you press the backspace key, characters such as "^?" and "^H" are displayed on the screen.
- The backspace key seems to be working correctly when entering text, but you later find characters such as "^?" and "^H" in configuration files and your software malfunctions.

Configure your terminal and "stty erase" to use the same key code for backspace. Consider using "^?" as the key code. Verify your configuration with the IBM Tivoli Monitoring distributed utility, Install: BackspaceCheckUtility.

Build TEPS Database utility

You can use this utility to build a blank database. Prior to the IBM Tivoli Monitoring v6.1 release, this utility would also populate the database with tables. Now, it is necessary to also run the BuildPresentation utility to build the tables in the database.

To build and populate a database, complete the following steps:

1. From the **Manage Tivoli Enterprise Monitoring Services** window, right-click **TEPS**.
2. Select **Advanced -> Utilities -> Build TEPS Database**.
3. Run the `BuildPresentation.bat` file found in *install_dir*\CNPS.

IBM Tivoli Monitoring Operations Logging

You can use this logging facility to determine the cause of IBM Tivoli Monitoring problems. IBM Tivoli Monitoring Operations Logging replaces MSG2 logging. With MSG2 logging, physical space problems can occur due to MSG2 logs that grow without bound until a process is stopped. IBM Tivoli Monitoring Operations Logging enables you to configure log file management to avoid these problems.

Note: This functionality is not supported for agents. It is only supported for the log messages produced through the MSG2 facility as used by the Tivoli Enterprise Monitoring Server and Tivoli Enterprise Portal Server.

Windows and UNIX systems

The new optional logs replace the Tivoli Enterprise Monitoring Server log files *install_dir*\cms\kdsmain.msg on Windows systems and *install_dir*/logs/*hostname*_ms_*timestamp*.log on UNIX-based systems. For the Tivoli Enterprise Portal Server, they replace the *install_dir*\logs\ kfwservices.msg file on Windows systems and the *install_dir*/logs/kfwservices.msg file on UNIX-based systems.

To use the new logging facility for the Tivoli Enterprise Monitoring Server, modify the *install_dir*\cms\KBBENV file on Windows systems or the *install_dir*/config/*hostname*_ms_*TEMS ID*.config file and *install_dir*/config/kbbenv.ini file on UNIX-based systems. Add the following line to the file:

```
MSG_MODE=kms
```

To disable the new logging facility and return to original logging, either remove this line in the file or change it to:

```
MSG_MODE=MSG2
```

To use the new logging facility for the Tivoli Enterprise Portal Server, modify the *install_dir*\cnps\kfwenv file on Windows systems, or the *install_dir*/config/cq.ini file on UNIX-based systems. Add the following line to the file:

```
MSG_MODE=kcq
```

To disable the new logging facility and return to original logging, either remove this line from the file or change it to:

```
MSG_MODE=MSG2
```

When you have enabled the new logging facility, the Tivoli Enterprise Monitoring Server writes a new log file: *install_dir*/itmLogs/itmc_*hostname*_kms.log. The Tivoli Enterprise Portal Server also writes to a new file: *install_dir*/itmLogs/itmc_*hostname*_kcq.log.

The properties file (*install_dir*/itmLogs/itmc_kms.properties for the Tivoli Enterprise Monitoring Server and the *install_dir*/itmLogs/itmc_kcq.properties file for the Tivoli Enterprise Portal Server) determines the maximum size and the number of rolling log files. The default is 100000 bytes per file and 3 files.

You can modify these values by changing these parameters in the properties file: fh.maxFileSize=1000000 fh.maxFiles=3. When the log file exceeds the maxFileSize, the file moves to a new name, for example, itmc_*hostname*_kms1.log, and new messages are then written to the original file name, for example, itmc_*hostname*_kms.log. The process continues for the number of maxFiles.

z/OS systems

To use the new logging facility for the Tivoli Enterprise Monitoring Server, modify the RKANPARU member. Add the following line to the file:

```
MSG_MODE=kms
```

To disable the new logging facility and return to original logging, either remove this line in the file or change it to:

```
MSG_MODE=MSG2
```

The number of log datasets is determined by how many datasets are defined in the Tivoli Enterprise Monitoring Server JCL procedure. The amount of data that can be written to each dataset depends on the amount of space allocated at the time each dataset is created.

To use IBM Tivoli Monitoring Operations Logging on z/OS systems, complete the following procedure:

1. Create the log datasets. You must create at least one to use the new logging facility, but it is best to create three. The only limit to the number of datasets that you create is the limit imposed by the system (typically, about 70). Each dataset must reside on a disk device. The DCB attributes are DSORG=PS, RECFM=VB, LRECL=256. The BLKSIZE specification must be at least 260, but you can allow it to default to the system-determined value for best performance. The amount of space allocated to the datasets is not critical. Allocating five 3390 cylinders allows space for about 50000 log records. (The number varies, depending on the lengths of the messages.)

   Note: Do not specify secondary allocations. Any secondary allocations are ignored.
2. Edit your Tivoli Enterprise Monitoring Server JCL procedure (typically named CANSDSST, but can be named otherwise). For each of your datasets, add a DD statement with the DDNAME "RKMSLGnn" that points to the dataset with DISP=SHR. The first dataset should use "RKMSLG00" as the DDNAME, with "nn" incrementing by one for each additional dataset.

   Note: DO NOT SKIP VALUES of "nn." If any values are skipped, subsequent OpsLog DD statements are ignored.

You can examine the contents of the log datasets using ISPF Browse or any equivalent tool. Note that the dataset that is currently receiving log data might appear to be empty. You can force a switch to the next dataset (which in turn will flush any buffered log data to the current dataset), using the MODIFY OPSLOGSW console command. The syntax of this command is:

```
F procname,OPSLOGSW,KMS
```

"KMS" indicates that the log associated with Tivoli Enterprise Monitoring Server is to be processed.

ITMSuper

The ITMSUPER tool performs audits of the Tivoli Monitoring environment (topology, connectivity, application support consistency checks, situations distribution, warehouse analysis, etc). A Windows environment is required. This tool can be run in stand-alone mode by pointing to the Tivoli Enterprise monitoring server on any platform. You may run the ITMSUPER tool from a Windows client without having other IBM Tivoli Monitoring software installed. The ITMSUPER Tools are included in the IBM Support Assistant (ISA), a free local software serviceability workbench that helps you resolve questions and problems with IBM software products. To install the ISA software, go to http://www.ibm.com/software/support/isa.

Chapter 5. Installation and configuration troubleshooting

This chapter contains the following sections, which provide information about problems that might occur during installation, upgrading from previous versions, and uninstallation of the product and product components:

Frequently asked questions

General installation frequently asked questions

The following table lists general installation frequently asked questions.

Table 26. General frequently asked questions

Question	Answer
Are fix packs required if a user migrates Candle monitoring agent to IBM Tivoli Monitoring.	Fix packs for CNP196 are delivered as each monitoring agent is migrated to IBM Tivoli Monitoring. **Note:** The IBM Tivoli Monitoring download image or CD provides application fixpacks for the monitoring agents that are installed from that CD (for example, the agents for operating systems such as Windows, Linux, UNIX, and i5/OS®). The migration software for other agents is located on the download image or CDs for that specific monitoring agent, such as the agents for database applications.If you do not migrate the monitoring agent to IBM Tivoli Monitoring, the agent continues to work. However, you must migrate to have all the functionality that IBM Tivoli Monitoring offers.
Do presentation files and customized OMEGAMON DE screens for Candle monitoring agents need to be migrated to a new zLinux system.	The migration from version 350 to IBM Tivoli Monitoring handles export of the presentation files and the customized OMEGAMON DE screens.

Windows installation frequently asked questions

Table 27. Windows installation frequently asked questions

Question	Answer
How can I determine if Windows Security logging is on?	If the sysadmin account that you use to log on to Tivoli Enterprise Portal is not a Windows Administrator, you do not see the security log. Windows security logging is not turned on by default. Normally, data is not collected in the security log unless the Windows administrator turns it on. The Record Count = 0 in the Windows monitored logs report confirm that security logging is not turned on.

Table 27. Windows installation frequently asked questions (continued)

Question	Answer
How can I diagnose problems with product browse settings?	1. Click on **Start > Programs > Tivoli Monitoring > Manage Tivoli Enterprise Monitoring Services** to display the Manage Tivoli Enterprise Monitoring Services window. 2. Right-click the Windows agent and select **Browse Settings**. A text window displays. 3. Click **Save As** and save the information in the text file. If requested, you can forward this file to IBM Software Support for analysis.

UNIX-based systems installation frequently asked questions

Table 28. Frequently asked questions for UNIX-based systems installation

Problem	Solution
The product was installed as root. Without re-installing the product, how can I change from root to another ID?	If you installed and started the agent as root, the files do not have correct permissions, so the result is unpredictable. For this reason, do not use root ID either to install or start the UNIX-based systems agents. Create a user ID with all the authority and permissions to install, run or use any other ID other than root. As root, run the command UnSetRoot , which is located under `install_dir/bin/` directory. This script resets all the files under the `install_dir` directory, owned by root. `UnSetRoot [ -h CANDLEHOME ] userID` After executing the above script, run the **SetPerm** command, which is located under `install_dir/bin/` directory. This command sets root permission for certain UNIX-based systems agent files.
How can I set the trace option to capture any abends (core files)?	Add the following in the agent .ini file. For an example if it is KUX agent, add the following line in `install_dir/config/ux.ini` file `KBB_SIG1=trace –dumpoff`
In an environment of 50 servers with at least one agent per server, a new agent (vt) was installed outside the firewall. The new agent must be configured on Tivoli Enterprise Monitoring Server for IP.PIPE communication. Is it necessary to change all the other UNIX-based systems agents for IP:PIPE?	Is it not necessary to change all the other UNIX-based systems agents for IP:PIPE. You have to configure only the agent, which connects to the Tivoli Enterprise Monitoring Server through a firewall. However, you must configure the Tivoli Enterprise Monitoring Server for IP.PIPE communication. While configuring the agent, which communicate through the firewall, you get the following options: • Does the agent connect through a firewall? [YES or NO] (Default is: NO) • IP.PIPE Port Number (Default is: 1918) • Enter name of KDC_PARTITION (Default is: null)
Does SNMP need to be turned on to monitor UNIX-based systems host? The monitoring server is running WINNT4.0 and monitoring agent is running on HPUX?	If you are communicating only through Tivoli Enterprise Monitoring Server you do not need SNMP. However, if you are sending traps to the emitter through the Tivoli CA uni-center or HP Open-view, SNMP is required.

Table 28. Frequently asked questions for UNIX-based systems installation (continued)

Problem	Solution
Pressing the backspace key, characters such as "^?" and "^H" appear on the screen. The backspace key appears to be working correctly when entering text, but you later find characters such as "^?" and "^H" in configuration files and your software malfunctions.	If you receive one of these symptoms when using the backspace on UNIX computers, you have incorrectly configured the backspace key. Configure your terminal and "stty erase" to use the same key code for backspace. Consider using "^?" as the key code. Verify your configuration with the IBM Tivoli Monitoring distributed utility, Install: BackspaceCheckUtility.
When running the install.sh script on a Linux system, I get a Memory fault (core dump) at different, random stages of the install, regardless of what selections I make.	When I run the command "getconf GNU_LIBPTHREAD_VERSION" on my system, the response I receive is "linuxthreads-0.10" or something similar. This is caused by the /etc/profile entry of "LD_ASSUME_KERNEL=2.4". If I unset this variable or change the value of /etc/profile to "2.6", the getconf command returns "NPTL 2.3.4" or something like it. This enables me to run the `install.sh` script without causing the memory fault. **OR** Changing the JAVA_COMPILER variable to NONE before upgrading allows me to continue without hitting the core dump.

Table 28. Frequently asked questions for UNIX-based systems installation (continued)

Problem	Solution

Why does a Linux or UNIX-based installation to a non-default path create directories in the default `/opt/IBM/ITM` path?	This is an expected condition. The following example depicts an AIX installation to a non-default location. The following links are created when the **SetPerm** command is run:
	`/opt/IBM/ITM/tmaitm6`
	`/opt/IBM/ITM/tmaitm6/links`
	`/opt/IBM/ITM/tmaitm6/links/aix52`
	`/opt/IBM/ITM/tmaitm6/links/aix52x6`
	`/opt/IBM/ITM/tmaitm6/links/aix53`
	
	The **SetPerm** command creates those links by design. Some of the binaries have hard-coded execution paths. This coding is required by the operating system in order to invoke a program object in authorized mode [root owned with UID].
	
	The *IBM Tivoli Monitoring Installation and Setup Guide* documents installation on a single target location. However, by using local testing and configuration control, you can install to multiple target locations and run Tivoli Monitoring from all of them. For example, you can run multiple remote monitoring servers on a single server. Of course, the multiple monitoring servers require a non-default configuration, such as using different base port numbers.
	• If all installations on the system are at the same maintenance level, running the **SetPerm** command and updating the hard-coded `/opt/IBM/ITM/tmaitm6/links` directory structure does not cause any problems.
	• If all installations on the system are not at the same maintenance level, running the **SetPerm** command and updating the hard-coded `/opt/IBM/ITM/tmaitm6/links` directory structure can cause problems. This scenario needs more testing than the scenario where all installations are at the same level.
	
	The following procedure might resolve problems you encounter in the latter scenario:
	• Maintain an installation on this system with the most current maintenance.
	• Run the **SetPerm** command from this installation each time after other installations apply maintenance or add agents.
	• Run the **SetPerm** command from this installation each time after other installations run the **SetPerm** command or the **secureMain** commands.
	
	Note: For some cases, the OS Agents for example, only one agent can be installed because of the agent's interaction with the operating system.

General installation problems and resolutions

This section describes general installation problems and resolutions.

Agent Builder application support is not displayed in listappinstallrecs output if it is manually installed without recycling the monitoring server

If you run the scripts to manually install the Agent Builder application support on the Tivoli Enterprise Monitoring Server (TEMS) and specify both the user name and password, the expected result is that the application support files are loaded without causing the TEMS to restart. After that, if you run the **tacmd listapplinstallrecs** command to verify the application support installation, the support is not listed in the command output. As a result, a lower version

SDA-enabled Agent Builder agent might override the higher version application support when it is connected through that TEMS. To avoid this situation, you must recycle the monitoring server.

Debugging mismatched application support files

After upgrading your monitoring server and portal server to Tivoli Monitoring V6.2.3, you might be warned that the portal server identified mismatched support files. Mismatched files are identified when you forget to upgrade the agent support files during your upgrade or you forget to upgrade the TEPS support, but upgrade the agent support files. To remedy this situation, complete the support upgrade specified by the warning. See Table 1 on page 13 for more information.

Startup Center fails to reset the sysadmin password on the hub Tivoli Enterprise Monitoring Server configuration panel

If the Startup Center fails to reset the sysadmin password on the hub Tivoli Enterprise Monitoring Server configuration panel, reset the password manually.

Startup Center fails to create the Tivoli Warehouse database and user

If the Startup Center fails to create the Tivoli Data Warehouse database and user, follow the Warehouse Proxy Agent configuration instructions to create the Tivoli Data Warehouse database and user. See "Configuring a Warehouse Proxy agent" in the *IBM Tivoli Monitoring Installation and Setup Guide*.

On UNIX systems, a new user is not created or a password is not reset in the Startup Center when you use a non-root user to install Warehouse Proxy Agent and Tivoli Enterprise Portal Server

On UNIX systems, a new user cannot be created and a password cannot be reset in the Startup Center when you use a non-root user to install Warehouse Proxy Agent and Tivoli Enterprise Portal Server. To remedy this situation, create the user or reset the password manually.

On Windows systems, an Tivoli Monitoring Warehouse DSN is not created in the Startup Center

If the Tivoli Monitoring Warehouse DSN is not created by the Startup Center, create the DSN manually by using the Warehouse Proxy Agent configuration instructions. See "Configuring a Warehouse Proxy agent on Windows" in the *IBM Tivoli Monitoring Installation and Setup Guide*. For more information, check the *WAREHOUSE_ODBC.log* and *WAREHOUSE_ODBC.trc* files under the target system *<your temp directory>\DSNUtil (for example, C:\Temp\DSNUtil).*

Startup Center fails to test DSN with database connectivity

If you have an existing 32-bit Warehouse database in the 64-bit DB2 instance, the Startup Center fails to test the DSN for database connectivity after creating the Tivoli Monitoring Warehouse DSN. The WAREHOUSE database is not upgraded from 32-bit to 64-bit automatically. For more information, check *WAREHOUSE_ODBC.log* and *WAREHOUSE_ODBC.trc* under target system *<your temp directory>\DSNUtil (for example, C:\Temp\DSNUtil).*

Startup Center shows some system types as "Unknown Operating System"

When you run the discovery process for available machines, the Startup Center might not identify the type of operating system for some systems. These operating systems are listed as *Unknown Operating System*.

This issue does not prevent the use of the affected systems. If the operating system type of a specific system cannot be discovered, you are given the opportunity to categorize the system manually in a later step. When you assign systems to the components, if a system categorized as "Unknown Operating System" is assigned to a component, you can select the correct operating system from the list in the window that is displayed. After you have specified the correct OS, the system is moved to the correct category in the list.

The Startup Center uses Nmap OS detection to categorize systems. Nmap OS detection works by running through a set of probes against target IP implementations and comparing responses with those in the fingerprint database. These responses are affected by the specific IP stack creating the response, which allows for OS detection. However, in some cases it can also be affected by the IP stack on the system where nmap is running, as well as intermediate firewalls and routers, for example. In other words, for the same target OS type, several different fingerprints in the database might be required in order to address these variations. For additional information, see "Dealing with Misidentified and Unidentified Hosts" at the Nmap site: `http://nmap.org/book/osdetect-unidentified.html`

Whenever you find an OS that is not discovered correctly, you should ideally force nmap to generate a signature, so that you can submit it to Insecure for integration into the Nmap fingerprint database.

The nmap command is located on the Startup Center media in:

- *(W32) StartupCenter/SDE/nmap-5.21-win32*
- *(Linux) StartupCenter/SDE/nmap-5.21-linux-x86*

Run the **nmap -O -sSU -T4 -d <***target***>** command, where <*target*> is the misidentified system in question. The fingerprint is a series of lines where each start with "OS". Submit the information at `http://insecure.org/cgi-bin/submit.cgi?corr-os`.

Receive fatal errors when running a self-describing monitoring agent installation

Certain fatal error conditions on a self-describing monitoring agent installation on a monitoring server require you to manually use commands to reset and remove the metadata error record in the TAPPLPROPS table. When the installation errors have been manually corrected on the monitoring server, you can retry a new self-describing monitoring agent installation on the affected hub or remote monitoring server installations.

To clear up these errors, you must be able to identify the source of the error condition. These error condition messages are provided by the monitoring server workload manager (WLM) in RAS1 or MSG2 error messages, or audit facility messages. You must examine these messages to identify the specific problems in the monitoring server installation process and in the TAPPLPROPS table.

You can view and delete the monitoring server metadata or seed installation records stored into the TAPPLPROPS table by using the **tacmd listappinstallrecs** command and the **tacmd deleteappinstallrecs** command. You must first log in to the monitoring server by using the **tacmd login** command. For more information about these commands, see the *IBM Tivoli Monitoring Command Reference*.

To use these two commands, complete the following steps:

1. Use the **tacmd listappinstallrecs** command to see the status of a self-describing monitoring agent installation.
2. Analyze RAS1 or MSG2 error messages and perform the proper actions to clean up the failed installation.
3. Use the **tacmd deleteappinstallrecs** command to delete the records in error.
4. Retry the installation.

Unable to update the Tivoli Data Warehouse agent by using the command line interface

When using remote deployment to upgrade the Tivoli Data Warehouse agents (Warehouse Proxy Agent and Summarization and Pruning Agent), you must use a specific workaround to ensure that the upgrade is successful.

On UNIX and Linux systems, you must add the following variable to the `hd.ini` file for the Warehouse Proxy Agent or the `sy.ini` file for the Summarization and Pruning Agent, and then restart the agent:

```
CTIRA_SYSTEM_NAME=$RUNNINGHOSTNAME$
```

On Windows systems, you must add the following line to the `KHDCMA.INI` file for the Warehouse Proxy Agent or the `KSYCMA.INI` file for the Summarization and Pruning Agent, and then reconfigure and restart the agent:

```
CTIRA_SYSTEM_NAME=%computername% .TYPE=REG_EXPAND_SZ
```

Receive duplicate insert errors (SQL1 return code 80) after an agent switches away from the remote monitoring server and then switches back

When a Global Access List hub monitoring server is installed with a previous version of a remote monitoring server, you will see duplicate insert errors (SQL1 return code 80) after an agent switches away from the remote monitoring server and then switches back. These messages do not indicate an environment execution error.

Upgrade SQL file not found when installing application support on the standby hub

When adding application support to the hubs in a hot standby setup, after the first hub has been seeded, you might receive an error message similar to the following about the `productcode_upg.sql` file not being found while seeding the second hub:

```
Seeding support for Monitoring Agent for Microsoft SharePoint Server [8 of 10]
KCIIN1602E ERROR - file not found:
/boadata/IBM/ITM/tables/cicatrsq/SQLLIB/kqp_upg.sql
Option "-f install|upgrade" can be used with the "itmcmd support" command to force
using the pristine installation or upgrade support file for the product's
application support. Seeding failed.
Seeding support for Monitoring Agent for Microsoft Virtual Server [9 of 10]
KCIIN1602E ERROR - file not found:
/boadata/IBM/ITM/tables/cicatrsq/SQLLIB/kqr_upg.sql
```

```
Option "-f install|upgrade" can be used with the "itmcmd support" command
to force usingthe pristine installation or upgrade support file for the
product's application support. Seeding failed.
```

This error is not necessarily a fatal error. It simply means the application did not provide an upgrade seeding file. There are generally two types of seeding files: install and upgrade. The installer determines which one to apply by checking to see if there are already situations belonging to the application on the target hub. If no situation is found, then the installation seeding file is chosen, otherwise the upgrade seeding file is used if provided. In a hot standby setup, as soon as one hub is seeded, the other hub can copy the situations immediately. So when seeding is applied to the second hub, the installer detects existing situations and looks for the upgrade seeding file instead. Even though some applications do not provide upgrade seeding files, because the hubs automatically synchronize seeded data, it is generally not a serious issue. Seeding can still be forced on the second hub by using the -f option.

Many files in the First Failure Data Capture log directory

On Windows systems, there are eWAS logs in the following location of the IBM Tivoli Monitoring home directory:

CANDLE_HOME\CNPSJ\profiles\ITMProfile\logs\ffdc\

And, on UNIX systems, they are found in the following directory:

CANDLE_HOME/*arch*/iw/profiles/ITMProfile/logs/ffdc/

These log files might contain the following exceptions:

```
org.omg.CORBA.BAD_OPERATION
CORBA.TRANSIENT
ClassNotFound on MQJMS
```

These exceptions can be ignored and have no impact on either eWAS or IBM Tivoli Monitoring functionality.

Receive a message after installing a self-describing capable agent

After you install a self-describing capable agent, you see an error message if the self-describing application support packages are not present on the installation media:

```
Unable to install agent name support packages required for self-describing mode.
Check installation log file for more details.
```

You can review the details of installation failure by reading the installation main log file. The following entries should be stored in the log file:

```
Unable to install agent name support packages required for self-describing mode.
Following error(s) detected:
        list of error(s)
Self-describing mode for agent name is not enabled.
When the problem is fixed, reinstall agent name to enable self-describing mode.
```

A reported failure means that the agent is installed without using the self-describing mode. You can relaunch the agent installation to attempt support installation again. Before relaunching the installation, ensure that the failure will not reappear by checking the previous installation log for the reasons for the failure. Correct the obtained failure reasons (for example, fix the contents of the manifest, unlock required files or folders). The alternative is to leave the agent

installed in non-self-describing mode. When relaunching, select only the agents that must be installed with installation self-describing mode support.

If the reinstallation fails, an appropriate message is displayed, and the failure reasons are logged in the main installation log file. If no errors are encountered, the installation ends successfully.

Monitoring agents fail to start after agent support or multi-instance agents are installed

Monitoring agents on an IBM Tivoli Monitoring V6.2.1 (or later) managed system that have an unsupported system GSKit version installed might fail to start after an IBM Tivoli Monitoring V6.2 Multi-Instance Agent or IBM Tivoli Monitoring V6.2 Agent Support is locally installed.

The installer used by both IBM Tivoli Monitoring V6.2 Multi-Instance Agents (including fix packs) and IBM Tivoli Monitoring V6.2 Application Support causes monitoring agents on an IBM Tivoli Monitoring V6.2.1 managed system (or later) to revert back to using the system GSKit instead of the IBM Tivoli Monitoring embedded GSKit. This issue occurs on local installations only. Remote installation (remote deploy) does not have this issue.

If a system GSKit is installed on the managed system at a level supported by IBM Tivoli Monitoring, the monitoring agents continue to operate normally.

Monitoring agents might fail to start, however, if all of the following conditions are met:

- The managed system does not have a system GSKit installed or the system GSKit is at a version not supported by IBM Tivoli Monitoring V6.2.1 or later.
- The agent is configured to use secure communications (IP.SPIPE) rather than normal communication (IP.PIPE).

If agents on a managed system fail to start after an IBM Tivoli Monitoring V6.2 Multi-Instance Agent or IBM Tivoli Monitoring V6.2 Agent Support is installed, any one of the following corrective actions can be taken:

- Run **kinconfig.exe -G** on the managed system.
- OR
- Reconfigure any of the IBM Tivoli Monitoring V6.2.1 (or later) monitoring agents on the managed system by running **kinconfig.exe -rK***productcode*.
- OR
- Install another IBM Tivoli Monitoring V6.2.1 monitoring agent (or later).

Incorrect behavior after an uninstallation and re-installation

You might experience incorrect behavior if you uninstall then reinstall the product without rebooting. For example, you might experience the following problems:

- Inability to create trace logs.
- Agents do not start.
- Agents data is corrupt.

Reboot the system to resolve the problems.

Where Remote Deployment of agents is not supported

Remote Deployment is not supported for OMEGAMON agents. It is also not supported in environments with a z/OS Tivoli Enterprise Monitoring Server.

Remote Deployment is not supported when the Tivoli Enterprise Monitoring Server, Tivoli Enterprise Portal Server or the Tivoli Enterprise Portal are on the same system as the agent. It is also not supported if the target endpoint has a Tivoli Enterprise Monitoring Server, Tivoli Enterprise Portal Server or the Tivoli Enterprise Portal installed on it.

This restriction includes the following commands:

- tacmd viewagent
- tacmd startagent
- tacmd stopagent
- tacmd restartagent
- tacmd configuresystem
- tacmd updateagent
- tacmd removesystem
- tacmd createnode
- tacmd cleardeploystatus
- tacmd restartfaileddeployment
- tacmd checkprereq
- tacmd addsystem

Application Support Installer hangs

The Application Support Installer (ASI) gets to the screen indicating "Please select which applications you would like to add support for." but hangs there. After selecting the "Next" button, the installation hangs there and does not update the screen. The `%TEMP%\ITM_AppSupport_Install.log` (Windows) or `\tmp\ITM_AppSupport_Install.log` (UNIX and Linux) also fails to be updated after this point, even after waiting for hours.

Change to the directory where `setup.jar` exists, and then use **java -jar setup.jar**to run the installer.

An agent bundle is not visible from the Tivoli Enterprise Portal

The bundle has been added to the depot and is viewable from there, but it is missing from the list of agents available for deployment from the Tivoli Enterprise Portal for a given node. You cannot deploy an agent from the Tivoli Enterprise Portal if the xml version in the depot is later than the installed version because the newer xml might contain configuration properties that the back-level agent does not support. This issue was noticed for the DB2 agent.

Agent Management Services fails after deployment on Linux Itanium and xLinux with kernel 2.4 systems

Agent Management Services fails after deployment on Linux Itanium and xLinux with kernel 2.4 systems when the -o KDYRXA.AUTOCLEAN=YES option is used. The Proxy Agent Services agent will not start when the deployment process completes if the option that removes the temporary directory used by remote deployment was used. To start the OS agent when this problem occurs, do one of the following actions:

- On the agent system, manually restart the OS agent.
- On the agent system, run `$CANDLEHOME/bin/itmcmd execute -c lz startWatchdog.sh`.
- Go to the Agent Management Services workspace for the agent in question and run the 'AMS Start Agent' Take Action against the Proxy Agent Services agent with a resetRestartCount of 0.

Watchdog utility requires Windows Script Host 5.6

The OS Agent watchdog utility calls scripts that require Windows Script Host 5.6 at a minimum. If these scripts are run on a system running an earlier version of Windows Script Host (for example 5.1), then the script continues to run, and over time results in multiple cscript processes running on the system.

Upgrade Windows Script Host to version 5.6 or later.

Unable to deploy monitoring agents from the Tivoli Enterprise Portal

Receive an error when attempting to deploy an monitoring agent from a previous version of IBM Tivoli Monitoring through the Tivoli Enterprise Portal:

```
KFWITM291E An agent configuration schema was not found" error
popup.
```

The application support for the version being deployed must be installed to the portal server, or the agent configuration xml file (for example, `r2_dd_062100000.xml`) must be manually copied to the same location in the portal server (`../classes/candle/kr2/resources/config`) where the current-level configuration xml file (for example, `r2_dd_062200000.xml`) resides.

Installing application support with a silent installation response file fails

Running the Application Support Installer with a silent installation response file to apply application support on the monitoring server, the portal server, or the Tivoli Enterprise Portal fails and displays a failure message:

```
Error
java.lang.ArrayIndexOutOfBoundsException: 0
```

Additionally, the resulting application support files contained in the support package are not installed.

Using the Application Support Installer with the Silent Installation Response file option is not supported. The recommended mechanism for the installation is using the GUI interface.

Unable to run gsk7ikm.exe

Unable to run `c:\IBM\ITM\GSK7\bin\gsk7ikm.exe` as it fails with the following error

```
Failed to parse JAVA_HOME setting
```

On UNIX and Linux systems, complete the following steps:

1. Open console.
2. Get the IBM Java location by running the following script:
   ```
   CANDLEHOME/bin/ CandleGetJavaHome
   ```

3. Export variable JAVA_HOME to point to the IBM Java path. For 64bit, gsk7ikm has to be 64bit java.
4. Check the path for a local gskit. This path is `CANDLEHOME/config/ gsKit.config`. GskitInstallDir points to a 32bit GSKit and GskitInstallDir_64 points to a 64bit GSKit.
5. Run GSKit key manager by running the following depending on your system setup: `GskitInstallDir/bin/ gsk7ikm_32` (32bit on HP) `GskitInstallDir/bin/ gsk7ikm` (32bit on Linux, Aix, or Solaris) `GskitInstallDir _64/bin/ gsk7ikm_64` (64bit)

On Windows systems:

1. Run **cmd**.
2. Get the IBM Java location by running the following script:
   `CANDLEHOME\InstallITM\GetJavaHome.bat`
3. Set the JAVA_HOME variable that points to the IBM Java location.
4. Get the GSKit location by running the following script:
   `CANDLEHOME\InstallITM\GetGSKitHome.bat`
5. Change the directory to `GSKit path\bin`.
6. Run the `gsk7ikm.exe` file.

*_cq_*.log files appear

Some of the `*_cq_*.log` files are from seeding operations. So, exception messages are expected by design.

SPD: Installing a bundle on the wrong operating system, architecture, or kernel

When you attempt to install a bundle on a system that does not correspond to the correct binaries (for example, installing a 32 bit bundle on a 64 bit system, or installing a 2.4 kernel-level bundle on a 2.6 kernel-level system). Look at the logs (Software Package Block (SPB) logs are located in the temporary directory of the system, `/tmp` for UNIX or `%temp%` for Windows). These will show that GSKit could not be installed.

To identify the right bundle for a particular system, the generated Software Package Definition (SPD) file uses the naming convention: *product_code interp*.spd. The interp tells you in which operating system, architecture, or kernel the bundle can be installed.

Installing a Software Package Block (SPB) on top of an existing, running IBM Tivoli Monitoring agent

When you attempt to install another IBM Tivoli Monitoring agent bundle using Tivoli Configuration Manager (TCM) or the Tivoli Provisioning Manager (TPM) on a system that has another IBM Tivoli Monitoring agent running, the second agent is not successfully installed due to overlapping libraries and ports configuration.

To prevent this problem, stop the running agent, and use Tivoli Configuration Manager (TCM) or Tivoli Provisioning Manager (TPM) to install the second agent.

Problems with the SPB file

If an Software Package Definition (SPD) file, created with the **tacmd exportBundles** command, is moved to a different system to create an SPB, the files copied by the

tacmd exportBundles command need to be moved with the SPD file as well, and the SOURCE_DIR in the default_variable section of the SPD file needs to be updated to reflect the new directory where the agent files are located.

Installation was halted and now receive message about active install

If for any reason the installation was halted, either by invoking Ctrl-C or by a power outage, if you then run uninstallation, you receive the following message:

```
An install may currently be running in
"/data/itmfp6_preUPGR" from the following machine(s):
Continue with this uninstallation [1-yes, 2-no; "2" is default]?
```

Recovery from a hard kill of the installer is currently not a supported scenario since the current installer does not have built-in rollback capability. Executing a hard stop of the installer will leave some or all IBM Tivoli Monitoring functions (including uninstall) in an unpredictable or disabled state.

However, you should be able to continue with the uninstallation after ensuring that there is indeed no installation being run on the system.

Receive an install.sh error when installing two components or agents in the same installation directory

Installing two components or agents in the same `CANDLEHOME` or installation directory is supported as long as the user ID used to run the installation is always the same.

Installing two components or agents in the same `CANDLEHOME` or installation directory using different user IDs is not supported.

When attempting to install IBM Java 1.5.0 on Windows 64 bit system nothing happens

Only 32-bit browsers are supported on the AMD 64 Windows environment due to the lack of a native 64-bit Web Start or Java Plug-in supports.

During a remote Tivoli Enterprise Monitoring Server upgrade, you receive a "The Backup procedure for TEMS database files has failed." pop-up

During a remote Tivoli Enterprise Monitoring Server upgrade, you receive the following pop-up message:

```
"The Backup procedure for TEMS database files has failed. If you continue with the
installation your customized tables could be lost.
Would you like to abort the installation?"
```

If you click **YES**, there is a risk of losing your customized tables. To ensure that you do not lose data, complete the following steps:

1. Click **NO** and exit the upgrade installation.
2. Restart the remote Tivoli Enterprise Monitoring Server system.
3. Stop all the IBM Tivoli Monitoring components from the 'Manage Tivoli Enterprise Monitoring Services' window.
4. Rerun the upgrade installation now with the remote Tivoli Enterprise Monitoring Server in the stopped state.

The upgrade installation is complete.

On Solaris systems, GSKit installation fails to install

If you have previously installed GSKit, and then manually removed it, the installation might fail. Perform the following actions to remove the two gskit installations, and then continue the installation as normal:

```
pkgrm gsk7bas
pkgrm gsk7bas64
```

Remote configuration of deployed Monitoring Agent for DB2 agent fails

The following message is returned when running the tacmd addsystem command:

```
The agent action SETCONFIG failed with a return code of -1073741819
for product code ud.
```

Remote configuration and installation of a database agent requires that IBM Global Security Kit (GSKit) be installed in directory C:\Program Files\ibm\gsk7, or that the GSKit directory be defined in the Windows System environment variable ICCRTE_DIR. DB2 9.1 installs the GSKit package in C:\ibm\gsk7 and the ICCRTE_DIR environment variable is not exported as a System environment variable. Therefore, tacmd addsystem remote configuration processing cannot execute and results in the failure message reported to the user.

Choose one of the following resolutions that best fits your environment:

- Install the GSKit product by executing the InsGSKit.exe program in the target directory C:\Program Files\ibm\ directory.
- Assign the System Environment variable named ICCRTE_DIR to the directory path of the currently installed GSKit product (for example, C:\ibm\gsk7).
- When the error is reported, manually configure the Monitoring Agent for DB2 Service Startup Parameters to use the correct user name and password to interact with the DB2 9.1 product. Ensure that the InteractsWithDesktop Service is not enabled for this DB2 Agent Service.

Monitoring Server cannot find your deployment depot

If you create a shared deployment repository named *depot* on the server hosting the deployment depot and you create this repository in a subdirectory of the *depot* directory, the monitoring server will not be able to find your deployment depot, and you will receive this message:

```
KDY2077E: The specified agent bundle depot \\hubtems\depot is not a directory.
Either the agent bundle depot directory does not exist or it is not a directory.
The agent bundle depot directory does not exist because no bundles have been added.
```

Create the repository at the *C:\IBM\ITM\CMS* level of the directory structure, *not* at the *C:\IBM\ITM\CMS\depot* level. Then set DEPOTHOME to `DEPOTHOME=\\hubtems\centralrepository\depot`.

The agent installation log on the endpoint indicates that error AMXUT7502E occurred

The error AMXUT7512E might occur when running the Distributed Monitoring Upgrade Toolkit. The agent was not installed for one of the following reasons:

- There is another installation in progress that cannot complete until the computer is restarted.

–OR–

- You are attempting to install a component that is already installed.

Refer to the `lcfd.log` on the endpoint and the agent installation log as listed in Table 29 to determine the exact cause of the problem.

Table 29. lcfd log file

Windows	UNIX-based systems
install_dir/Install/Abort IBM Tivoli Monitoring timeStamp.log	*install_dir*/logs/candle_installation.log

Contact IBM Software Support if you cannot install the agent. See Chapter 2, "Collecting and reviewing troubleshooting data," on page 5 for information on what types of data to collect before contacting Support.

Failure occurs when sharing directories for the agent deploy depot

Although it is more efficient to use a network shared directory for the agent deploy depot directory, there are weaknesses that might negatively impact deployment in large enterprises:

- If an NFS is used to contain the depot and there is a problem with the NFS, then the deployment activity is suspended for all deployments in progress.
- For UNIX environments, the directories that are mentioned on the shared directory must have the names of each of the Tivoli Enterprise Monitoring Server servers.
- Administrator privileges need to be assigned based on a domain user ID. This is impractical and is contrary to the desired effect of sharing.

You receive a KFWITM290E error when using deploy commands with a z/OS monitoring server

Remote Deployment is not supported in environments with a z/OS Tivoli Enterprise Monitoring Server.

Running deployment in a hot-standby environment

The IBM Tivoli Monitoring hot-standby capability allows your monitoring environment to continue operating in the event of environmental or operational issues with the primary hub monitoring server (for detailed information about Tivoli Monitoring's hot-standby feature, see the *IBM Tivoli Monitoring High-Availability Guide for Distributed Systems*). You should refrain from deploying or updating agents when IBM Tivoli Monitoring is converting to a mirror monitoring server. No agent deployments or remote deployment operations should be executed from a hot-standby mirror hub, as this might cause your deployment transactions to get stuck in a queued state, and you might not be able to clear them.

Difficulty with default port numbers

You can use Telnet to test if the port is open in the firewall. Use the following command for this test:

```
telnet hostname 15001
```

where 15001 is the port number in question.

Selecting Security Validation User displays a blank popup

While configuring the Tivoli Enterprise Monitoring Server you have an option to select the Security Validation User. When selecting this option a blank popup is displayed. The Security Validation is working despite a blank popup with this label that has a yellow triangle and exclamation point:

```
TEMS User Authentication actions are needed!
```

When installing a monitoring agent on top of the Systems Monitor Agent, you receive an error

If you try to install a monitoring agent (that is not one of the agents built with IBM Tivoli Monitoring v6.2.2 Agent Builder) on top of the Systems Monitor Agent, you receive an error:

```
install.sh failure: KCI1163E cannot read file "/opt/IBM/ITM/registry/imdprof.tbl".
```

Monitoring agents that have been configured to connect to a monitoring server cannot be installed on the same system as those that have been configured for autonomous operation.

Also, monitoring agents that have been configured for autonomous operation cannot be installed on the same system as those that are connected to a monitoring server.

OS Agent does not install and a message indicates it was already installed

The file `status.properties`, located in `$DBDIR/AMX/data/` is not deleted when you uninstall the Upgrade Toolkit. The Upgrade Toolkit refers to the old `status.properties` file that contains information indicating there the OS Agent was installed. You might experience this problem if you do the following in the order listed:

1. Upgrade an endpoint.
2. Uninstall the Upgrade Toolkit.
3. Clean the endpoint manually.
4. Reinstall the Upgrade Toolkit.
5. Attempt to upgrade the endpoint you previously upgrade in 1.

use the following steps to verify that information in the `status.properties` file is causing this problem:

1. Open the `status.properties`,
2. Look for an entry like the following example:

   ```
   #Copyright IBM Corporation 2005 #Wed Sep 14 15:54:43 CDT 2005 @Endpoint\:
   \:east@EndpointClass\:TMF_Endpoint\:\:Endpoint=COMPLETE @Monitor\:Coast\
   :120401@Threshold\:critical=COMPLETE
   ```

   In this example, the status of the endpoint "east" is COMPLETE, which indicates that it was upgraded successfully. The witmupgrade command does not upgrade any item with the COMPLETE status and reports that it was already upgraded.

To upgrade the endpoint, the status for the endpoint "east" must be the INCOMPLETE, such as in the following example:

```
@Endpoint\:\:east@EndpointClass\:TMF_Endpoint\:\:Endpoint=INCOMPLETE
```

The only way to change the endpoint status in the `status.properties` file to INCOMPLETE is to perform a rollback on the upgrade of the item. See the *IBM Tivoli Monitoring: Upgrading from Tivoli Distributed Monitoring*.

Rolling back the upgrade

You can use the rollback option (**–r** option) of the **witmupgrade** command to remove the new IBM Tivoli Monitoring resources that you created. This is a necessary step if you want to repeat the test scenario. Rolling back the upgrade for the test scenario removes the Windows OS monitoring agent from the Windows endpoint and also removes the new situations and managed system list.

Follow these steps to roll back the upgrade:

1. Change to the `$DBDIR/AMX/shared/analyze` directory:
   ```
   cd $DBDIR/AMX/shared/analyze
   ```
2. Type the following command to roll back the upgrade:
   ```
   witmupgrade -x profilemanagers/DM_TEST_PM.xml -r -f scans/baseline.xml
   ```

   where:

   -x profilemanagers/DM_TEST_PM.xml
   Specifies the name and location of the output file that resulted from the assessment of the DM_TEST_PM profile manager.

   -r Indicates that the purpose of this command is to perform a rollback.

   -f scans/baseline.xml
   Specifies the name and location of the baseline file to use as input for this command.
3. Restart the Windows endpoint.

The rollback option can also be used to roll back an endpoint upgrade or a profile upgrade independently. By rolling back the profile manager upgrade, you roll back all upgrades (profile manager, profile, and endpoint) in one step.

"SQL1_OpenRequest status = 79" return code occurs during when upgrading an agent

The return code `SQL1_OpenRequest status = 79` occurs in the agent log when the application support is added during an upgrade. This return code results from an attempt to delete a table entry that does not exist in the table. When you add application support for a V6.1 agent, the return code is expected behavior because the agent application support data does not exist in the table.

An IBM Tivoli Monitoring 6.1 upgraded agent is not configured to point to the same Tivoli Enterprise Monitoring Server as it was before upgrading the agent

During upgrade of agents from OMEGAMON 350 to IBM Tivoli Monitoring 6.1, the OMEGAMON 350 agent specific Tivoli Enterprise Monitoring Server configuration data does not persist to the upgraded IBM Tivoli Monitoring 6.1 agent. The upgraded agents are configured to use the agent default settings. Do the following to change the default settings configured for OMEGAMON 350:

1. Right-click an agent in the Manage Tivoli Enterprise Monitoring
2. Select **Set defaults for all agents ...**

Installation of OS agent on a Microsoft Windows Server 2003 fails with this error: "Unable to establish BSS1 environment, can't continue.."

This error is caused by the deletion of the gskit directory, whether intentionally or by accident, without clearing the registry information. If gskit was previously installed by another product and has a dependency on it, for example DB2 9.1, then let that product reinstall it, or if there are no other products that depend on the version of that gskit, then you can clear the GSK7 entry in the registry that can be found under `My Computer\HKEY_LOCAL_MACHINE\SOFTWARE\IBM\GSK7`. Then rerun the IBM Tivoli Monitoring installation to allow the gskit to be reinstalled.

Note: Create a backup of the registry before editing it.

After upgrading to IBM Tivoli Monitoring V6.1, the link to the Queue Statistics workspace in the navigation tree is incorrect

The link to the Queue Statistics workspace in the navigation tree opens the Open Queue Handles workspace instead of the Queue Statistics workspace. Use the following steps to correct the link:

1. Open the Queue Statistics workspace from the navigation tree.
2. Ensure that Queue Statistics workspace opened instead of the Open Queue Handles workspace.
3. From the Tivoli Enterprise Portal select **Edit** > **Properties**.
4. Place a check in the **Assign as default for this Navigator Item** box.

Some rows do not display in an upgraded table

You might not see all tables after upgrading the Warehouse Proxy to IBM Tivoli Monitoring V6.1 because some tables might be corrupted. Do the following to find the errors that occurred during the upgrade:

1. Edit the `KHDRAS1_Mig_Detail.log` file.
2. Search for the word EXCEPTION.

The KHD_MAX_ROWS_SKIPPED_PER_TABLE environment variable allows you to skip bad data. KHD_MAX_ROWS_SKIPPED_PER_TABLE indicates the number of rows per table to skip to migrate if the data that needs to be inserted is incorrect. When this number is reached, migration of the table is aborted.

Tivoli Enterprise Monitoring Server and Tivoli Enterprise Portal Server automatically start after running Application Support Installer

After running the Application Support Installer the Tivoli Enterprise Monitoring Server and Tivoli Enterprise Portal automatically start, even if they were not running before the install. The behavior is harmless and there is no workaround currently.

Errors occur during installation of Event IBM Tivoli Monitoring Event Forwarding tool

The product functions normally in spite of the error. Check the installation log for more details.

```
One or more errors occured during the replacement of files (tecSyncAllFile1)
with files (tecSyncAllFile1).
Refer to install log for more details.
```

```
One or more errors occured during the replacement of files (tecSyncAllFile2)
with files (tecSyncAllFile)1.
Refer to install log for more details.
One or more errors occured during the replacement of files (tecSyncAllFile3)
with files (tecSyncAllFile1).
Refer to install log for more details.
.
.
.
```

Missing LSB tags and overrides warning message at the end of installation

During the installation process, you might see these unexpected warning messages:

```
insserv: warning: script 'S02ITMAgents2' missing LSB tags and overrides
insserv: warning: script 'ITMAgents2' missing LSB tags and overrides
```

These warnings are caused by an older installer missing some tags required by the chkconfig utility, used to manage system startup files. These warnings do not adversely affect the installation, and can safely be ignored.

Windows installation problems and resolutions

On Windows systems, the installation fails randomly when installing different features

On Windows systems, the installation fails randomly when installing different features. An example of the error looks like:

```
7-9-2008 10:49:35 OnMiaMoving - Processing Feature [KIWWICNS]
7-9-2008 10:49:35 OnMiaMoving - Error log
[C:\IBM\ITM\InstallITM\MiaError.log] created.
7-9-2008 10:49:35 OnMiaMoving -
Feature KIWWICNS [Tivoli Enterprise Portal Server Extensions]
 will be installed.
7-9-2008 10:49:35 OnMiaMoving -
CMD[C:\temp\tmv621-d8185a-200807040554.base_windows\WINDOWS\KIWWICNS.exe]
 Parameters[backup=n force=y silent=y "installdir=C:\IBM\ITM"
 "backupdir=C:\IBM\ITM\Backup\MIA"
 "-lC:\IBM\ITM\InstallITM\MiaInstall.log"] issued.
7-9-2008 10:51:23 OnMiaMoving -
Install for Feature[KIWWICNS/Tivoli Enterprise Portal Server Extensions]
 successful RC=-1073741819.
7-9-2008 10:51:32 OnMiaMoving -
Install for Feature[KIWWICNS/Tivoli Enterprise Portal Server Extensions]
 may have failed, please check!
```

Checking the %CANDLE_HOME%\MiaInstall.log file you find errors similar to:

```
2008/07/09 10:48:35 [D] Installing file: CNPS\classes\cnp.jar
 --> C:\IBM\ITM\CNPS\classes\cnp.jar
2008/07/09 10:48:35 [C] EXTRACTFILE src='CNPS\classes\cnp.jar'
 dest='C:\IBM\ITM\CNPS\classes\cnp.jar'
2008/07/09 10:48:37 [E] ERROR: File extraction failed: CNPS\classes\cnp.jar
 -> C:\IBM\ITM\CNPS\classes\cnp.jar (3)
2008/07/09 10:48:37 [S] Internal Error - trying rollback
2008/07/09 10:48:37 [S] Attempting to stop child process
2008/07/09 10:48:51 [S] Rollback successful
```

The return code (3), indicates the software could not create a file due to either an issue with file permissions or a corruption on the hard drive. First check the file

permissions of the destination file. Running the Windows chkdsk and defragmentation programs might resolve issues with corruption on the physical hard drive.

Problems that are cleared by rebooting the Windows system

There are a set of problems that are cleared by rebooting the Windows system that has been installed or upgraded:

- Situations do not fire after upgrade
- Remote update of a Windows system fails because of a pending rename that requires a reboot

  Note: In this case, a 'RC_INFO: Pending rename operations found, must reboot before install can continue' message is found in the Abort IBM Tivoli Monitoring for `Databases.log` file.

When installing and configuring the Tivoli Enterprise Monitoring Server on Windows Server 2008, a number of popups and errors occur

To install and configure the Tivoli Enterprise Monitoring Server on Windows Server 2008, there are a number of manual steps and workarounds that must be performed:

1. Disable the Windows firewall by following these steps:
   a. Login to Windows Server 2008, and start the Server Manager.
   b. In the Security Information section, click **Go to Windows Firewall**.
   c. In the Overview section, click **Windows Firewall Properties**. This displays the Windows Firewall with Advanced Security window.
   d. To completely disable the firewall, it must be turned off in 3 places in the window:
      - Domain Profile
      - Private Profile
      - Public Profile

      Each of these tabs must be individually selected, and the Firewall state must be changed to Off. Each time you change the state to Off, click **Apply**.
   e. After you have changed the Firewall state in all of the profiles, click OK.
2. Configure the monitoring server to work correctly with Windows User Account Control (UAC).
   - Using Windows Explorer, navigate to the IBM Tivoli Monitoring product install directory (default is `c:\IBM\ITM`).
   - Navigate to the appropriate subdirectory, right-click one of the executable files listed below, and select Properties.
     - `itm_home\CMS\cms.exe`
     - `itm_home\CMS\kdsmain.exe`
     - `itm_home\CMS\kdstsns.exe`
     - `itm_home\InstallITM\kinconfg.exe`
   - When the Properties window appears, select the Compatibility tab.
   - In the Privilege Level section, check the box next to "**Run this program as an administrator**.
   - Click **OK**.
   - Repeat this procedure for each of the files listed.

After an upgrade, the Tivoli Enterprise Portal Server is in the 'stop pending' state and cannot be manually started

After the upgrade, the Tivoli Enterprise Portal Server was in the 'stop pending' state. Attempts to manually start the Tivoli Enterprise Portal Server failed. End the kfwservices process from the Windows task manager and then attempt the manual start. Your Tivoli Enterprise Portal Server can then be started and stopped.

This behavior can happen if a program that locks files is running in the background, such as Norton Antivirus.

When running the setup.exe, an unknown publisher error message displays

If you run the `setup.exe` from a network drive on Windows, a window displays with the following message:

```
File Download - Security Warning
The Publisher could not be verified.
Are you sure you want to run this software?
```

Selecting **Cancel** closes the window and the installation cannot complete. To install the software without this problem, map the network drive and run the `setup.exe` file from a DOS prompt.

The error "Could not open DNS registry key" occurs

This message is informational an no action is required. The Windows agent reports the fact that it could not find a registry entry for the DNS Server Event Log, indicating that the DNS Server Event Log is not installed. You can stop all situations and recycle the Tivoli Enterprise Monitoring Server with no situations in ACTIVATE AT STARTUP to prevent this message being written to the trace log.

Agent not connecting to Tivoli Enterprise Monitoring Server

If you find a message similar to "Unable to find running TEMS on CT_CMSLIST" in the Log file, the Agent is not connecting to the Tivoli Enterprise Monitoring Server. Confirm the following to ensure connectivity:

- Multiple network interface cards (NICs) exist on the system.
- If multiple NICs exist on the system, determine which one is configured for the monitoring server. Ensure that you specify the correct hostname and port for communication in the IBM Tivoli Monitoring environment.

InstallShield displays the error "1607: Unable to install InstallShield Scripting Runtime" during installation on Windows from a network-mounted drive

When running `setup.exe` on Windows from a network mounted drive, the following error occurs:

```
InstallShield: 1607: Unable to install InstallShield Scripting Runtime.
```

This is an InstallShield limitation. You cannot install the product from the specified network drive. Try installing from another network drive. Install the product from a local drive if you continue to receive the error.

Installation on a Windows 2003 server fails with Error Number: 0x80040707

The following error can occur while installing IBM Tivoli Monitoring V6.1 on a Windows 2003 Server:

This error can occur for the following reasons:

1. Windows Service Pack 1 (or higher) is not installed.
2. Windows Installer 3.1 (KB893803) is not installed.

KB893803 is included in SP1. You must install Windows Service Pack 1 or higher or the KB893803 individual update. You can download the update from www.windowsupdate.com.

Extracting the nls_replace script causes remote deployment to fail

The tool used to extract the file might have an option to automatically convert CRLF for text files. If users extract the UNIX or Linux installation media tar files on Windows and this option is enabled, the files are modified and become incompatible on some platforms. The CR/LF conversion must be disabled or another tool used to extract the files that does not convert the text files.

Upgrade tool deploys agent to the wrong directory

The baseline XML file used for Tivoli Distributed Monitoring upgrade contains attributes that specify an installation directory for OS monitoring agents on Tivoli endpoints. When an endpoint is upgraded, the Upgrade tool normally deploys the OS monitoring agent to the specified directory on the endpoint. However, if the CANDLE_HOME environment variable is already set on a Windows endpoint, the Upgrade tool deploys the monitoring agent to the directory specified by the environment variable, even if a different directory is specified in the baseline file. The CANDLE_HOME environment variable is already set if any IBM Tivoli Monitoring V6.1 component is already installed on the endpoint.

Deploying an agent instance without providing any configuration properties causes KUICAR020E error

The problem occurs after you have already successfully deployed a multi-instance agent (such as a database agent) to a node, and then tried to deploy another instance without providing any configuration properties (which is an error). You see this error message:

```
KUICAR020E: The addSystem command did not complete because a deployment error
occurred.
Refer to the following error returned from the server:
 The monitoring server encountered an error while deploying the managed system.
The kuiras1.log file may provide more information about this error.
 If you require further assistance resolving the error, contact IBM Software
Support.
The agent received incorrect SQL.
The CONTEXT column was not specified and is a required parameter.
```

A correct message would tell you that required configuration properties were not provided when using the -p|--property|--properties command line option. When you have provided the required configuration properties using the -p|--property|--properties command line option, the agent instance is properly deployed.

Uninstallation is not available for Application Support on Windows systems

Currently, there is not a workaround.

Problems installing directly from the .zip file

Instead of installing directly from the `.zip` file, extract the files from the `.zip`, and then install from the `setup.exe` file.

Installation hangs or loops after presenting initial splash screen

When installing IBM Tivoli Monitoring or IBM Tivoli Monitoring agents on Windows systems, IBM Tivoli Monitoring installation should present a pop-up requesting reboot if files are locked. However, there are times when the IBM Tivoli Monitoring installation does not inform you of locked files. This can cause the IBM Tivoli Monitoring installation to loop or hang. If you experience a delay longer than fifteen minutes during an IBM Tivoli Monitoring Windows installation, cancel the IBM Tivoli Monitoring install processes and reboot the system.

Unable to discover systems within a specified IP range when running the Startup Center from eclipse.exe

If you run the Startup Center from **eclipse.exe**, the distributed installation process might not discover systems within the IP range that you specify. Instead, run the Startup Center from **launchStartup.bat**. Note that this behavior is limited to distributed installations of Windows systems, not of Linux or UNIX systems when running the Startup Center from **launchStartup.sh**.

UNIX-based system installation problems and resolutions

This chapter describes known problems related to installation and uninstallation that might occur with IBM Tivoli Monitoring.

On a RHEL6 64-bit system, the Tivoli Monitoring installer fails with errors

On a RHEL6 64-bit system, the Tivoli Monitoring installer fails with errors similar to the following example:

```
--------------------------------
runGSkit: ----- Running command:
/opt/IBM/ITM/li6243/gs/bin/private_verifyinstall -----
/opt/IBM/ITM/li6243/gs/bin/gsk7ver: error while loading shared
libraries: libstdc++.so.5: cannot open shared object file:
No such file or directory Error: Verify Failed
Expected Details of gskit in /opt/IBM/ITM/li6243/gs
Got
runGSkit: return code from command is 99
runGSkit: ----- End of running command -----
runGSkit: error Return error code: 99
runGSkit: error GSKit check failure, script: /opt/IBM/ITM/li6243/gs/bin/
private_verifyinstall
runGSkit: error li6243 - GSK check error, verifyInstall test failed
runGSkit: Backup failed GSKit installation into /opt/IBM/ITM/tmp/badGSKit_keep.tar
```

Tivoli Monitoring requires both the 32-bit and 64-bit compat-libstdc++ libraries installed on the 64-bit system. The installation fails because of the missing 32-bit libstdc++.so.5.

Use the following commands to verify that both the 32-bit and 64-bit versions of the libraries are installed. An example of the command output is displayed below:

```
--------------------------------
# rpm -q --filesbypkg compat-libstdc++-33
compat-libstdc++-33 /usr/lib64/libstdc++.so.5
compat-libstdc++-33 /usr/lib64/libstdc++.so.5.0.7
compat-libstdc++-33 /usr/lib/libstdc++.so.5
compat-libstdc++-33 /usr/lib/libstdc++.so.5.0.7

# rpm -q --qf "%{NAME}-%{VERSION}-%{RELEASE}.%{ARCH}\n"
compat-libstdc++-33
compat-libstdc++-33-3.2.3-61.x86_64
compat-libstdc++-33-3.2.3-61.i386
```

If any entries under `/usr/lib64` are missing under `/usr/lib`, locate and install the 32-bit version of the compat-libstdc++-33 package.

Application agent remote deployment on workload partition fails

The remote deployment of an application agent fails with the error:

```
KDY0034E: An unexpected error occurred. The agentpc agent was restarted
but the agent version is not as expected. Current agent version is
agentVersion and the expected version is expectedVersion. The deployment
failed as the expected agent version is different from the current version.
```

To enable remote deploy on some workload partitions, you must change the `install.sh` file, located in the Tivoli Monitoring depot:

```
CANDLE_HOME/tables/TEMS/depot/PACKAGES/unix/kci/<VERSION>/install.sh
```

Replace the following part:

```
if [ -n "$fieldSep" ]  # BigK.
then
  cat $rFile | grep -i "$thisMachShort" > /dev/null 2>&1
  [ $? -eq 0 ] || return
  fld23=$(cat $rFile | grep -i "$thisMachShort" | cut -d "$fieldSep" -f2-4)
    # fld23 -> ms|35594
else  # dinkySQL.
  cat $rFile | sed "s/  */ /g" | grep -i "$thisMachShort" | cut -c1 | grep "N"
     > /dev/null 2>&1
  [ $? -eq 0 ] || return
  fld23=$(cat $rFile | sed "s/  */ /g" | grep -i "$thisMachShort" | grep "^N"
     | cut -d" " -f2)  # fld23 -> ms35594
fi
```

with this part:

```
typeset thisMachHostname=$(hostname|cut -d. -f1)
typeset thisMachNetwork=$($CANDLEHOME/bin/ITMhostName -na|sed 's/ /|/g')
typeset thisMachList="$thisMachShort|$thisMachHostname|$thisMachNetwork"

  if [ -n "$fieldSep" ]  # BigK.
  then
    cat $rFile | egrep -i -e "($thisMachList)" > /dev/null 2>&1
    [ $? -eq 0 ] || return
    fld23=$(cat $rFile | egrep -i -e "($thisMachList)" | cut -d "$fieldSep" -f2-4)
      # fld23 -> ms|35594
  else  # dinkySQL.
    cat $rFile | sed "s/  */ /g" | egrep -i -e "($thisMachList)" | cut -c1 | grep
       "N" > /dev/null 2>&1
```

```
  [ $? -eq 0 ] || return
  fld23=$(cat $rFile | sed "s/  */ /g" | egrep -i -e "($thisMachList)" | grep
     "^N" | cut -d" " -f2)  # fld23 -> ms35594
fi
```

Message is received about the Korn Shell after running the `install.sh` file

You receive the following message after running the `install.sh` file:

```
This system is using a version of the Korn Shell (ksh) which will allow the
installation of specific older releases of ITM Monitoring application agents
to regress the installation, configuration and execution tools for
this installation. Refer to the Flash note titled
"Newer ksh shell may allow regression of ITM installation"
for more information, including steps to take to avoid damage
to your IBM Tivoli Monitoring installation.
```

This technote includes detailed descriptions of the root cause, and also information on how to deal with this issue:

```
http://g01zciwas003.ahe.pok.ibm.com/support/dcf/preview.wss?host=g01zcidbs003.ahe.\
pok.ibm.com&db=support/swg/tivtech.nsf&unid=FACF542BAA62D17B8525765C006BC192&\
taxOC=SSCQLMD&MD=2009/11/05%2012:11:58&sid=
```

AIX stat_daemon memory leak

There is a memory leak in the process stat_daemon that is fixed by an AIX APAR on AIX 5.3 and AIX 6.1. To fix the memory leak, install APAR IZ62080 for AIX 5.3 and APAR IZ58432 for AIX 6.1.

UNIX and Linux install.sh command fails with error code: 99 and error code: 4

Installation on UNIX and Linux systems uses `install.sh` command; running this command fails with a "runGSkit failure: Return error code: 99" and a "install.sh failure: Return error code: 4". Because it failed within runGSkit when it called verifyInstall, review the *`InstallDirectory`*`/logs/candle_installation.log` file and look for references to runGSkit. For example, output similar to the following might be present:

```
runGSkit: ----- Running command: /opt/IBM/ITM/ls3263/gs/bin/private_verifyinstall
/opt/IBM/ITM/ls3263/gs/bin/gsk7ver: error while loading shared libraries:
libstdc++.so.5:
cannot open shared object file: No such file or directory
Error: Verify Failed
Expected Details of gskit in /opt/IBM/ITM/ls3263/gs
Got
runGSkit: return code from command is 99
runGSkit: ----- End of running command -----
runGSkit: error Return error code: 99
runGSkit: error GSKit check failure, script: /opt/IBM/ITM/ls3263/gs/bin/private_
verifyinstall
runGSkit: error ls3263 - GSK check error, verifyInstall test failed
```

In the example above, the `libstdc++.so.5` file is not present. This comes from the package compat-libstdc++-33-3.2.3-61.s390.rpm. When this package is installed, the problem no longer occurs.

Receive KUIC02101W error

The error states that the Java Runtime Environment shared library could not be loaded. Java will execute using unsecured credentials.

On some Solaris, Linux, and HP platforms, IBM Tivoli Monitoring has files with different bit sizes: executable files are 64 bit, while the provided JRE is 32 bit. This mismatch does not allow the JNI to work properly, so the current method cannot be used, and the previous method will be used.

Receive JVMDG080 or JVMXM012 Java errors

- RedHat 5.0 ships with "SE Linux" turned on by default. It has to be set to permissive in order for the install to run. Edit the `/etc/selinux/config` file to specify SELINUX=permissive.
- A Java library is missing classes. Install the following to get libXp.so.6:
  - libXp-1.0.0–8.s390x.rpm
  - libXp-1.0.0–8.s390.rpm
- The just-in-time compiler (JIT) needs to be turned off. Issue the export JAVA_COMPILER=NONE command before issuing `./install.sh`.

On HP-UX systems, where the hostname does not equal the nodename, the upgrade installation fails to stop running processes

Running IBM Tivoli Monitoring processes were not shutdown by the installer during the upgrade of the Tivoli Enterprise Monitoring Server or agents when the nodename does not equal the hostname on HP-UX systems. On HP-UX, if the system has a hostname longer than 8 characters then the nodename should be set to 8 characters or less. If the nodename and the hostname are not in sync then the you must shutdown all IBM Tivoli Monitoring processes before starting an addition product installation or upgrade.

EIF Slot Customization does not work on upgraded zlinux systems

When you open the EIF Slot Customization Editor from the Situation editor, slot names under the Base Slots panel do not display for the class. Clicking **Select Event Class** does not cause default event classes to display. When typing a new event class name, slot names under the Base Slots panel do not display.

The following setting should be added to the *CANDLEHOME*/*platform*/iw/profiles/ITMProfile/config/cells/ITMCell/nodes/ITMNode/servers/ITMServer/server.xml file. The section: genericJvmArguments="-DKFW_DATA=/products/e6/itm/ls3263/cq/data"/> should be changed to: genericJvmArguments="-Djava.compiler=NONE -DKFW_DATA=/products/e6/itm/ls3263/cq/data"/>.

The portal server must be restarted to have this change go into effect.

Running of the KfwSQLClient binary fails on Linux and AIX systems

Depending on the system, the following environment variable should be set before running the command:

- Linux: LD_LIBRARY_PATH
- Aix: LIBPATH

The variable value can be taken from the CANDLEHOME/config/cq.config file.

Failed to attach to the DB2 instance db2inst1 ERROR: Unable to create TEPS, return code = 3

While installing a Tivoli Enterprise Portal Server on a UNIX based system and using a DB2 database, the following error message is displayed (where db2inst1 is the supplied name of the DB2 instance):

```
Failed to attach to the DB2 instance db2inst1
ERROR: Unable to create TEPS, return code = 3
```

Ensure that the DB2 instance is started by running the **db2start** command as the instance user:

```
$ su - db2inst1
$ db2start
```

Installation on SLES9 terminates with install.sh failure:KCI1008E terminating... license declined

On systems when LAP cannot run and Java does not function, a bad return code is returned to `install.sh`. The problem can be manually recreated by running the JAVA command used to launch LAP or simply by running Java –version from the jre under `CANDLEHOME`. Indications show that the system might be missing an OS patch required for the level of Java or possibly an incorrect version of Java has been packaged and installed on the system.

Command line interface program of the Application Support Installer is not currently available

The command line interface program of the Application Support Installer is not currently available, thus you cannot run the install in command line mode. However, you can run the install in silent mode instead. If your UNIX or Linux computer does not have X-Windows set up, you must use the silent installation method.

Silent installation on UNIX-based systems of Tivoli Enterprise Monitoring Server returns an encryption key setting error

The following errors occurs if you attempt a silent install on UNIX-based systems or UNIX-based systems and the encryption key is not exactly 32 characters.

```
Exception in thread "main" candle.kjr.util.CryptoFailedException:
CRYERR_INVALID_KEY_LENGTH
 at candle.kjr.util.CRYPTO.validateKeyLength(CRYPTO.java:911)
 at candle.kjr.util.CRYPTO.setKey(CRYPTO.java:452)
 at ITMinstall.gskSetkey.<init>(gskSetkey.java:179)
 at ITMinstall.gskSetkey.main(gskSetkey.java:26)
```

Set the encryption key parameter in the silent install file to exactly 32 characters as in the following example:

```
INSTALL_ENCRYPTION_KEY=IBMTivoliOMEGAMONEncrytionKey61
```

The error "Unexpected Signal: 4 occurred at PC=0xFEC3FDE4" occurs during installation

A Java VM heap dump occurs during installation, which uses the JRE. Use the following steps to resolve the problem:

1. In a terminal window, run the following command to display the Java command:

   ```
   java -version
   ```

2. Determine where the Java executable is located by running:
   ```
   which java
   ```
3. Rename or uninstall the Java executable.

   Note: This effects any other applications which depend on Java. Be sure that it is safe to do so. If unsure just rename the Java executable.
4. Run the following command again to ensure that the java executable is not found in the path:
   ```
   which java
   ```
5. Install the product.

Installing IBM Tivoli Monitoring on Red Hat 5 and see the following error: "KCI1235E terminating ... problem with starting Java Virtual Machine"

If you try to install IBM Tivoli Monitoring on Red Hat 5 with SELinux set to "permissive" or "disabled" mode ("enforced" mode is not supported by IBM Tivoli Monitoring) directly after rebooting the system, and you see the following error: "KCI1235E terminating ... problem with starting Java Virtual Machine" at the beginning of the installation before the license is displayed, try executing the **prelink -a** command to resolve the issue.

Installation of the IBM Tivoli Monitoring on the Linux S390 R2.6 64-bit operating system fails with the message "LINUX MONITORING AGENT V610Rnnn unable to install agent" where nnn is the release number

Perform the following steps to resolve this problem before running the installation again:

1. Run the following command before running any installation or configuration command for the agent:
   ```
   export JAVA_COMPILER=NONE
   ```
2. Install the `s390x.rpm` RPM (Red Hat Package Manager) files, in addition to the `s90.rpm` files, located in the CD ISO images for Red Hat As 4.0 s390x:
   - `compat-libstdc++-295-2......s390x.rpm`
   - `compat-libstdc++-33-3.......s390x.rpm`

     It requires the two `s390x.rpm` files, in addition to the `s390.rpm` files. You can obtain the required RPM files from the CD for Red Hat As 4.0 s390x.

The UNIX OS agent (ux) version 350 does not start on AIX 5.3 after upgrading other agents to version 6.1.0

Do one of the following to enable UNIX OS agent (ux) version 350:

- Upgrade the UNIX OS agent to version 6.1.0.

  –OR–
- Add the following line to the `uxaix513.ver` file in the `$CANDLEHOME/registry`:
  ```
  runArch = aix533
  ```

Note: Create a backup of the registry before editing it.

Troubleshooting z/OS-based installations

This section describes some problems you might experience with z/OS-based installations, including problems you can resolve with the Installation and Configuration Assistance Tool (ICAT). It includes the following sections:

IBM Tivoli Monitoring z/OS initialization checklist

Use the IBM Tivoli Monitoring z/OS initialization checklist to troubleshoot problems with your IBM Tivoli Monitoring installation on z/OS. The IBM Tivoli Monitoring z/OS initialization checklist includes the following sections:

Tivoli Monitoring Services Engine initialization

Tivoli Monitoring Services Engine is a collection of basic Operating System and Communication service routines built specifically for the OS/390® and z/OS Operating environments. All IBM Tivoli Monitoring address spaces load and employ the services of Tivoli Monitoring Services Engine.

Initializing the Tivoli Monitoring Services Engine service: Tivoli Monitoring Services Engine successful initialization is noted by message KLVIN408 IBM OMEGAMON PLATFORM ENGINE VERSION 400 READY. There are two classes of Tivoli Monitoring Services Engine initialization failures:

- Failures that result from unsupported Tivoli Monitoring Services Engine startup parameters. For example: `User abend U0012`
- Failures that result from protocol initialization failures. For example: `User abend U0200`

Repairing Tivoli Monitoring Services Engine initialization failures: For U0012 Abends, incorrect Engine STARTUP parameters, examine and correct the parameters pointed to by the RKLVIN DD statement of the started task JCL. Most often, U0012 Abend failures can be resolved by backing out the last change made to the Tivoli Monitoring Services Engine startup parameters. For U0200 Abends, the root cause of the protocol failures must be remedied. These failures are covered in "TCP/IP service initialization" on page 96 and "SNA service initialization" on page 98.

RAS1 service initialization

The Reliability, Availability and Servicability (RAS1) service refers to the RAS1 building block (Basic Services component) used for diagnostic tracing. Nearly all diagnostic information for IBM Tivoli Monitoring is delivered via the RAS1 (trace) component. This component is configured in member KBBENV of RKANPAR using the KBB_RAS1 environment variable. Often, customers redirect the initialization member via CT/Engine INITLIST processing. INITLIST processing is

always echoed to the RKLVLOG with the KLVIN411 message. The following shows an example of a typical KBBENV override to KDSENV

```
KLVIN410 INITLIST MEMBER KDSINIT BEING PROCESSED
 KLVIN411 KLVINNAM=KDSINNAM
 KLVIN411 KLVINTB=KDSINTB
 KLVIN411 KLVINVLG=KDSINVLG
 KLVIN411 KLVINNAF=KDSINNAF
 KLVIN411 KLVINVPO=KDSINVPO
 KLVIN411 KLVINSTG=KDSINSTG
 KLVIN411 KLVINVAM=KDSINVAM
 KLVIN411 KBBENV=KDSENV
```

In this instance, configuration of KBB_RAS1 must display in member KDSENV of RKANPAR.

TCP/IP service initialization

TCP/IP service is Transmission Control Protocol. TCP/IP provides end-to-end connectivity for application-layer codes such as telnet, FTP, and the IBM Tivoli Monitoring Server, Tivoli Enterprise Portal Server, and the Tivoli Enterprise Monitoring agents.

Initializing the TCP/IP service: TCP/IP services for this address space are available if any of the following messages are present:

```
"KDE1I_OpenTransportProvider") Transport opened: socket/ip.tcp
"KDE1I_OpenTransportProvider") Transport opened: socket/ip.pipe
"KDE1I_OpenTransportProvider") Transport opened: socket/ip.udp
```

These messages are only displayed when KDC_DEBUG=Y is active in the environment; KDC_DEBUG=Y must be added to member KDSENV of RKANPAR (or the appropriate initialization member) to obtain the level of tracing required to have these messages echoed to the RAS1 log. IF KDC_DEBUG=Y is set and if none of these messages are in the log, then initialization of the TCP/IP service failed.

Repairing TCP/IP service initialization failures: Use the following steps to ensure the TCP/IP transport service is available:

Note: Failure at any of the following prevents the TCP/IP service from initializing in the address space.

1. Ensure the INITAPI service is successful. See “The INITAPI call” on page 96.
2. Ensure the Name Resolution is successful. See “Name Resolution” on page 97.
3. Ensure the first SEND ran without error. See “The First SEND” on page 98.

The INITAPI call

IBM's implementation of TCP/IP requires that an address space perform an INITAPI before issuing an TCP/IP service request. The INITAPI establishes a communication pipe between the TCP/IP and the OMEGAMON Platform address space. The INITAPI identifies the TCP/IP stack to be used by name. The TCP/IP stack name used in the INITAPI is configured in the KLXINTCP member of RKANPAR. This step must complete successfully. An INITAPI failure is fatal: no TCP/IP services are available to the address space.

Confirming that the INITAPI call was successful: The following messages indicate a successful INITAPI:

```
KLXIN001 HPNS INTERFACE AVAILABLE
KLXIN001 SOCKET INTERFACE TO TCPIPL AVAILABLE
```

Repairing the INITAPI call failures: Most of INITAPI failures are the result of the wrong name specified in KLXINTCP. The following is a classic example of an INITAPI failure:

```
KLVIN405 STARTUP MODULE: KLXINTCP, SEQUENCE(1), USING RKANPAR MEMBER KLXINTCP
KLXIN001 TCP/IP CONFIGURATION: TCP/IP_USERID=TCPIPG
KLXIN003 TCP/IP INTERFACE INITIALIZED
KLXIN009 SOCKET INTERFACE TO TCPIPG UNAVAILABLE: RC(FFFFFFFF) ERRNO(000003F3)
KLXIN004 TCP/IP INTERFACE NOT OPENED: RC(4)
```

Notice that the INITAPI failure is characterized by a return code of (-1) and an ERRNO value, in this case X'3F3' or decimal 1011. ERRNO-s have names. These names are found in TCPERRNO.H and decimal 1011 is EIBMBADTCPNAME. The most common INTIAPI ERRNOs are EMVSINITIAL (156), EIBMBADTCPNAME(1011), and *no-name*(10218).

Reasons for INITAPI failures include:

- The name specified in KLXINTCP is wrong. TCP/IP_USERID is selected based on the specification for TCPIPJOBNAME found in the file pointed to by SYSTCPD in the TCP/IP started task JCL. The default (if no TCPIPJOBNAME exists) is TCPIP. There exists field documentation on the RACF® procedure. These two items should be checked first.
- The started task name does not have RACF authority for the OMVS segment. All address spaces must be given RACF (or ACF2) permission for the OMVS segment to use TCP/IP services. Failure to grant this permission (which is granted to the started task name) can result in INITAPI failures.
- MAXPROCUSER has been exceeded. For MAXPROCUSER problems, you can use console operator command SETOMVS MAXPROCUSER=xxx to increase the current MAXPROCUSER value (as seen by D OMVS,O).

Name Resolution

IBM Tivoli Monitoring V6.1 depends on IBM's HPNS EZASMI getaddrinfo and EZASMI getnameinfo calls for resolver services. These calls are used to find the symbolic name and dotted-decimal IP address of the default network interface for the z/OS image. A failure in either EZASMI call results in failure to initialize the TCP/IP service for the z/OS address space.

Confirming that the Name Resolution calls are successful: The following message indicates Name Resolution was successful:

```
kdebprc.c,661,"interface_discovery") IPV4 interface list: 'SYSL'
 9.42.46.26: source=hostname:0, seq=0, flags=0441
```

In this example, the interface 'SYSL' is found and **source=hostname** indicates that the hostname SYSL was successfully resolved to an IP address.

Repairing the Name Resolution failures: The following messages illustrate a Name Resolution failure:

```
kdebprc.c,661,"interface_discovery") IPV4 interface list: 'WINMVS2C'
9.20.138.199: source=GE1, seq=0, flags=0441
kdebprc.c,214,"register_string") Unable to resolve interface address: WINMVS2C
```

In the messages above, the absence of **source=hostname** indicates an interface was discovered but the name is not resolvable to an address. Typically, this error results when the z/OS image does not contain a TCP/IP resolver setup file that provides either GLOBAL or DEFAULT configuration data. Consequently, native z/OS address spaces are not enabled for name resolution by default. By adding a DD

statement for SYSTCPD to the started task JCL of the IBM Tivoli Monitoring task (pointing to a usable file in USER.PARMLIB(TCPDATA)), resolver support can be enabled.

The following messages illustrate a variant of name resolution failure:

```
kdebprc.c,661,"interface_discovery") IPV6 interface list: 'NULL'
"KDE1I_OpenTransportProvider") Status 1DE00048=KDE1_STC_NOINTERFACESREGISTERED
```

The messages above indicate that no (IPV6) interface is registered. This can also result in TCP/IP service initialization failure for the IBM Tivoli Monitoring address space. The absence of an interface can only be fixed by the z/OS TCP/IP administrator.

The First SEND

This section provides information about confirming whether or not First SEND was successful as well as how to repair failures in the First SEND.

Confirming that he First SEND was successful: The sequence of the following communication messages indicate the first SEND operation (an lb__lookup RPC request) and the first RECEIVE operation:

```
 "KDCR0_Send") request FFFF/0.0 (200): ip.pipe:#9.42.46.26[1918]
 "KDCR0_InboundPacket") response FFFE/0.0 (320): ip.pipe:#9.42.46.26[1918]
 "KDCL_GetBinding") Using LLB at ip.pipe:#9.42.46.26[1918]
```

When the first network I/O is successful, the response indicates link and transport connectivity with the hub computer.

Repairing the failures in the First SEND: There are two consideration specific to OS/390 and z/OS platforms:

- RACF permission to the started task for the OMVS segment
- Presence of the well known port on the TCP/IP Port List.

The RACF permission problem might not be detected until the failure of the first network I/O. The "KDCR0_Send" request fails with **Errno 2**: EACCESS. This failure can occur with the first use of the started task name.

A similar problem results in EACCESS: the well-known port is defined on the TCP/IP port list. ISPF Option 6, "netstat portlist" confirms the presence of the well-known port in the TCP/IP reserved port list. The well-known port should not be on this list.

SNA service initialization

IBM Tivoli Monitoring Address Spaces can configure be configured to use SNA exclusively, or in conjunction with TCP/IP, as a transport service. This configuration is done in the environment member (xxxENV) of RKANPAR. If SNA services are viewed as optional, then removal of KDCFC_ALIAS, KDCFC_MODE, and KDCFC_TPNAME from the xxxENV member of RKANPAR will effectively disable use of SNA.

Initializing the SNA: The following messages are printed in the RAS1/ RKLVLOG when the local SNA configuration is processed from the XXXENV member of RKANPAR:

```
 kbbssge.c,52,"BSS1_GetEnv") KDCFP_ALIAS=KDCFC_ALIAS=KLXBS_ALIAS="ASIAGLB"
 kbbssge.c,52,"BSS1_GetEnv") KDCFP_TPNAME=KDCFC_TPNAME=KLXBS_TPNAME="SNASOCKETS"
 kbbssge.c,52,"BSS1_GetEnv") KDCFP_MODE=KDCFC_MODE=KLXBS_MODE="CANCTDCS"
 kdes1rp.c,140,"getEnv") AF_SNA configuration: Alias(ASIAGLB) Mode(CANCTDCS)
TpName(SNASOCKETS)
```

KDCFC_ALIAS identifies the APPL definition of the Independent Logical Unit to be used in this process. KDCFC_MODE identifies the LOGMODE name, the same name found in the LOGMODE specification of the KDCFC_Alias APPL definition. KDCFC_TPNAME is the Transaction Processing Name. The message which indicates the LOCALLU is operational (the configuration is good) is the "transport opened" message:

```
kde1otp.c,118,"KDE1I_OpenTransportProvider") Transport opened: com1/sna.pipe
```

Repairing SNA initialization failures: There following lists the reasons for SNA initialization failures:

- The ILU configured for use is not available to the application. The ACBNAME (or APPLNAME) is properly defined in SYS1.VTAMLST but not in the connectable state (CONCT). The ACB must be varied ACTIVE to NET prior to Omegamon Platform Address Space startup. The MVS command to verify the state of the ACB is "D NET, ID=acbname,E" .
- The ILU is available but not a valid LU6.2 definition. In this case, the is a **KBBCM001** message with an SNA sense code found in the `RAS1/RKLVLOG`. Diagnose the 8-byte SNA sense code (typically, 087Dnnnn) using the "SNA Formats and Protocol" manual.
- The LOGMODE is not a valid LU6.2 LOGMODE, or the LOGMODE and MODETAB specification associated with the ILU definition are not the same, by name, on both systems hosting the endpoints. This is most likely the case for SNA session establishment hangs. The message in the RKLVLOG is "Receive XID pending: NULL", and it is followed by another RPC timeout message.

The Server list

IBM Tivoli Monitoring processes build and query a list of possible Tivoli Enterprise Monitoring Server hub addresses, called the Server list. This server list contains local (LLB) and global (GLB) entries. The LLB entries of the Server list are derived. The GLB entries of the Server list are built from the content of the KDCSSITE member of RKANPAR. Shown below are two server lists. The first Server List is for a Tivoli Enterprise Monitoring Server hub, the second Server List is for a remote Tivoli Enterprise Monitoring Server. See the following example:

```
(Server list for a HUB CMS)
LLB entry 1 is ip:#10.248.16.1.1918.
LLB entry 2 is sna:#ATOOEN01.K10DSLB.CANCTDCS.SNASOCKETS.135.
GLB entry 1 is ip:#10.248.16.1.1918.
GLB entry 2 is sna:#ATOOEN01.K10DSLB.CANCTDCS.SNASOCKETS.135.
GLB entry 3 is ip:#10.248.16.1.1918.
GLB entry 4 is sna:#ATOOEN01.K10DSLB.CANCTDCS.SNASOCKETS.135.
(Server list for a REMOTE CMS)
LLB entry 1 is ip:#10.248.17.2.1918.
LLB entry 2 is sna:#ATOOEN01.K20DSLB.CANCTDCS.SNASOCKETS.135.
GLB entry 1 is ip:#10.248.16.1.1918.
GLB entry 2 is sna:#ATOOEN01.K10DSDS.CANCTDCS.SNASOCKETS.135.
GLB entry 3 is ip:#10.248.17.2.1918.
GLB entry 4 is sna:#ATOOEN01.K20DSLB.CANCTDCS.SNASOCKETS.135.
```

Confirming the Server list is correct: In general, the first half of the GLB server list always points to the Tivoli Enterprise Monitoring Server hub. The first half of the GLB entries in the Server list are taken from member KDCSSITE of RKANPAR. If the LLB entries are derived (implicitly) and the GLB entries are explicitly configured in the KDCSSITE member, you can diagnose and repair the errors in KDCSSITE.

- The number of LLB entries must be half the number of GLB entries. If this is not the case, then there might be a mismatch between the number of transports services configured to this Tivoli Enterprise Monitoring Server (the

KDC_FAMILIES environment variable) versus the number of transports configured for the hub Tivoli Enterprise Monitoring Server (KDCSSITE).

- For a hub Tivoli Enterprise Monitoring Server, each LLB entry must be identical to the corresponding GLB entry in the Server list. As in the Server list for a hub Tivoli Enterprise Monitoring Server example, LLB entry 1 is the same as GLB entry 1 and LLB entry 2 is the same as GLB entry 2.
- For a remote Tivoli Enterprise Monitoring Server, the opposite is true: each LLB entry must be different than the corresponding GLB entry in the Server list. As in the example (Server list for a REMOTE Tivoli Enterprise Monitoring Server), LLB entry 1 is different than GLB entry 1, LLB entry 2 is different than GLB entry 2.

Repairing errors in the Server list: Errors in SNA initialization might be name mismatches. Examine the LLB entries and the GLB entries for the Omegamon Platform address space for typographical errors. The VTAM® network ID is victim of frequent error. Typically the VTAM network ID (the first component of the SNA socket address, ATOOEN01 in the example above) is the same for ALL entries. While it CAN differ, typically, it does not. A difference between the LLB VTAM net ID and the GLB VTAM net ID is often an error in member KDCSSITE of RKANPAR.

Local Location Broker service initialization

An intrinsic part of Remote Procedure Call architecture is the location broker. RPC servers (callers of rpc__listen) publish their service and the address of this service in a location broker. RPC clients (callers of rpc__sar) use the location broker to obtain the address of a server prior to making a call to that server. Use of the location broker is well-defined by the lb__lookup() Remote Procedure Call. It is also appropriate to mention that there are two types of location brokers: the local location broker (LLB) and the global location broker (GLB). There is one local location broker for every RPC server (The Tivoli Enterprise Monitoring Server has it's own LLB. The monitoring agent, the Warehouse Proxy agent, and the Tivoli Enterprise Portal Server all have their own instance of a LLB.) RPC servers, by definition, publish the service offered and address of this service in their local location broker.

Confirming the Local Location Broker service initialized: The bind messages in the RKLVLOG indicate the success or failure of the LLB service initialization. One of two message IDs prefix the LLB status messages, depending on how the LLB service was started. **KDSNC007** is the message prefix issued on successful LLB process initialization when the LLB is started internally by the Tivoli Enterprise Monitoring Server.

```
 KDSNC004  Bind of local location broker complete= ip.pipe:#9.42.46.26.21343.
 KDSNC004  Bind of local location broker complete= ip:#9.42.46.26.21343.
 KDSNC004  Bind of local location broker complete= sna:
(USCACO01.VWCTHLB.CANCTDCS.SNASOCKETS).135.
 KDSNC007  Local Location Broker is active
```

Repairing errors in Local Location Broker service initialization: Bind failures due to insufficient authorization are reported with **Errno. 2** (EACCESS)o the Local Location Broker (as the name LOCAL implies) is done with a local socket address. The bind fails for the following reasons:

- Insufficient authorization
- The address is unavailable

```
 (32645848-E8E45647:kdebnws.c,64,"KDEB_NewSocket")
Status 1DE00000=KDE1_STC_CANTBIND.
 (3265B3F0-E8E45647:kdebnws.c,84,"KDEB_NewSocket")
```

```
<0x176A97D4,0x10> BSD bind details:
Family 2, Socket 0, Status 1DE00000, Errno 2.
    00000000   00022EE1 00000000  00000000 00000000   ................
 (326B1EA8-E8E45647:kdcsuse.c,98,"KDCS_UseFamily") status=1c010005,
"cant bind socket",
 ncs/KDC1_STC_CANT_BIND
 2001.252 04:42:41 KDC00008 Unable to create location server, status 1C010005
```

Bind failures due to address-in-use:

```
 (3ACDB600-DEB3B73F:kdebnws.c,62,"KDEB_NewSocket") Status 1DE00030=KDE1_STC_
ENDPOINTINUSE
 (3ACF5028-DEB3B73F:kdcsuse.c,99,"KDCS_UseFamily") status=1c010005, "cant bind
socket", ncs/KDC1_STC_CANT_BIND
```

Bind failure due to address-in-use but not fatal:

```
 (1CF7B1F8-E6D9D743:kdcsuse.c,99,"KDCS_UseFamily") status=1c010005, "cant bind
socket", ncs/KDC1_STC_CANT_BIND
 KDSNC007   Local Location Broker is active
```

If the bind failure is due to EADDRINUSE but the Broker service is started, the error might not be fatal. Determine whether or not the bind of this IBM Tivoli Monitoring address space was to the LLB in that address space. In some instances, an address space can bind to the LLB of another address space. This can only occur in the same system image. If the bind failure is fatal, then another process on this system image has the 'well-known' port. Bind failures due to insufficient authorization are fixed by granting RACF permission for the OMVS segment to the Omegamon Platform started task name.

Global Location Broker service initialization

The Global Location Broker (GLB) differs from the Local Location Brokers in one important respect other than the name: there is only one GLB for the domain or enterprise. By definition, there will be only one Local Location Broker which points to the Global Location Broker for the domain. The RPC server LLB which points to the GLB (and there will be only one of these in an enterprise) is, by definition, the hub. The important thing to remember from all this discussion of local and global brokers is this: For a process to locate the Tivoli Enterprise Monitoring Server hub, the process must query (issue lb__lookup() RPC requests to) the list of candidate Global Location Brokers in order as specified in the global site text file (`glb_site.txt` on distributed platforms and the KDCSSITE member of RKANPAR for OS/390 and z/OS platforms). Below are the product communication messages which enumerate the candidate GLB list (GLB entry 1, GLB entry 2, etc):

```
 GLB entry 1 is ip.pipe:#9.42.46.26.21343.
 GLB entry 2 is ip:#9.42.46.26.21343.
 GLB entry 3 is sna:(USCACO01.VWCTHLB.CANCTDCS.SNASOCKETS).135.
 GLB entry 4 is ip.pipe:#9.42.46.26.21343.
 GLB entry 5 is ip:#9.42.46.26.21343.
 GLB entry 6 is sna:(USCACO01.VWCTHLB.CANCTDCS.SNASOCKETS).135.
```

Connectivity between the Omegamon/XE and Tivoli Enterprise Monitoring Server address space fails if this list is incorrect. The GLB entries display in the order in which they are configured in the global site text file. Additionally, the address of the local platform is appended to this list. This is an RPC architecture requirement. It allows the local platform to be queried when the GLB list has been exhausted and no hub is found.

Confirming the Global Location Broker service initialized: The bind messages in the RKLVLOG indicate the success or failure of the GLB service initialization. A message ID prefixes the GLB status messages and indicates how the GLB service

was started. **KDSNC008** is the message prefix issued on successful GLB process initialization when the LLB is started internally by the Tivoli Enterprise Monitoring Server.

```
 Bind of global location broker complete= ip.pipe:#9.42.46.26.21343.
 Bind of global location broker complete= ip:#9.42.46.26.21343.
 Bind of global location broker complete= sna:
(USCACO01.VWCTHLB.CANCTDCS.SNASOCKETS).135.
 Global Location Broker is active
```

Repairing errors in Global Location Broker service initialization: GLB service failures occur because there are errors in member KDCSSITE of RKANPAR. Each socket address in KDCSSITE is assumed to be the socket address of the Tivoli Enterprise Monitoring Server hub. If none of the entries in the `KDCSSITE` file are the correct socket address of the Tivoli Enterprise Monitoring Server hub, this process initialization fails.

Tivoli Enterprise Monitoring Server hub availability

The following message indicates the Tivoli Enterprise Monitoring Server hub is available:

```
ko4locbr.cpp,731,"Mgr::locateEverbody") lbLookupHub returned error <0>,
                                         ip<ip:#9.42.46.26.21343>
                                         sna<> pipe <ip.pipe:#9.42.46.26.21343.>
```

Do the following if the Tivoli Enterprise Monitoring Server hub is not available:

- Review the RAS1 log for the Tivoli Enterprise Monitoring Server to ensure it is connected.
- Review network topology to ensure Firewall policy does not prohibit connection initiation from the Tivoli Enterprise Monitoring Server hub.
- Review "Transport opened" on the Tivoli Enterprise Monitoring Server to ensure at least one transport service is common between it and this Tivoli Enterprise Monitoring address space.

z/OS-based installations problems and resolutions

This section describes problems that might occur with a z/OS-based installation.

How do you customize the following Tivoli Enterprise Monitoring Server configuration values using the Configuration tool?

You can increase the following storage-related parameters if IBM Software Support personnel instructs you to do so:

- Web Services SOAP Server
- startup console messages
- communications trace
- storage detail logging and associated intervals
- minimum extended storage
- primary and extended maximum storage request size
- language locale
- persistent datastore parameters

Use the following steps to increase the storage-related parameters:

1. From the **Configure the Tivoli Enterprise Monitoring Server** main menu, select the **Specify configuration values** option.
2. On the next panel, press **F5=Advanced** to open the **Specify Advanced Configuration Values** panel. The next panel includes the following options:

- Enable OMEGAMON SOAP Server (applicable to a Hub Tivoli Enterprise Monitoring Server only)
- Enable startup console messages
- Enable communications trace
- Enable storage detail logging and associated intervals
- Specify the Virtual IP Address (VIPA) type
- Specify the minimum extended storage
- Specify the primary and extended maximum storage request size
- Specify the language locale for globalization
- Specify the persistent datastore parameters

3. Customize the fields with the preferred values in the **Specify Advanced Configuration Values**.
4. Select the **Create runtime members** option to regenerate the "DS#3xxxx Create runtime members" job from the **Configure the Tivoli Enterprise Monitoring Server** main menu.
5. Submit the job and check for good condition codes.
6. Recycle the Tivoli Enterprise Monitoring Server.

'DATA SET NOT FOUND' JCL error occurs when submitting the DS#3xxxx Tivoli Enterprise Monitoring Server 'Create runtime members' job.

Ensure the following:

- The pp#1xxxx RTE Build job successfully ran for this RTE. To perform the RTE Build job,
  1. Place the **B** option next to the RTE on the KCIPRTE RTE main menu to instruct Configuration tool generates the pp#1xxxx mRTE Build job.
  2. Ensure that the RTE Build job contains allocations for the &rvhilev.&rte.RKDS* and &rvhilev.&rte.RK* runtime libraries.
  3. Submit the RTE Build job.
- The **Tivoli Enterprise Monitoring Server in this RTE** field is set to **Y** on the RTE Update panel if the RTE Build job does not contain &rvhilev.&rte.RKDS* libraries. If you must edit the field, regenerate the RTE Build job.

Refer to the *IBM Tivoli Monitoring Installation and Setup Guide* manual for more information about configuring a z/OS Tivoli Enterprise Monitoring Server and the RTE Build job.

The error 'CMSLIST NOT ALLOWED' occurs on the 'Specify Advanced Configuration Values' panel when Tivoli Enterprise Monitoring Server type equals hub.

The F10=CMSLIST key from the **Specify Advanced Configuration Values** panel is only applicable to a remote Tivoli Enterprise Monitoring Server. This PF Key allows the remote Tivoli Enterprise Monitoring Server to select a hub Tivoli Enterprise Monitoring Server to which it can connect. The F10=CMSLIST function key is unavailable to a hub Tivoli Enterprise Monitoring Server. Go to the previous **Specify Configuration Values** panel to verify what type of Tivoli Enterprise Monitoring Server you are configuring

The 'Enter required field' error occurs for the 'Global location broker applid of Hub' or the 'Network ID of Hub' VTAM-related fields

On the **Specify Configuration - Hub Values for Remote Tivoli Enterprise Monitoring Server** panel, the message "Enter required field" occurs although the remote z/OS Tivoli Enterprise Monitoring Server connects to the Hub Tivoli Enterprise Monitoring Server through IP protocols. If you are configuring a remote z/OS-based Tivoli Enterprise Monitoring Server that connects to a non-z/OS Hub Tivoli Enterprise Monitoring Server via the IP or IPPIPE communication protocol, use the following steps as a resolution:

1. On the **Specify Configuration - Hub Values for Remote Tivoli Enterprise Monitoring Server** panel, enter any value in the following fields:
   - **Global location broker applid of Hub**. For example, enter default "CTDDSLB" if this VTAM APPLID is not used.
   - **Network ID of Hub**. For example, enter the NETID value from SYS1.VTAMLST(ATCSTRnn)).

   Note: Neither of these values adversely affect the connection for the remote Tivoli Enterprise Monitoring Server.
2. From the **Configure the Tivoli Enterprise Monitoring Server** main menu, select the **Specify communication protocols** option.
3. On the **Specify communication protocols** panel, specify the IP protocols of choice and ensure. Specify **SNA.PIPE** as one of the protocols that the remote Tivoli Enterprise Monitoring Server uses for connection.
4. Navigate forward to specify the communication protocols values for the selected protocols.
5. From the **Configure the Tivoli Enterprise Monitoring Server** main menu, select the **Create runtime members** option to generate the DS#3xxxx Create runtime members job.
6. Submit the job and check for good condition codes.
7. From the **Configure the Tivoli Enterprise Monitoring Server** main menu, select the **Complete the configuration** option.
8. Review the remaining tasks to finish the configuration of the product before starting the Tivoli Enterprise Monitoring Server.

The pp#Mxxxx Tivoli Enterprise Monitoring Server migration job generated by the Configuration tool ended with a condition code=08.

The JCL used to upgrade an existing RTE to IBM Tivoli Monitoring v6.1 level must perform several steps to ensure the existing data is not lost nor corrupted. The batch job stops processing data in the event of an error, such as insufficient DASD. The batch job is not submitted a second time but three batch job are created that can be used to restore the data to its original state. Therefore, the upgrade JCL can be submitted to run and start from the beginning to allow for conditions that initially caused the problem to be corrected. Based on what step was running when the failure occurred, you might need to run one or more of the following jobs in RKANSAM:

- KDSRSTRO
- KDSRSTRN
- KDSRSTRV

Use the following VSAM migration steps:

1. Run RNMEVSAM/ALLCVSAM step to:
   - Rename the previous version's VSAM file to a backup VSAM name.
   - Allocate the new V610 VSAM file based on the new format.

   Note: This step applies to VSAM files containing data that do not need to be converted.

   –OR–Edit and submit KDSRSTRN to restore to files to the original state.
2. Run KDSRCONV step to:
   - Allocate the new V610 VSAM libraries using temporary XKDS* VSAM names.
   - REPRO the previous version VSAM file data (RKDS*) to flat file.
   - Convert the fields to ASCII and resize columns accordingly. REPRO the converted flat file to the new XKDS* VSAM libraries.
   - Write out the output from the conversion.

   –OR–Edit and submit KDSRSTRV to restore a file to original state.
3. Run RNMEEIBO step to rename the previous version's VSAM files (RKDS*) to backup VSAM names (BKDS*) if the KDSRCONV step is successful.

   –OR–Edit and submit KDSRSTRO to restore file to original state.
4. Run RNMEEIBN step to rename the new V610 XKDS* VSAM libraries to the runtime RKDS* VSAM names if the RNMEEIBO step is successful.

   –OR–Edit and submit KDSRSTRN to restore to original state.

   Note: By default the restore jobs runs against all of the processed datasets. The comments section of these jobs detail that some of the datasets can be commented out depending on the time and nature of the failure experienced. For instance, only 4 of 7 datasets were renamed during RNEVSAM, so only those 4 must be restored to their original names. If you are not certain which job to run or what datasets to comment out in these jobs, contact IBM Software Support.

The Tivoli Enterprise Monitoring Server starts normally in a system without the Integrated Cryptographic Service Facility but does not connect to the Tivoli Enterprise Portal Server

Although Integrated Cryptographic Service Facility (ICSF) provides robust password encryption, you are not required to use it as it can affect compatibility with the z/OS OMEGAMON monitoring products. Perform the following steps so that the Tivoli Enterprise Portal Server can connect to the Tivoli Enterprise Monitoring Server:

- During configuration:
  1. Select **Configure the Tivoli Enterprise Monitoring Server** > **Specify configuration values** > **Integrated Cryptographic Service Facility (ICSF) installed?**
  2. Specify **N** in the on the **Integrated Cryptographic Service Facility (ICSF) installed?** panel.
- After the Tivoli Enterprise Monitoring Server configuration is complete and it is running:
  1. The Tivoli Enterprise Portal Server configuration must be modified to use an older, less robust encoding algorithm. Edit the `kfwenf` file in *`install_dir`*`\CNPS`, where *install_dir* is `C:\IBM\ITM` by default in a text editor.
  2. In a line by itself, type the text USE_EGG1_FLAG=1
  3. Save the document and exit.

4. Stop the Tivoli Enterprise Portal Server, if it is running, then start it.

On a system with one or more existing OMEGAMON monitoring environments, the global CSI is corrupt and cannot be used for installing a new version

Use the following steps manually merge existing datasets with IBM Tivoli Monitoring V6.1 datasets only after IBM Software Support instructs you to do so:

1. Backup the following datasets:
   - Runtime
   - Target
   - INSTDATA
   - INSTDATW
   - INSTJOBS
   - INSTLIB
   - INSTLIBW
   - INSTQLCK
   - INSTSTAT

   Note: You must backup the specified datasets.
2. After installing the product on a new CSI, refer to the Program Directory document to verify that the datasets contain enough allocated space for the new libraries.
3. From the ISPF panel 3.3 or a JCL batch job, copy the contents of the new modified Target libraries in Table 30 to their counterparts in the old Target libraries, ensuring that like-named members are replaced.

Table 30. Modified target libraries

TKANCMD
TKANCUS
TKANDATV
TKANHENU
TKANMAC
TKANMOD
TKANMODL
TKANPAR
TKANPENU
TKANSAM
TKCIINST
TKNSLOCL

4. Manually delete obsolete datasets listed in Table 31 from TKANMODL that interfere with operation of new version of Tivoli Enterprise Monitoring Server on z/OS.

Table 31. TKANMODL obsolete members

KLXABIND
KLXACLOS
KLXAHBAD

Table 31. TKANMODL obsolete members (continued)

KLXAHBNM
KLXAINIT
KLXAINTE
KLXAOPEN
KLXAPEER
KLXARECV
KLXASELF
KLXASEND
KLXASLIH
KLXAWAIT
KLXAXDAT
KLXAXTPL
KLXI@INT
KLXI@IUC
KLXIDESP

Where Remote Deployment of agents is not supported

Remote Deployment is not supported for OMEGAMON agents. It is also not supported in environments with a z/OS Tivoli Enterprise Monitoring Server.

Uninstallation problems and workarounds

This section provides information about how to troubleshoot an uninstallation.

Unable to uninstall multi-instance agent from a managed system on windows 64bit

When uninstalling a multi-instance agent from a managed system that also has an IBM Tivoli Monitoring v622 Fix Pack 2 agent installed, instances are not uninstalled, leaving an entry in the MTEMS. This only occurs on the Windows 64-Bit platform. Other IBM Tivoli Monitoring components running on the system continue to operate normally.

Remove the agent instances first and then uninstall the agent. If the agent was already uninstalled, you can re-install the agent again, remove the instances, and then uninstall the agent again.

Prompted for .msi file during uninstallation process started from 'Add/Remove Programs' on systems with v6.2.2 installed

Press cancel, and enter the path to the .msi file on the original installation image from which the feature was installed. You can also cancel the entire uninstallation process and start the installer from the original image and continue the uninstallation process, as you were doing, from 'Add/Remove Programs.'

If the original installation image is not available:

1. Cancel the current uninstallation process.

2. Move the temporary INSTALL.ver and INSTALLX.ver files from the *CANDLE_HOME*\InstallITM\ver directory to a safe location and start the uninstallation process again.
3. When the feature is successfully removed, restore the INSTALL.ver and INSTALLX.ver files back to the *CANDLE_HOME*\InstallITM\ver directory.

Uninstallation is blocked by another process that is using the IBM Tivoli Monitoring eclipse help server

Kill the javaw tasks associated with the IBM Tivoli Monitoring eclipse help server on the system so that the uninstall can continue.

Uninstallation of an agent produces help errors

After uninstalling an IBM Tivoli Monitoring v6.1.1 agent and its application support files, the IBM Tivoli Monitoring Online (F1) Help produces an error when selected. The browser displays "The page cannot be displayed" with a URL of http://host:9999/help/index.jsp. To solve this problem complete the following steps:

- Stop the Eclipse Help Server and the Tivoli Enterprise Portal Server.
- Open a DOS Prompt, then navigate to the HOME\CNB\classes\candle directory.
- Run the helpmerg.bat file.
- Start the Eclipse Help Server.
- Start the Tivoli Enterprise Portal Server.

Note: The Tivoli Enterprise Portal Server might not have to be stopped and started for this procedure.

Uninstallation of an agent occurring more than once stops the OS agent

If uninstallation an agent is performed more than once, it stops the Monitoring Agent for Windows OS agent as well as other IBM Tivoli Monitoring components. Also, an error message does not appear in the console.

After uninstallation, Tivoli Enterprise Monitoring Server folder is not deleted

There is no negative impact from these files being left on the system.

Removing a failed installation on Windows

The following sections describe the process for removing a release that is partially installed and cannot be removed by using the Add and Remove Programs tool. The following topics are discussed:

Table 32. Removing a failed installation on Windows

Goal	Where to find information
Remove a failed installation from computer that has never had IBM Tivoli Monitoring or Candle OMEGAMON installed.	“Removing a failed first time installation” on page 109
Remove a failed installation from a computer that you were trying to upgrade from Candle OMEGAMON.	“Removing a failed upgrade” on page 109

Removing a failed first time installation

Use the following steps to remove a partially installed IBM Tivoli Monitoring installation:

1. Ensure that there is no entry in the Add and Remove Programs tool for the component that you attempted to install. If there is an entry, use that entry to uninstall the product. If there is no entry, proceed to the next step.
2. Open the Windows Explorer and navigate to the IBM Tivoli Monitoring installation directory (`C:\IBM\ITM` by default).
3. Launch the Manage Tivoli Enterprise Monitoring Services utility by double-clicking the `KinConfg.exe` file located in either the `Install` or `InstallITM` subdirectory.
4. If any agents, the portal server, or the monitoring server are listed in the Manage Tivoli Enterprise Monitoring Services window, right-click each and click **Advanced > Unconfigure**. Repeat this step for all components that are listed. Close the Manage Tivoli Enterprise Monitoring Services utility.
5. Open the Windows Control Panel.
6. Double-click **Administrative Tools** and then double-click **Services**.
7. Verify that all related IBM Tivoli Monitoring services have been removed. These services match those listed in the Manage Tivoli Enterprise Monitoring Services window.
8. Open the Registry Editor by clicking **Start → Run** and typing `regedt32`. Click **OK**.

   Note: Create a backup of the registry before editing it.
9. Expand the key HKEY_LOCAL_MACHINE registry key.
10. Expand the SOFTWARE registry key.
11. Expand the Candle registry key and record any sub-keys that are present. If the Candle key does not exist, proceed to step 15.
12. Expand the OMEGAMON registry key under the Candle key and record the content of the OMEGAMON key values.
13. Delete the Candle registry key and all sub-keys.

    On Windows XP, you can right-click the Candle registry key and click **Delete**.
14. Close the Registry Editor.
15. Open the Windows Explorer and find the IBM Tivoli Monitoring installation location on your system. The default value is `C:\IBM\ITM`.
16. Delete this directory and all subdirectories.
17. Remove the IBM Tivoli Monitoring bookmark from the Start menu:
    a. Click **Start** from the Windows desktop to display the Start menu items.
    b. Click **Programs**.
    c. Right-click IBM Tivoli Monitoring to display the bookmark menu options.
    d. Click **Delete** to remove the IBM Tivoli Monitoring bookmark from the Windows desktop start menu.

You can now install IBM Tivoli Monitoring.

Removing a failed upgrade

To remove a failed upgrade, first ensure that there is no entry in the Add and Remove Programs tool for the new component you are attempting to install. If there is an entry, use that entry to uninstall the product. If there is no entry, use the following steps to remove the failed upgrade.

The first step to removing a failed upgrade is to determine where the install failed: either before the files were copied or after the files were copied. For GUI installations, the files are copied after you click **Next** on the Start Copying Files window. If you performed a silent installation, look for a pair of entries separated by a blank line:

```
FirstUIBefore exiting to file copy
FirstUIAfter entry after file copy
```

If neither exist, then the installation failed before the files were copied. See "Installation failed before files were copied."

If both entries exist, the installation failed after the files were copied. See "Installation failed after files were copied"

Installation failed before files were copied: Check to see if the entry for your previous installation exists in the Add and Remove Programs tool. If it does not exist, follow the instructions in "Removing a failed first time installation" on page 109. Your previous installation is too corrupt to use and must be completely removed. You must either completely reinstall the previous release and then upgrade to IBM Tivoli Monitoring or just install IBM Tivoli Monitoring without attempting to upgrade.

If the entry exists in the Add and Remove Programs tool, you can still use your existing Candle OMEGAMON installation. Launch Manage Candle Services to start all components.

Installation failed after files were copied: If your installation failed after the files were copied, your current installation has been corrupted by the partial installation of IBM Tivoli Monitoring. You must either completely reinstall the previous release and then upgrade to IBM Tivoli Monitoring or just install IBM Tivoli Monitoring without attempting to upgrade.

Check the Add and Remove Programs tool to see if either your previously installed Candle OMEGAMON or IBM Tivoli Monitoring is available.

If neither are available, see "Neither products are available in the Add and Remove Programs tool."

If one is available see "One product is available in the Add and Remove Programs tool" on page 111.

If both are available, "Both products are available in the Add and Remove Programs tool" on page 112.

Neither products are available in the Add and Remove Programs tool: Use the following steps if neither Candle OMEGAMON or IBM Tivoli Monitoring exists in the Add and Remove Programs tool:

1. Open the Windows Explorer and navigate to the IBM Tivoli Monitoring installation directory. By default, the installation location is `C:\IBM\ITM\Install`, `C:\IBM\ITM\InstallITM`, `C:\Candle\Install`, or `C:\Candle\InstallITM`.
2. Launch the Manage Tivoli Enterprise Monitoring Services utility by double-clicking the `KinConfg.exe` file located in either the `Install` or `InstallITM` subdirectory. Launch the `KinConfg.exe` from the `InstallITM` directory if possible.

3. If any agents, the portal server, or the monitoring server are listed in the Manage Tivoli Enterprise Monitoring Services window, right-click each and click **Advanced > Unconfigure**. Repeat this step for all components that are listed. Close the Manage Tivoli Enterprise Monitoring Services utility.
4. Open the Windows Control Panel.
5. Double-click **Administrative Tools** and then double-click **Services**.
6. Verify that all related Candle OMEGAMON and IBM Tivoli Monitoring services have been removed. These services match those listed in the Manage Tivoli Enterprise Monitoring Services window.
7. Open the Registry Editor by clicking **Start → Run** and typing `regedt32`. Click **OK**.

   Note: Create a backup of the registry before editing it.
8. Expand the key HKEY_LOCAL_MACHINE registry key.
9. Expand the SOFTWARE registry key.
10. Expand the Candle registry key and record any sub-keys that are present. If the Candle key does not exist, proceed to step 14.
11. Expand the OMEGAMON registry key under the Candle key and record the content of the OMEGAMON key values.
12. Delete the Candle registry key and all sub-keys.

    On Windows XP, you can right-click the Candle registry key and click **Delete**.
13. Close the Registry Editor.
14. Open the Windows Explorer and find the Candle OMEGAMON and IBM Tivoli Monitoring installation directories. The default value for Candle OMEGAMON is C:\Candle; the default value for IBM Tivoli Monitoring is C:\IBM\ITM.
15. Delete this directory and all subdirectories.
16. Use the steps in "Verifying the uninstallation" on page 112 to verify that you successfully removed the failed upgrade.
17. Remove the IBM Tivoli Monitoring bookmark from the Start menu:
    a. Click **Start** from the Windows desktop to display the Start menu items.
    b. Click **Programs**.
    c. Right-click IBM Tivoli Monitoring to display the bookmark menu options.
    d. Click **Delete** to remove the IBM Tivoli Monitoring bookmark from the Windows desktop start menu.

One product is available in the Add and Remove Programs tool: Use the following steps if an entry for either Candle OMEGAMON or IBM Tivoli Monitoring exists in the Add and Remove Programs tool:

1. Attempt to uninstall both releases from the Add and Remove Programs entry.
2. If this is successful, proceed to "Verifying the uninstallation" on page 112.
3. If this is not successful and the entry has been removed from the Add and Remove Programs tool, see "Neither products are available in the Add and Remove Programs tool" on page 110.
4. If the entry is still present in the Add and Remove Programs tool, copy the `KINWIINS.VER` file (from the `\WINDOWS\VERFILES\KINWIINS.VER` directory on the installation CD) to the *<itm_installdir>*`\Install\Ver` directory, where *<itm_installdir>* is the IBM Tivoli Monitoring installation directory.

   Delete the `KINWIINSMSTR.VER` file from this directory if it exists.

Note: You might need to create the `Install\Ver` subdirectory if it is does not exist.

5. Attempt to uninstall the release again. If it fails again, contact IBM Software Support for assistance. See Chapter 2, "Collecting and reviewing troubleshooting data," on page 5 for information on what types of data to collect before contacting Support.

Both products are available in the Add and Remove Programs tool: Use the following steps if both the Candle OMEGAMON or IBM Tivoli Monitoring entries exist in the Add and Remove Programs tool:

1. Uninstall IBM Tivoli Monitoring through the Add and Remove Programs tool.
2. Uninstall Candle OMEGAMON through the Add and Remove Programs tool.
3. Proceed to "Verifying the uninstallation."

Verifying the uninstallation: Use the following steps to verify that you successfully removed the failed installation:

1. Verify that the installation home directory and all contents have been removed.
2. Open the Registry Editor by clicking **Start → Run** and typing `regedt32`. Click **OK**.
3. Expand the key HKEY_LOCAL_MACHINE registry key.
4. Expand the SOFTWARE registry key.
5. Verify that the Candle registry key and all sub-keys have been removed from HKEY_LOCAL_MACHINE\SOFTWARE.

You are now ready to install IBM Tivoli Monitoring.

Incorrect behavior after an uninstallation and reinstallation

You might experience incorrect behavior if you uninstall then reinstall the product without restarting the system. For example, you might experience the following problems:

- Inability to create trace logs.
- Agents do not start.
- Agents data is corrupt.

Restart the system to resolve the problems.

Tivoli Data Warehouse database does not uninstall

When you uninstall IBM Tivoli Monitoring, the Tivoli Data Warehouse database is not removed and the ODBC data source exists. You must remove the Tivoli Data Warehouse database and the ODBC manually.

The agent installation log on the endpoint indicates that error AMXUT7512E occurred

The error AMXUT7512E might occur when running the Distributed Monitoring Upgrade Toolkit. The agent was not uninstalled for one of the following reasons:

- There is another uninstallation in progress that cannot complete until the computer is restarted.

  –OR–

- The uninstallation requires stopping a process that is currently in use by a another component.

Refer to the lcfd.log on the endpoint and agent installation log as listed in Table 33 to determine the exact cause of the problem.

Table 33. Installation logs

Windows	UNIX-based systems
install_Dir/Install/Abort IBM Tivoli Monitoring timeStamp.log	*install_Dir*/logs/candle_installation.log

You can manually uninstall the operating system agent by running the command for your platform as listed in Table 34:

Table 34. Uninstall OS command

Windows	UNIX-based systems
LCF_BINDIR\\..\\TME\\ITMUpgrade \\ITMUpgradeManager\\setup.	*LCF_BINDIR*/../TME/ITMUpgrade/ ITMUpgradeManager/uninstall.sh

Contact IBM Software Support if you cannot uninstall the agent. See Chapter 2, "Collecting and reviewing troubleshooting data," on page 5 for information on what types of data to collect before contacting Support.

Prompted to uninstall a database that was not running during uninstallation

During uninstallation, when prompted for the DB2 user name and password in order to remove the Tivoli Enterprise Portal Server from the DB2 database, you were prompted with the following question:

```
would you like to delete the Tivoli Enetrprise Portal MSSQL/MSDE Database
```

The Microsoft MS SQL Server database was not running. My Tivoli Enterprise Portal Server is installed and configured with a DB2 database and not a Microsoft MS SQL Server database.

It is likely that the system you are using at one time had a Microsoft MS SQL Server database installed that was not properly uninstalled. It does not matter whether the database is running or not; if the data source exists you will be asked the question, and if you answer yes there will be an attempt to remove the database.

Chapter 6. Connectivity troubleshooting

This section provides descriptions of and resolutions for problems you might experience with connectivity, including logging in, passwords, and communication among IBM Tivoli Monitoring components. Tivoli Enterprise Portal monitors the connections between server and client and server and host data sources continuously. When Tivoli Enterprise Portal detects a connection error it can repair the error and your client session can resume unaffected. Use the information in this section to diagnose and recover from connectivity problems.

If you are running the Tivoli Enterprise Monitoring Server on z/OS, see "Troubleshooting z/OS-based installations" on page 95 for information about configuration problems affect connectivity.

A monitoring process fails to startup after changing a .profile for root

IBM Tivoli Monitoring processes such as the monitoring server, portal server, warehouse proxy agent, summarization and pruning agent, and other agents are all started while you are logged on as a user ID on Linux and UNIX systems. For many shell environments, the user ID has a `.profile` file that is run during the initial processing to ensure a consistent working environment. The `.profile` must satisfy these requirements:

- During startup, do not start any user interaction when there is not a connected console.
- Ensure that a korn shell [ksh] is available. In general, any shell can be used for `.profile` except csh, which has problems with output redirection.
- Eliminate any logic that can create an error associated with undefined variable evaluation; or use korn file controls to suppress the errors.
- Set the PATH statements to what is needed for the environment.
- Ensure that the `.profile` completes and does not loop.

If any of these requirements are violated, then the results can be failure to start or even failure for normal server processes to start. The `.profile` should be simple and clear. This might require creating a special user ID for this purpose to avoid impacting other users.

The Tivoli Enterprise Portal Server does not start after installation

Check the following log files for messages that indicate why the Tivoli Enterprise Portal Server did not start:

Table 35. The Tivoli Enterprise Portal Server does not start after installation

Log file	For messages that indicate . . .
`kfwras1.log`	A failure during upgrade.
	The Tivoli Enterprise Monitoring Server hub did not connect.
`install_dir\cnps\sqllib\migrate.log`	Any error.

Cannot log in to the Tivoli Enterprise Portal

The following table provides resolutions for problems logging in to the Tivoli Enterprise Portal.

Table 36. Cannot log in to the Tivoli Enterprise Portal

Problem	Corrective action and solution
User authorization failed -OR- `KFWITM215E: Unable to process logon request`	• Ensure the user ID and password are correct. • Verify that the monitoring server has started. • Define the user in the portal server. • Configure the TEPS or TEPS2 data sources. • If security validation is active on the hub monitoring server, make sure the user ID is defined to the security system. For more information on security validation see the *IBM Tivoli Monitoring Installation and Setup Guide* or *OMEGAMON XE and Tivoli Management Services on z/OS: Common Planning and Configuration Guide*.

`KFWITM010I: Tivoli Enterprise Portal Server not ready.`
 	
-OR-
 	
`KFWITM402E: Communication with the Tivoli Enterprise Server could not be established.`
	• Wait for the portal server to establish connection.
	To determine whether or not the portal server is ready for portal client logon, search the portal server trace log for this text string: `Waiting for requests`. If that string is not found, the portal server has not completed initialization. Portal server initialization can take as long as 20 minutes.
	To view the trace log, open Manage Tivoli Monitoring Services, right-click the portal server, and select **Advanced** > **View trace log**.
	• Recycle the portal server.
	
	For more information see "Tivoli Enterprise Portal Server does not start or stops responding" on page 17.

If the status bar displays the Validating User Credentials message continuously, the monitoring server stopped.
 	
-OR-
 	
The message
`TEP has lost communication with TEMS`
displays continuously.
 	
-OR-
 	
`KFWITM008W The Tivoli Enterprise Portal Server has lost contact with the Tivoli Enterprise Monitoring Server.`
	If you are an administrator, restart the monitoring server. Otherwise, notify an administrator and wait for the monitoring server to be restarted.

Table 36. Cannot log in to the Tivoli Enterprise Portal (continued)

Problem	Corrective action and solution
Portal client cannot connect to the portal server because of firewall configuration. -OR- `KFWITM392E: Internal error occurred during logon.`	By default the portal client connects to the portal server on port 1920 or 15001. Open the blocked port or reassign ports accordingly. For environments with multiple interfaces reconfigure the portal server to specify a specific interface by following the instruction below. • On Windows: Use `ipconfig /all` to verify the current network interface configuration. Start the Manage Tivoli Monitoring Services and right-click the TEPS entry, and choose **Advanced** > **Set network interface**. Enter the correct IP address here. • On UNIX or Linux: Use `ifconfig -a` to verify the current network interface configuration. Edit the agent *.ini file and add `KDEB_INTERFACELIST=`*`IP_address`*, where *IP_address* is the correct address. For more information see "Configuring port number assignments for the portal server" in the *IBM Tivoli Monitoring Installation and Setup Guide*.
The portal server cannot initialize because of a DB2 shutdown. -OR- `KFWITM009I: The Tivoli Enterprise Portal Server is still being initialized and is not ready for communications.`	Start DB2 or wait for DB2 to finish initializing. If you receive message `KFWITM009I` you can look at the most recent trace log to verify that the portal server is initialized by searching for the text string `Waiting for requests. Startup completed`.

Table 36. Cannot log in to the Tivoli Enterprise Portal (continued)

Problem	Corrective action and solution
If the Tivoli Enterprise Portal Server connection to LDAP is lost.	When the portal server is configured to authenticate against the LDAP server (with optionally enabled Single Sign-On capability), if you lose the portal server to LDAP connection, this will cause any log in attempt to fail with error code KFWITM393E: "User ID or password is invalid". This authentication failure will be reported for any user, including the default administrative user "sysadmin", and not only for users defined in the LDAP repository. Re-establish the connection to LDAP. As soon as the portal server to LDAP connection is re-established, you can log in to the Tivoli Enterprise Portal. If there is still a problem connecting with LDAP, de-configure LDAP authentication. If the LDAP connection is broken and the normal procedure to switch off LDAP-based authentication does not work, the following steps need to be performed: 1. For AIX® and Linux systems, stop the portal server with the **./itmcmd agent stop cq** command invoked from the installation directory. 2. Run the ./disableLDAPRepository.sh script from *candle_home*/*arch*/iw/scripts, where *arch* is the system architecture, for example "li6263" or "aix533." 3. Reconfigure the portal server and disable LDAP authentication using the **./itmcmd config -A cq** command invoked from the installation directory. 4. Start the portal server with the **./itmcmd agent start cq** command invoked from installation directory. The portal server authentication through the monitoring server is now enabled. 5. If the monitoring server was also configured to use LDAP and the reason for this procedure being applied is LDAP being out of service, ensure you also change the monitoring server configuration to not authenticate through LDAP, following steps from the monitoring server configuration help. 1. For Windows systems, stop the portal server service using the Manage Tivoli Enterprise Monitoring Services application. \ 2. Run the `disableLDAPRepository.bat` script from `candle_home\CNPSJ\scripts`. 3. Reconfigure the portal server using the Manage Tivoli Enterprise Monitoring Services application and disable the "Validate User with LDAP" option. 4. Start the portal server service using the Manage Tivoli Enterprise Monitoring Services application. The portal server authentication through the monitoring server is now enabled. 5. If the monitoring server was also configured to use LDAP and the reason for this procedure being applied is LDAP being out of service, ensure you also change the monitoring server configuration to not authenticate through LDAP, following the steps from the monitoring server configuration help.

Cannot connect to Tivoli Enterprise Portal Server

Before performing any of the following troubleshooting steps, verify that the connection problems are not the result of firewall settings. The following table provides resolutions for problems logging in to the Tivoli Enterprise Portal Server.

Table 37. Cannot connect to Tivoli Enterprise Portal Server

Problem	Resolution
KFWITM001W Unable to connect to Tivoli Enterprise Portal Server KFWITM215E Unable to process logon request	1. Check the `kfw1ras.log` for details if an attempt to log in fails with message KFWITM001W. The `kfw1ras.log` can list any of the following messages that indicate a reason for the failure: • `SQL1224N A database agent could not be started to service a request, or was terminated as a result of a database system shutdown or a force command.` • `SQL1226N The maximum number of client connections are already started. SQLSTATE=57030` Both messages SQL1224N and SQL1226N occur when the Tivoli Enterprise Portal Server attempts to validate the user ID entered in the browser. 2. Restart the database. 3. Attempt the log in again.

Table 37. Cannot connect to Tivoli Enterprise Portal Server (continued)

Problem	Resolution

A remote Tivoli Enterprise Portal client does not connect to a UNIX-based system Tivoli Enterprise Portal Server with the error message:
`KFWITM001W Unable to connect to Tivoli Enterprise Portal Server`
	A remote Tivoli Enterprise Portal client login window does not connect to a Tivoli Enterprise Portal Server hosted on a UNIX-based system, but the following are true:
	• A local Tivoli Enterprise Portal client connects to the Tivoli Enterprise Portal Server.
	• You can ping the Tivoli Enterprise Portal Server computer from the remote computer.
	• A Web browser can remotely connect to http://*host_name*:1920 to get to the service links, assuming the default service port of 1920 was used during installation.
	• A Web browser can remotely connect to http://*host_name*:15200 and see the Tivoli Enterprise Portal Web client initial frame window.
	The hostname might not resolve to the correct IP address on the local Tivoli Enterprise Portal Server host. To confirm that the hostname resolves to the correct IP address, run the following command from the host on which the Tivoli Enterprise Portal Server was installed:
	`ping hostname`
	–OR–
	`ping -s hostname`
	The ping command displays the IP address of the computer it pings. Ensure that the IP address is the same as the one to which the remote Tivoli Enterprise Portal client is attempting to connect. For example, if your Tivoli Enterprise Portal Server is located on a host with the hostname `tepshost`, and the host's `/etc/hosts` file includes an entry similar to the following:
	`127.0.0.1 localhost.localdomain localhost tepshost`
	The localhost must be an IPV4 interface and not IPV6. Running `ping tepshost` displays an IP address of 127.0.0.1, which is the address of the local loopback network interface and the reason a remote computer cannot connect to it. In this case, you must update the `/etc/hosts` file to give `tepshost` its own entry, as in the following example:
	`127.0.0.1 localhost.localdomain localhost`
	`192.168.0.9 tepshost`
	Note: Do not use localhost for 127.0.0.1 and simultaneously for ::1 (which is the IPv6 address).

Tivoli Enterprise Portal client cannot find Tivoli Enterprise Portal Server	1. Select **Start** > **Programs** > **Tivoli Monitoring Services** > **Manage Tivoli Enterprise Monitoring Services**. 2. Check that the Tivoli Enterprise Portal Server service is running and, if not, restart it. 3. If the Tivoli Enterprise Portal Server is started, see the `KFWRAS1.LOG` for any errors reported by the Tivoli Enterprise Portal Server application. When the server starts, an "event ID 1: KFW0001 - Tivoli Enterprise Portal Server (Tivoli Enterprise Portal Server) startup complete" information entry is logged. If you see an error entry, double-click the item to see the description.

Table 37. Cannot connect to Tivoli Enterprise Portal Server (continued)

Problem	Resolution

Cannot connect to the Tivoli Enterprise Portal Server because it stopped.	Do the following to determine if the Tivoli Enterprise Portal Server stopped and restart it:
	1. On the computer where the Tivoli Enterprise Portal Server is installed, select **Start > Programs > IBM Tivoli Monitoring Services > Manage IBM Services.**
	2. Optional: Right-click the Tivoli Enterprise Portal Server entry and select **Change Startup** from the menu.
	3. In the window that opens, select **System Account** and place a check in the **Allow Service to Interact with Desktop** box.
	4. Click **OK** to open a command prompt window when the Tivoli Enterprise Portal Server is started. Internal Tivoli Enterprise Portal Server commands display in the command prompt window.
	5. Verify that the Tivoli Enterprise Portal Server service is started. The Tivoli Enterprise Portal Server is started when the following messages display:
	`KfwServices: <timestamp> KFW1002I Starting Service: 'Configuration v1.0'`
	`KfwServices: <timestamp> KFW1003I Started Service: 'Configuration v1.0'`
	`KfwServices: <timestamp> KFW1002I Starting Service: 'Situation v1.0'`
	`KfwServices: <timestamp> KFW1003I Started Service: 'Situation v1.0'`
	`KfwServices: <timestamp> KFW1002I Starting Service: 'Automation v1.0'`
	`KfwServices: <timestamp> KFW1003I Started Service: 'Automation v1.0'`
	`KfwServices: <timestamp> KFW1002I Starting Service: 'CEV v1.0'`
	`KfwServices: <timestamp> KFW1003I Started Service: 'CEV v1.0'`
	`KfwServices: <timestamp> KFW1002I Starting Service: 'Startup Complete v1.0'`
	`KfwServices: <timestamp> KFW1003I Started Service: 'Startup Complete v1.0'`
	`KfwServices: <timestamp> KFW1020I ********* Waiting for requests. Startup complete *********`
	6. Do one of the following:
	• If it is stopped, start the Tivoli Enterprise Portal Server.
	• If it is started, recycle the Tivoli Enterprise Portal Server.

If you are running the Tivoli Enterprise Portal in browser mode and reaching the Tivoli Enterprise Portal Server across network, the network system might not be able to resolve the host name.	Do the following on the computer where the Tivoli Enterprise Portal Server is installed: 1. In Manage Tivoli Enterprise Monitoring Services, right-click the Tivoli Enterprise Portal – Browser service and select **Reconfigure** from the menu. 2. In the Launch URL field, change host name in http://hostname:1920///cnp/client to the IP address of the Tivoli Enterprise Portal Server to specify the numerical address, for example: http://10.21.2.166:1920///cnp/client. 3. Click **OK**. 4. Start Tivoli Enterprise Portal browser mode using the IP address instead of the host name. 5. If you are still unable to connect, contact IBM Software Support. See Chapter 2, "Collecting and reviewing troubleshooting data," on page 5 for information on what types of data to collect before contacting Support.

Cannot launch the Tivoli Enterprise Portal on an XP computer after installation with the message KFWITM215E

The message `KFWITM215E: Unable to process logon request occurs`. A firewall setting on the client computer prevents the Tivoli Enterprise Portal client from connecting to the Tivoli Enterprise Monitoring Server. Set the IBM JVM (Java launcher) as a trusted program to allow the Tivoli Enterprise Portal client to connect to the Tivoli Enterprise Monitoring Server. You might need to include the IBM Java program in the programs section of your firewall software and include the IP addresses of other Tivoli Monitoring Services components in the access control for the firewall.

Tivoli Enterprise Portal Server is initializing and is not ready for communications

If you attempt to start Tivoli Enterprise Portal just after starting the Tivoli Enterprise Portal Server, the Tivoli Enterprise Portal Server is not ready for requests from the client until initialization and kfwservices.exe, is fully started. The Tivoli Enterprise Portal Server is not ready for requests from the client until its process, `kfwservices.exe` is fully started. Keep the Logon window open and click **OK** after waiting a moment or two.

Tivoli Enterprise Portal Server lost contact with the Tivoli Enterprise Monitoring Server and is attempting to reconnect

This message displays when the Tivoli Enterprise Portal Server lost its connection to the Tivoli Enterprise Monitoring Server, usually because the Tivoli Enterprise Monitoring Server stopped or is recycling. See also KFW_CMW_RECYCLE_DELAY.

DB2 errors during a logon attempt to the Tivoli Enterprise Portal and portal server

You are able to log in but, receive an error message that you cannot open a workspace in the Tivoli Enterprise Portal.

Before completing the steps below, verify with your database administrator that the following bullets below are not the cause of the problem:

- The database manager has not been started on the database server.
- The database manager was stopped.
- The database agent was forced off by the system administrator.
- The database manager has already allocated the maximum number of agents.
- The database agent was terminated due to an abnormal termination of a key database manager process.

If the problem is not due to any of the above, it is most likely that the application is using multiple contexts with local protocol. In this case the number of connections is limited by the number of shared memory segments to which a single process can be attached. For example, on AIX, the limit is ten shared memory segments per process. Do the following to resolve the problem:

1. On the system with the database that you want to connect to, configure the database manager to use TCP/IP on AIX.
2. On the server system, log in as the DB2 instance owner.

3. Set DB2COMM to TPC/IP, for example:

   ```
   db2set DB2COMM=tcpip
   ```

4. Edit the `/etc/services` file to include both a DB2 connection service port and a DB2 interrupt connection if they do not already exist, such as,

   ```
   db2cDB2 50000/tcp # DB2 connection service port
   db2iDB2 50001/tcp # DB2 interrupt connection
   # service port
   ```

5. Update the database manager configuration, such as, db2 update dbm cfg using svcename db2cDB2. The argument after svcename must match the name of the DB2 connection port service that you placed in `/etc/services`.
6. Start and stop db2:

   ```
   % db2stop
   % db2start
   ```

After following these instructions, you should be able to open the Tivoli Enterprise Portal with workspaces.

Heartbeat issues when running IBM Tivoli Monitoring v6.x on a Linux guest using VMWare

When the Linux operating system is run as a guest using VMWare, it is possible for the clock of the Linux guest to run either faster or slower than real world time. If any IBM Tivoli Monitoring v6.x products are installed on Linux guests whose clocks are not running correctly, the result can be erratic system behavior. For example, if the Monitoring Agent for Linux OS is installed on a Linux operating system guest whose clock is running too slow, heartbeats from the agent are not produced on time. This results in the agent continuously going OFFLINE and ONLINE at the Tivoli Enterprise Monitoring Server, as the heartbeats arrive after the time interval has expired.

VMWare is aware of this issue, and has written several articles that address this problem. The following articles were current at the time this guide was published:

- "Clock in a Linux Guest Runs More Slowly or Quickly Than Real Time," http://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalID=1420
- VMWARE WHITE PAPER - "Timekeeping in VMware Virtual Machines," http://www.vmware.com/pdf/vmware_timekeeping.pdf

For the most up-to-date information on this issue, please consult the VMWare website (www.vmware.com).

How To Tell If You Have This Problem:

A simple way for determining whether or not your Linux guest has a clock problem is to benchmark it against a real world clock. Here is an example of a procedure that you can use:

1. From a Linux shell prompt, type "date" to get the current system date and time. While you are pressing **Enter**, look at a "real" clock (wall clock, watch, etc...) to get the real world time in minutes and seconds. Record the time from both your Linux guest and the "real" clock.

   ```
   Example:  Real Clock = 10:30:00, Linux Clock = 10:20:35
   ```

2. After 10 real time minutes have expired, type the "date" command again (you should type the "date" command ahead of time, so you only have to press **Enter** when 10 minutes have elapsed). Record the new times from both your Linux guest and "real" clock.

   ```
   Example:  Real Clock = 10:40:00, Linux Clock = 10:26:35
   ```

3. Compute the elapsed time for both your Linux guest and "real" clock. If the elapsed times are not the same, your Linux guest has a clock problem.

   Since we waited exactly 10 minutes using the "real" clock, we would expect that the elapsed time for the Linux clock would also be 10 minutes. Using the above figures, we can see that the elapsed time for the Linux guest is 6 minutes (10:26:35 - 10:20:35). Since this is less than the real world time, this means that the Linux guest clock is running slow. This causes the IBM Tivoli Monitoring product to behave erratically if the clock is not fixed.

Tivoli Enterprise Portal Server is unavailable

When a message indicates the server is unavailable, suspend further interactions until a message indicates the server is available unless you decide to end the current Tivoli Enterprise Portal session. When the Tivoli Enterprise Portal Server is available again, your client session is automatically reconnected and you can resume normal interactions. If the server is available and the client has not reconnected after three to five minutes, exit the browser, restart the browser, and restart a Tivoli Enterprise Portal client session.

Tivoli Enterprise Portal Server is not reconnecting

If the Tivoli Enterprise Portal Server does not reconnect, recycle the Tivoli Enterprise Monitoring Server and restart the Tivoli Enterprise Portal Server.

Cannot reconnect to the Tivoli Enterprise Monitoring Server

This message displays after the Tivoli Enterprise Monitoring Server goes down and attempts to reconnect. The Tivoli Enterprise Portal client attempts to log on once again to the Tivoli Enterprise Portal Server session. After a successful logon, the Tivoli Enterprise Portal client compares the Tivoli Enterprise Portal user authorities that were in effect when the original logon occurred with the current Tivoli Enterprise Portal user authorities. If any permission is different, you must restart the client session to ensure all components are synchronized with your user permissions. Changes to user permissions include navigator view assignment differences since the last logon.

If you want to apply new permissions for other users immediately, make all necessary changes and recycle the Tivoli Enterprise Monitoring Server. When the Tivoli Enterprise Monitoring Server recycle is complete, each user is reconnected and their user ID validated. If there were changes to their profiles, users must restart the Tivoli Enterprise Portal client session. The Tivoli Enterprise Portal client session doe snot to be restarted if no changes were made to their profiles.

Tivoli Enterprise Portal Server cannot connect to the Tivoli Enterprise Monitoring Server private interface

If the Tivoli Enterprise Monitoring Server is installed on an AIX server with a public and a private interface, the Tivoli Enterprise Portal Server cannot connect to the Tivoli Enterprise Monitoring Server. There are two environment variables you can set to control which interfaces to publish. For IPV4 use

KDEB_INTERFACELIST, for IPV6 use KDEB_INTERFACELIST_IPV6. In either address family, you can set those variables to set, restrict, or add to the interfaces in use.

Table 38. Control interface publishing

Interface control	Environment variable
To set specific interfaces for consideration:	`KDEB_INTERFACELIST=ip4addr-1 ... ip4addr-n` `KDEB_INTERFACELIST_IPV6=ip6addr-1 ... ip6addr-n`
To remove interfaces from consideration:	`KDEB_INTERFACELIST...=-ip4addr-1 ... -ip4addr-n` `KDEB_INTERFACELIST_IPV6=-ip6addr-1 ... -ip6addr-n`
To add interfaces for consideration:	`KDEB_INTERFACELIST=+ ip4addr-1 ... ip4addr-n` `KDEB_INTERFACELIST_IPV6=+ ip6addr-1 ...ip6addr-n`

where:

ip4addr
Specifies either a symbolic network name, or a raw form dotted decimal network address.

ip6addr
Specifies either a symbolic network name, or a raw form colon-separated hex digit network address.

Note: The plus sign must stand alone.

Chapter 7. Tivoli Enterprise Portal troubleshooting

This chapter describes problems you might experience with the Tivoli Enterprise Portal.

Cannot select the Create new group icon within the Object group editor

You use the Object group editor to organize situations, managed systems, and historical configurations into named collections that can be applied with a single action. After you select a specific node (for example, an operating system) within the Object group editor, the **Create new group** icon is enabled. When you expand your selection, the **Create new group** icon is disabled and cannot be selected. The current workaround is to simply reselect the node that you previously selected.

Cannot load product configuration data after changing warehouse database from Oracle to DB2 on Linux or UNIX

Changing your warehouse database from Oracle to DB2 on Linux or UNIX might prevent your system from loading product configuration data. As a consequence of this change, the Historical Collection Configuration panel displays a failure message:

```
Cannot load Product Configuration data
KFWITM220E Request failed during execution
```

To remedy this issue, peform the following procedure.

1. Stop the Tivoli Enterprise Portal Server.
2. Edit the `CANDLEHOME/config/.ConfigData/kcqenv` file by removing values from the KFW_JDBC_DRIVER, WHCLASS, WHURL, WHATTR, and WHDB2ATTR variables.
3. Start the Tivoli Enterprise Portal Server.

Stopped situations listed in Open state in the Manage Situation at Managed System window

For situations within policies, you might notice a inconsistency between the situation's current status and its status displayed in the Manage Situation at Managed System window. For example, create situation A and policy B (when situation A is true, write a message to the Universal Message console). Next, stop situation A. The message log indicates a situation status of Stopped, but the Manage Situation at Managed System window indicates that the situation status is Open. In the absence of policies, the Manage Situation at Managed System window reflects the current state of a situation. However, when policies are running, this assumption is not valid. A similar inconsistency occurs if you use the situation in the UNTIL clause of another situation.

Data in the Tivoli Enterprise Portal is missing and you receive an error

Data in the Tivoli Enterprise Portal is missing and you receive the following error:

```
KFWITM217E - SQL1_CreateRequest failed, rc=209
```

No support exists for the 64-bit data type at levels before IBM Tivoli Monitoring v6.2.1for the remote monitoring server. In IBM Tivoli Monitoring v6.2.1 and later, only 16-bit, 32-bit, and 64-bit data types are supported. For versions of Tivoli Monitoring earlier than v6.2.1, only 16-bit and 32-bit data types are supported.

JavaWebStart Tivoli Enterprise Portal fails to display help screens

The kjr.browser.default value must be set on non-Windows environments. For more information, see the Web Start: Specifying the browser location subsection in the *IBM Tivoli Monitoring Installation and Setup Guide*.

Client allows you to save a situation with an invalid character

It is possible to create and save a situation with a wildcard character such as an asterix (*). However, a situation created with this character is not valid.

Tivoli Enterprise Portal or the browser displays the yen symbol as a backslash in Japanese

The yen symbol is represented by x'5C' in the Japanese code page 943 and 932 (Shift-JIS). However, Windows systems also use x'5C' as the syntactic character "escape", "backslash", or a directory delimiter. In Unicode (used internally by Java), the backslash is U+005C and the yen symbol is U+00A5. The Java runtimes have two different converters for Shift-JIS code pages, depending on whether the input x'5C' should be treated as a backslash or the yen symbol. However, in the Tivoli Enterprise Portal or the browser, the JVM treats x'5C' as a backslash. This situation does not affect the function; it is only a display issue.

Using an administrator name with non-latin1 characters, cannot log onto the Tivoli Enterprise Portal

If you log onto a Windows system with an administrator name with non-latin1 characters, you cannot log onto the portal server by either the Tivoli Enterprise Portal desktop client or the Tivoli Enterprise Portal browser client. Set the cnp.browser.*installdir* Tivoli Enterprise Portal parameter to a path that does not contain any non-latin1 characters by completing the following steps:

1. Click **Start -> Programs -> IBM Tivoli Monitoring -> Manage Tivoli Monitoring Services**.
2. In the Manage Tivoli Monitoring Services window, right-click **Tivoli Enterprise Portal -> Browser** or **Tivoli Enterprise Portal -> Desktop_InstanceName** and click **Reconfigure**.
3. In the client configuration window that opens, double-click the cnp.browser.*installdir* parameter.
4. In the edit parameter window that opens, enter the path to where the browser view files should be installed on the client computer. If this is the browser client that you are configuring, use a path that is available at any computer from which users log on, such as `c:\temp`, and choose a path that does not contain any non-latin1 chars.
5. Select the In Use check box and click **OK**.
6. Click **OK** to save your changes.

Non-ASCII characters are not accepted in the user ID or the distinguished name field

If you have non-ASCII characters in your user ID or distinguished names within LDAP, and then add another user into the Tivoli Enterprise Portal, the characters are removed from the name and the user cannot log in. Remove the non-ASCII characters from distinguished name or the user ID.

The Tivoli Enterprise Portal desktop does not work when exporting DISPLAY

The Tivoli Enterprise Portal desktop does not work when exporting the DISPLAY from a Linux system to a Windows system running cygwin.

The Tivoli Enterprise Portal desktop client log on the Linux system, *install_dir*/logs/kcjras1.log, contains the following error:

```
EXCEPTION: Attempting to load home workspace: java.lang.IllegalArgumentException:
Width (0) and height (0)
```

Edit the cnp.sh startup file by doing one of the following:

- Add the java system property " -Dawt.toolkit=sun.awt.motif.MToolkit " by doing the following:
  1. Locate the *install_dir*/*architecture*/cj/bin/cnp.sh file on the Linux system.
  2. Change this line: ${TEP_JAVA_HOME}/bin/java -Xms64m -Xmx256m -showversion -noverify -classpath ${CPATH} -Dkjr.trace.mode=LOCAL ... to include the system property, ${TEP_JAVA_HOME}/bin/java -Xms64m -Xmx256m -showversion -noverify -classpath ${CPATH} -Dawt.toolkit=sun.awt.motif.MToolkit -Dkjr.trace.mode=LOCAL ...
- Use a 1.6 JRE to run the Tivoli Enterprise Portal desktop by doing the following:
  1. Locate the *install_dir*/*architecture*/cj/bin/cnp.sh file on the Linux system.
  2. Export TEP_JAVA_HOME=/opt/ibm/java-i386-60/.
  3. Export KCJ_HOME=... .

Tivoli Enterprise Portal browser client yields Error 2721 and will not run

This error occurs on Windows systems, and is due to registry issues with Java 1.5.0. The error occurs when you attempt to bring up the Tivoli Enterprise Portal from IBM Tivoli Monitoring v6.2.2 and then there is an automatic attempt to install Java 1.5.0. Use the Windows Add/Remove Programs utility and uninstall Java 1.5.0. Note: you can leave Java 1.4.2 installed. It does not affect this issue. When you have uninstalled Java 1.5.0, reboot your system. Now access the Tivoli Enterprise Portal, following any prompts to install Java 1.5.0 and the Tivoli Enterprise Portal should then launch and run on your Windows system.

Some attribute groups showing a different name in the Tivoli Enterprise Portal

The Tivoli Enterprise Portal pulls the attribute group names out of the resource bundle jar files for each product. At this time, these resource bundle jars are not guaranteed to be available to the CLI client. For example, KLZ CPU and KLZ Disk are listed in the Tivoli Enterprise Portal as Linux CPU and Linux Disk IO.

Monitoring agents show in an unexpected position in the navigation tree

In the Tivoli Enterprise Portal, the navigation tree represents all the agents in the environment with a top level of "Enterprise." The default presentation assumes that each agent of a particular type comes from a different IP address and hostname. When that is not true, the agent will display at an unexpected or random location. One example is when multiple agents are installed on a single server. Another example is when a high availability option like Microsoft Windows Clustering is used and an IP address is shared.

Changes to the agent environment variable "CTIRA_HOSTNAME" affect the display name in the workspace but not within the navigator tree. Here is an explanation of how to configure the portal server for desired navigator item display. The portal server has a configuration environment variable that changes the navigation tree to depend on the host name instead of the IP address: KFW_TOPOLOGY_CLUSTER_LIST. This variable is added to *installdir*\cnps\kfwenv file [Windows] or *installdir*/config/cq.ini [UNIX and Linux]. Its purpose is to force dependence on the hostname for navigator positioning instead of on the host address. A sample setting looks like this:

```
KFW_TOPOLOGY_CLUSTER_LIST=AFF_xxx AFF_yyy
```

Where the setting lists the agent affinities to which this hostname logic should apply. Here are some affinities for agents distributed with IBM Tivoli Monitoring version 6.1:

```
AFF_NT_SYSTEM                   "Windows OS"
AFF_ALL_UNIX                    "UNIX OS"
AFF_OS400_OM                    "i5/OS"
AFF_LINUX_SYSTEM                "Linux OS"
AFF_UNIX_LOG_ALERT              "UNIX Logs"
```

So, if you needed to use the hostname for navigator positioning for your Linux OS, UNIX OS and Unix Log monitoring agents, it would look like this:

```
KFW_TOPOLOGY_CLUSTER_LIST=AFF_ALL_UNIX  AFF_UNIX_LOG_ALERT AFF_LINUX_SYSTEM
```

There are many agents, so listing the affinity for each would be cumbersome. Here is a general method of figuring out the correct affinity name:

1. If you have an agent connected and showing as online, click on the navigator tree top node, then right click and select **Managed System Status**.
2. Make a temporary change to this workspace to show the agent affinity by right-clicking on any row and selecting Properties.
3. Click on the Filters tab.
4. Slide the scroll bar to the right and click on all the unset columns.
5. Click **OK** and slide the Managed System Status window to the right. For example, you should now see that for the Monitoring Agent for Windows OS, the affinity is: 00080000000000000000000000000000. You can export this

information to a .csv file and then work with that to extract the hex data. The affinity is the first 32 characters. Columns 33-34 are the product version code. Columns 35-43 are version flags.

6. Leave this workspace up, but when you switch away from this workspace be sure not to save it - since it was only a temporary change.
7. Open the installdir\cnps\affinity.properties [Windows] or the *installdir*/*arch*/cq/data/affinity.properties [Linux and UNIX] file. Confirm that "00080000000000000000000000000000" corresponds to the Monitoring Agent for Windows OS.
8. Next search for "tags.AFF_". Now you can see that Affinity 00080000000000000000000000000000 represents the AFF_NT_SYSTEM value. Using the above process, you can determine the correct settings for the agents where you need the KFW_TOPOLOGY_CLUSTER_LIST configuration.
9. You should recycle the portal server at this point and look at the display.

In many cases after you have completed the steps above, you have finished this task. However there are a few cases where additional configuration is necessary:

The host address is normally used for system identification, however with KFW_TOPOLOGY_CLUSTER_LIST set the first part of the Origin Node is used ("Primary:" is ignored). That first part defaults to the TCP/IP hostname, but it is replaced if CTIRA_HOSTNAME is set. This gives you control over deciding where an agent is positioned. Configuring an agent to have a specific CTIRA_HOSTNAME value manages cases where the IP address changes, and then KFW_TOPOLOGY_CLUSTER_LIST forces the navigation display to use that apparent hostname instead of the TCP/IP hostname.

Some agents require a different mechanism to change the apparent host name. In the case of the MQ Agent for example (AFF_MVS_MQM), update the mq.cfg file and add:

```
SET AGENT NAME(hostname)
```

Long hostnames can create confusion such as when a hostname is fully qualified. The default portal server processing only uses the first part of the fully qualified name, so two names like abc.xyz.large.com and abc.def.large.com would both appear at the node labeled abc. That can be controlled by adding the following to the portal server environment file (KFWENV/cq.ini):

```
KFW_TOPOLOGY_KEEP_DOT_IN_NODE_NAMES=Y
```

Remember the managed system names are limited to 32 characters - so the hostname:product can be truncated and cause accidental duplications. That would be another case where you would need to set the CTIRA_HOSTNAME.

Tivoli Enterprise Portal Desktop called through Java Web Start does not work properly after adding agents support for Tivoli Enterprise Portal Server

Launch the Manage Tivoli Enterprise Monitoring Services utility on the system where Tivoli Enterprise Portal Server is installed and execute the **TEPS reconfigure** action. Restart the Tivoli Enterprise Portal Desktop through the Java Web Start.

Receive a Loading Java TM0 Applet Failed.. error

There is a known problem with Firefox 3.5 (and possibily higher) that results in firefox a "Loading Java TM0 Applet Failed.." error when using the Java web browser client. There is a problem with way Firefox's JSObject is used to communicate between java and javascript. For more information, see the following website: http://groups.google.com/group/mozilla.feedback.firefox.prerelease/browse_thread/thread/cea83988856cffb6

tacmd createUser output indicates that the path to the Java home directory was not found

This problem occurs when issuing **tacmd createUser** on Windows 2003 SP1. The following error message is displayed:

```
KUICCU097E: The path to the Java home directory was not found.
 The directory name returned by the CandleGetJavaHome script was not found.
Call IBM Software Support.
```

To resolve this problem launch the `CandleGetJavaHome.bat` script located in `InstallITM` subdirectory of `ITM` home directory. Ensure that valid Java Home directory is returned. (This directory should exist and contain an installation of Java 1.5). If the message `CScript Error: Loading your settings failed. (Access is denied. )` is returned instead, ensure that the Windows Script Host (WHS) works properly in your environment.

To verify that Windows Script Host is working on your system, execute the following steps:

1. **Start --> Run**
2. Type `cmd` and hit Enter
3. Run the `cscript.exe` file.

If usage options are displayed, Windows Script Host is configured and working properly. If instead, the following error is displayed,

```
CScript Error: Loading your settings failed. (Access is denied. )
```

Follow the instructions on the Microsoft Support site to resolve this error in your environment before proceeding.

Cannot launch the Tivoli Enterprise Portal help

The Tivoli Enterprise Portal help might not display for the following reasons:

Popup blocker
If the browser toolbar has a popup blocker running, the help does not open whether you select **Contents** > **Index** from the Tivoli Enterprise Portal Help menu or click **Help** in a window. Turn off the popup blocker.

Internet Explorer shortcut keys the same for Tivoli Enterprise Portal
Some Tivoli Enterprise Portal shortcut keys are also used by Internet Explorer. If you are using the browser client and press F1 to open the Tivoli Enterprise Portal help, help for Internet Explorer displays instead. Select **Contents and Index** from the Tivoli Enterprise Portal Help menu.

JavaScript not enabled in Microsoft Internet Explorer
JavaScript might not be enabled in Microsoft Internet Explorer. See the Microsoft Knowledge Base Article 236846 for troubleshooting information.

http://support.microsoft.com/default.aspx?scid=kb;en-us;236846

Eclipse Help Server is not fully functional
If you make a request for help at the moment the Eclipse Help Server is not fully functional, wait until the start of this server has completed has completed, then refresh the help browser window or retry the help request.

On an Active Directory Server, sysadmin cannot logon to the Tivoli Enterprise Portal client

You receive the error message: invalid id/password. You must set the local security policy on an Active Directory server. If you installed IBM Tivoli Monitoring on a system where Microsoft Windows Active Directory is installed, you must update the local security policy on that system to include the sysadmin user so that you can log on to the Tivoli Enterprise Portal. This configuration task is necessary only on Active Directory systems and must be performed whether or not you plan to use the Monitoring Agent for Active Directory. Follow these steps to configure the local security policy:

- Enter secpol.msc at a command prompt. The Local Security Settings window is displayed.
- In the navigation pane on the left, select **Local Policies -> User Rights Assignments**.
- In the list of policies, right-click **Log on locally** and select **Security**.
- Click **Add**. The Select Users or Groups window is displayed.
- Select sysadmin from the list of user names.
- Click **Add**.
- Click **OK**.
- On the Local Security Policy Setting window, verify that the check box in the Effective Policy Setting column is selected for the sysadmin user.
- Click **OK** to save the new setting and exit.

Several enterprise workspaces are returning an error, KFWITM217E:Request Error,SQL1_CreateRequest Failed, rc=350

The following workspaces are Link Targets and should not be navigated to directly:

- Deploy Status By Product
- Deploy Status By Deploy Group
- Installation Logs

Attempts to navigate to them directly while in *ADMIN MODE* result in the observed error because required context is not available. Also, when navigating to any workspace that is the target of a link, that target workspace does not appear on the "Workspaces" menu.

You cannot paste non-ASCII characters in the Situation editor

You can type ASCII or non-ASCII characters in the Situation editor. You can paste ASCII characters in the Situation editor. However, you cannot paste non-ASCII characters in the Situation editor.

Situation editor cannot display advanced advice help files

In double-byte languages, when the font is set to italic, it cannot display the font in italics format.

After acknowledging a situation event and selecting the link for that situation, you might receive a message

You hover over a navigator item and then right click -> Quick Ack on any situation event. If you then select the link for the same situation , you might receive an error message. If you then wait without clicking **OK**, the Tivoli Enterprise Portal client exits.

If you encounter this problem, use any recent Sun JRE (1.5.0_14 or above). This problem is limited to IBM's 1.5 java.

Note: A Sun bug report bug_id=6578895 which describes the issue was fixed in Sun's 1.5.0_14.

Password problem using the LDAP Security option on Active Directory system

Create "ldapuser" on the Active Directory system. Configure the Tivoli Enterprise Portal Server with the LDAP Security option. Logon to the Tivoli Enterprise Portal as "sysadmin" and add "ldapuser" from the Administer Users option. In **User Information**, **Distinguished Name** should be "cn=ldapuser,o=ITMSSOEntry". Logon to the Tivoli Enterprise Portal as "ldapuser" with the ldapuser password credentials. Change the password of "ldapuser" from the Active Directory system. Reconfigure the Tivoli Enterprise Portal Server again for a new password. Restart the Tivoli Enterprise Monitoring Server and the Tivoli Enterprise Portal Server.

By default, both the old and the new passwords continue to work for approximately one hour after the password change. After one hour, the old password stops working. Windows 2003 Service Pack 1 introduced this behavior into Active Directory. Please refer to Microsoft KB article 906305 for information on what occurs and for instructions on disabling the behavior if necessary.

There is a memory leak in the Tivoli Enterprise Portal browser client when the number of workspace switches increases

When using the Tivoli Enterprise Portal browser client on a Windows system with Internet Explorer 6.x, 7.x, or Mozilla Firefox 2.x, a memory leak might be observed that continues to grow as the number of workspace switches increases. This problem is due to a handle leak introduced by the IBM Java 1.5 plug-in component. The same problem is present in the Sun Java 1.5 plug-in component. Restart the Tivoli Enterprise Portal browser client whenever the memory utilization of the browser being used (Internet Explorer or Firefox) becomes excessive. Typical symptoms of this problem include poor response time of the Tivoli Enterprise Portal client, as well as out-of-memory exceptions being written to the Tivoli Enterprise Portal client log files.

Help index and search text entry fields are disabled

For some reason, your browser is unable to load the Java applets necessary to enable the Index and Search fields, and is rendering the help in Pure HTML. If you view Tivoli Enterprise Portal help with Internet Explorer use the following steps to resolve this problem:

1. From the Internet Explorer browser toolbar go to **Tools** > **Internet Options** > **Advanced** > **Java (IBM)**.
2. Clear the **Use Java version 1.4.2 for <applet> (requires restart)** check box.

If the help index and search text entry fields are still disabled after clearing the **Use Java version 1.4.2 for <applet> (requires restart)** check box, see "On Linux, IBM Tivoli Enterprise Monitoring Agent topics do not display in the Help Contents or Index tabs" on page 135.

Java exception logging onto the Tivoli Enterprise Portal from a browser

If you encounter an exception that has the following text:

```
"java.lang.UnsatisfiedLinkError: com/webrenderer/server/
NativeMozillaLibrary.setMozPath"
```

delete the WebRenderer directory under the home path. For Linux systems, this path is `$HOME/.webrendererswing`, and for Windows systems, this path is `%HOMEPATH%/.webrendererswing`.

On Linux, IBM Tivoli Enterprise Monitoring Agent topics do not display in the Help Contents or Index tabs

You can see the Tivoli Enterprise Portal help topics in the Contents tab, but none for your installed monitoring agents. Change your default browser to Internet Explorer or complete the following steps:

1. If the help is open, close the browser window.
2. On the computer where the Tivoli Enterprise Portal Server is installed, locate the `contents.htm` file:

   Windows:
   `<install_dir>\cnb\classes\candle\fw\resources\help`

   UNIX-based systems:
   Linux: `<install_dir>/cnb/classes/candle/fw/resources/help`
3. Rename `contents.htm` to `contents.bak`.
4. Rename `contents_dhtml.htm` to `contents.htm`.

Tivoli Enterprise Portal Navigator items are listed in an unexpected order

When expanding items in the Tivoli Enterprise Portal Navigator, parent items might list child items in an unexpected order. Navigator items are ordered internally on the Tivoli Enterprise Portal Server and therefore might not reflect a logical ordering in any particular language. Use the **More...** indicator at the end of the branch of child items to append them until you locate a the item you need.

Clicking on the Timespan icon for one view brings up the data for another view

The timespan panel provides this check box at the bottom of the panel: **Apply to all views associated with this view's query**. If both views in question share the same query, and this check box is selected, a change in one view's time span also affects the other as expected. However, when the check box is unselected, this behavior is still exhibited.

If you want one of the views to not have the time span, you must now go back in and change it manually.

HEAPDUMPs and JAVACore files are placed on the desktops when running Tivoli Enterprise Portal in browser mode

The Tivoli Enterprise Portal client uses the IBM Java Plug-in, which is automatically installed on your computer with the Tivoli Enterprise Portal. Adjust the IBM Java Plug-in properties if performance is slow or your workstation receives HEAPDUMPs and JAVACore files, an out-of-memory condition, when you are logged on. Make the following adjustments to correct this problem:

- Increase the Java heap size settings. Set the minimum heap size to 128 MB. Set the maximum heap size to 256 MB. If you continue to experience problems, increase the maximum setting in increments of 64 MB until the symptoms disappear.
- When memory requests by the Tivoli Enterprise Portal cannot be satisfied from Java heap storage, the JVM performs garbage collection to reclaim free memory. If the Java heap size settings are too small, the amount of time it takes to perform garbage collection becomes excessive, resulting in high CPU utilization and poor response time. In some cases, Java HEAPDUMPS and JAVACore files are placed on user desktops, indicating an out-of-memory condition. Increasing the Java heap size parameters over the default values helps you avoid these problems.
- If you observe symptoms of heap memory exhaustion after changing the heap size settings to the suggested values, increase the maximum setting in increments of 64 MB until the symptoms disappear.
- Make sure the client workstation has enough memory to handle the maximum heap size. To determine if the client workstation has sufficient memory, observe the available physical memory (as shown on the Windows Task Manager Performance tab) when the workstation is not running the Tivoli Enterprise Portal client, but is running any other applications that need to run concurrently with the portal client. Verify that the client workstation has enough available physical memory to hold the entire maximum Java heap size for the Tivoli Enterprise Portal plus another 150 MB. The additional 150 MB provides an allowance for non-Java heap storage for the Tivoli Enterprise Portal and extra available memory for use by the operating system.
- Set the Java Plug-in cache to an unlimited size to avoid performance problems due to insufficient cache space for Tivoli Enterprise Portal JAR files.
- If you have just upgraded to a new release or fix pack, clear the plug-in cache to remove old versions of the Tivoli Enterprise Portal JAR files.

Complete the following steps to adjust the Java Plug-in settings:

1. Open the Windows Control Panel.

2. Double-click **IBM Control Panel for Java(TM)** to display the Java(TM) Control Panel.
3. From the **Java(TM)** tab:
   a. Click **View**.
   b. Double-click on the **Java Runtime Parameters** field and enter: `-Xms128m -Xmx256m` .
4. Click **OK**.
5. From the **General** tab complete the following steps to clear the browser cache:
   a. Click **Delete Files...**
   b. Check the box labeled **Downloaded Applets**.
   c. Click **OK**.
6. Click **OK** in the Java(TM) Control Panel.

Note: On 64-bit systems when a 32-bit SUN JRE is already installed, the 32-bit SUN JRE control panel appears independently when you access Start->Control Panel->Add or Remove Programs->Java. After installing a 64-bit SUN JRE over the 32-bit SUN JRE, the 32-bit SUN JRE control panel disappears from the location, and the 64-bit SUN JRE control panel appears when you access Start->Control Panel->Add or Remove Programs->Java instead of the 32-bit SUN JRE control panel. If you want to access the 32-bit SUN JRE control panel, use the `32bit_jre_install_dir/bin/javacpl.exe` file.

Java errors occur with the IBM v1.4.2 JRE

If you experience any problems using the IBM 1.4.2 JRE use the version shipped with IBM Tivoli Monitoring v6.1.

IBM Tivoli Monitoring v6.2 ships with IBM 1.5.0 JRE. Use this version if you have installed IBM Tivoli Monitoring v6.2.

Web Portal Client does not work with Sun JRE

Update one file associated with the Tivoli Enterprise Portal browser client in order to ensure that the Sun JRE is used. The file name is `jrelevel.js`, and it is located in the `\IBM\ITM\CNB` directory on Windows systems. Here is the default value currently seeded in the file:

```
var jreLevel    = "1.5.0"
```

The following value picks up the latest 1.5.x_xx version

```
var jreLevel = "5.0"; -- "family" JRE identifier
```

The following value use the default JRE, which should be the Sun JRE assuming it was the last one installed:

```
var jreLevel = "*"; --
```

Clear the browser cache and restart your browser client. To clear the browser cache Open Java Control Panel (start/Control Panel/Java), and complete the following steps:

1. Select the General tab.
2. Click **Delete Files...**.
3. Check the box labeled "Downloaded Applets:".

4. Click **OK**.

You can find the browser log in the following directory (ensure that your folder options are set to display hidden files):

- `C:\Documents and Settings\Administrator\Application Data\IBM\Java\Deployment\log>plugin150.trace` (for IBM java plugin)
- `C:\Documents and Settings\Administrator\Application Data\Sun\Java\Deployment\log>plugin150_xx.trace` (for sun jre)

Tivoli Enterprise Portal has high memory usage and poor response time

The amount of Java memory used by the Tivoli Enterprise Portal increases with the size of the monitored environment. If the maximum Java heap size setting is too low, the amount of time spent by the JVM performing garbage collection can become excessive, resulting in high CPU utilization and poor response time. Verbose garbage collection (GC) data can be used to determine if excessive garbage collection occurs. If the percentage of time spent performing garbage collection is greater than 5%, increase the maximum Java heap size (the -Xmx parameter) to provide more memory and reduce garbage collection activity. For more information about collecting verbose GC data and Java heap tuning parameter changes, refer to the IBM Developer Kit and Runtime Environment, Java 2 Technology Edition, Version 1.4.2 Diagnostics Guide (SC34-6358-01), which is available from http://www.ibm.com/developerworks/java/jdk/diagnosis/. Use the following steps to increase the maximum Java heap size.

Tivoli Enterprise Portal browser client

Edit the Java heap parameters using the Java Plug-in Control Panel. Before you change the values for the Java Plug-in, consider that any changes affect all Java applications that use the Java Plug-in. See "Preparing your Tivoli Enterprise Portal environment" in the *IBM Tivoli Monitoring Administrator's Guide* for more information.

1. Open the Windows Control Panel.
2. Double-click Java Plug-in for IBM Java V1.4.2 (or right-click and select Open). If you have multiple Java Plug-ins, check that you have the properties for the right plug-in opened: The About tab shows V1.4.2, and the Cache or Certificates tab shows IBM in the path or in the signed certificate.
3. In the Advanced tab, select the IBM JRE 1.4.2 from the Java Runtime Environment list.
4. In the Java Runtime Parameters field, enter `-Xms128m -Xmx256m`.
5. Click **Apply**.

Tivoli Enterprise Portal desktop client

Edit the `cnp.bat` file in `install_dir\CNP` to change the Java heap parameters in the set command to `-Xms128m -Xmx256m`.

Tivoli Enterprise Portal has high memory usage

The amount of Java memory used by the Tivoli Enterprise Portal depends on the size of the monitored environment. The largest component of the memory usage is for the Java heap, which contains both short-term and long-term data. When a memory request cannot be satisfied from free Java heap storage, "garbage collection" is performed to reclaim free memory. There are many Java heap tuning parameters for IBM Java run-time environments that can be used to influence

garbage collection and memory management. Notable among these are the minimum free percentage (-Xminf) and maximum free percentage (-Xmaxf) parameters. IBM Java documentation provides the following descriptions:

-Xminf<number>
A floating point number, 0 through 1, that specifies the minimum free heap size percentage. The heap grows if the free space is below the specified amount. The default is .3 (that is 30%).

-Xmaxf<number>
A floating point number between 0 and 1, which specifies the maximum percentage of free space in the heap. The default is 0.6, or 60%. When this value is set to 0, heap contraction is a constant activity. With a value of 1, the heap never contracts.

You can lower the amount of free space maintained in the Java heap at the expense of higher CPU utilization and longer response time by setting the minimum free and maximum free percentages to lower values.

Default values:
-Xminf0.30 –Xmaxf0.60

Consider the following values:
-Xminf0.15 –Xmaxf0.30

The IBM Java documentation warns that setting these values too low can cause poor Java performance. For more information on Java heap tuning parameters, refer to the IBM Developer Kit and Runtime Environment, Java 2 Technology Edition, Version 1.4.2 Diagnostics Guide (SC34-6358-01), which is available from http://www.ibm.com/developerworks/java/jdk/diagnosis/.

Data is not returned to the Tivoli Enterprise Portal client

Do the following to ensure that data can return to the Tivoli Enterprise Portal client:

- Ensure that the monitoring agent is online.
- Verify that all the application-related files were installed with the Tivoli Enterprise Portal Server.
- Check the `kfwras1.log` for errors.
- Set the following trace option in the `KFWENV` file:
  `(UNIT:ctsql INPUT)`

DirectDraw thread loops infinitely causing poor Tivoli Enterprise Portal performance

Java uses DirectDraw by default but VMWare does not support DirectDraw. Perform the following steps for both desktop and browser clients from Manage Tivoli Enterprise Monitoring Services to set Java Runtime not to use DirectDraw for graphic rendering:

1. Right-click **Tivoli Enterprise Portal**.
2. Select **Advanced > Edit Variables . . .**
3. Double-click the line with `sun.java2d.noddraw` to open the **Edit Tivoli Enterprise Portal Parm** window.
4. Ensure the value is true.
5. Click the **In Use** box so to place a check-mark in the box.

6. Click **OK** to close the window.
7. Click **OK** to close the configuration window.

Workflow Editor is disabled and the following tools do not display: Event Console, Graphic View, Edit Navigator View (Navigator view toolbar)

If you did not enable Manage Tivoli Enterprise Monitoring Services during installation, the Workflow Editor is disabled and the following tools do not display:

- Event Console
- Graphic View
- Edit Navigator View (Navigator view toolbar)

1. On the computer where the Tivoli Enterprise Portal Server is installed, select **Start** > **Programs** > **Tivoli Monitoring Services** > **Manage Tivoli Enterprise Monitoring Services.**
2. Right-click the Tivoli Enterprise Portal Server service, point to Licensing and select Tivoli Enterprise Portal Server from the menu.
3. In the Tivoli Enterprise Portal Service License window, enter the new license key if one was issued.
4. Check **Enable Tivoli Enterprise Monitoring Server**.
5. Click **OK**.

   When you click **OK**, the server stops and a message in Tivoli Enterprise Portal says the server is unavailable. If you do not close the client work session, after the server has been started again (next step), another message says your Tivoli Enterprise Portal permissions have changed and prompts you to restart.
6. Restart the Tivoli Enterprise Portal Server and, after startup is complete, restart the Tivoli Enterprise Portal client.

Situations are not firing

Do the following to determine why situations are not firing in the Tivoli Enterprise Portal:

- Confirm the situation is firing in the event console.
- Ensure that the situation was distributed.
- Verify whether the situation is associated with a node in the Tivoli Enterprise Portal Navigator.
- Ensure that the situation condition is true.
- Check the operations log of the agent.

Historical UADVISOR situations are started on the agent if historical collection is configured to collect data

Anytime you configure an IBM Tivoli Monitoring historical collection for any agent, UA or otherwise, the name of the history situation is always called UADVISOR_xxxxx. If you see these UADVISOR_xxxxx entries in the list of defined situations, even though they were never explicitly defined, these history situations were automatically defined by an IBM Tivoli Monitoring component.

At the bottom of each view, you see a historical workspace KFWITM217E error

At the bottom of each view, you see the following historical workspace KFWITM217E error: Request failed during execution, and a red icon.

Ensure that you configure all groups that supply data to the view. In the Historical Configuration view, ensure that data collection is started for all groups that supply data to the view. Views containing multi-row attributes show this message if no row data are collected.

Installation of situation data fails due to I/O on VSAM data sets

After installation of application support, product-provided situations do not appear in the Tivoli Enterprise Portal Situation editor or do not auto start. This problem occurs only with a z/OS hub monitoring server.

Explanation: The definitions of product-provided situations are installed on the hub Tivoli Enterprise Monitoring Server when application support for a product is installed. If the VSAM data sets in which the data is stored have filled up so that the data cannot be added, situations definitions may not be installed or the definitions may be incomplete.

If application support has been installed, check the `NonResSeedk`*`pp`*`.log` files in install_dir\cnps\logs for errors (where *pp* is the two-letter product code of a monitoring product for which you installed support). Any `SQL1_OpenRequest status=81` errors may indicate that you have a VSAM I/O error.

Workaround: If you see this error, check data sets whose names end in RKDS* to determine if they are out of space or have run out of extents. For example, *&rhilev.&rte.&vsamfsv.RKSSSITF*, where *&rhilev* is the VSAM runtime high-level qualifier, *&rte* is the RTE name, and *&vsamvsf* is the monitoring server EIB VSAM low-level qualifier." Refer to the TEMS started task to see a complete list of VSAM EIB files.

If the data sets are out of space:

1. Use IDCAMS to copy the data to a flat file.
2. Delete the existing file.
3. Modify the ICAT *PP*#1*xxxx* job to increase the size (where *PP* is the two-letter product code for the product [**DS** for a standalone Tivoli Enterprise Monitoring Server] and *xxxx* is the RTE JCL suffix) as follows:
   a. Invoke the Configuration Tool by executing this TSO command:
      `EX '&shilev.INSTLIB'`

      where *&shilev* is the installation high-level qualifier.
   b. On the Configuration Tool MAIN MENU, enter **3 (Configure Products)** and select the product you are want to configure (ITM Tivoli Monitoring Services or an OMEGAMON XE monitoring agent) on the PRODUCT SELECTION MENU.
   c. On the RUNTIME ENVIRONMENTS (RTES) menu, type **B** for (Build libraries) next to the runtime environment in which the monitoring server is configured, and press **Enter**. The PP#1xxxx job that allocates the runtime libraries is displayed.

d. Edit the CYL() parameter in the job to increase the VSAM allocation to whatever value your DASD can accommodate

4. Submit the PP#1xxxx job.
5. Use IDCAMS to copy data from the flat file to the new VSAM.
6. Reinstall the application support for the product or products whose situations are missing or not starting correctly.

For instructions on installing application support for a monitoring agent installed on z/OS, refer to the configuration guide for your monitoring agent.

For instructions on installing application support for monitoring agents installed on a distributed system (Windows, UNIX, Linux) see the *IBM Tivoli Monitoring: Installation and Setup Guide*.

kshsoap client fails because of missing libraries on UNIX-based systems

On UNIX-based systems, the CandleSoapClient shell script calls kshsoap binary from inside, while sourcing the environment. You do not need to run the kshsoap binary, as required on a Windows platform.

Category and Message field of the universal message does not accept DBCS

To record a DBCS IBM Tivoli Monitoring V6.1 universal message when a situation is true, following these steps on Tivoli Enterprise Portal client:

1. Open the Situation editor.
2. Select a situation.
3. Select the **Action** tab.
4. Check **Universal Message** button.
5. Move the cursor to **Message** or **Category** text field.
6. Enable Input Method (IM) for DBCS.
7. Type a key to input DBCS.

However, at step 7, nothing is set into the text field because the text field does not accept double byte characters (DBCS). Disable the Input Method and input only single byte characters (SBCS).

An error occurs when remotely removing an instance on Windows

The following log shows an error occurs when remotely removing an instance on Windows.

```
(4300DFC2.0000-828:kbbssge.c,52,"BSS1_GetEnv") KBB_RAS1="ERROR ^>
C:\IBM\ITM\tmaitm6\logs\KNTRAS1.LOG"
(4300DFC2.0001-828:kbbssge.c,52,"BSS1_GetEnv") CANDLE_HOME="C:\IBM\ITM"
(4300DFCE.0000-828:kdytasks.cpp,1063,
"runCommand") Bad return code (3221225477) from command
"C:\IBM\ITM\TMAITM6\kdy_xa.exe -r DB2:FROBERTS:UD
-pc ud" (4300DFCE.0001-828:kdytasks.cpp,1066,"runCommand")
STDOUT [0 characters] is:  (4300DFCE.0002-828:kdytasks.cpp,1069,
"runCommand") STDERR [76 characters] is: Error line(391): Unable to delete file:
C:\IBM\ITM\tmaitm6\KUDCMA_DB2.exe
(4300DFCE.0003-828:kdytasks.cpp,3291,"setConfig") KDY1008E Received bad return code
[3221225477] from two-way translator
command [C:\IBM\ITM\TMAITM6\kdy_xa.exe -r DB2:FROBERTS:UD -pc ud]
```

```
(4300E020.0000-864:knt10agt.cpp,243,"getBinaryPath")
Error retrieving binary path for process ID 8.
(4300E021.0000-864:knt10agt.cpp,243,"getBinaryPath")
Error retrieving binary path for process ID 8
```

This error can occur when the Tivoli Enterprise Monitoring Server is restarted and the agent displays offline even though its running because the agent did not register a heartbeat yet.

Agents display offline in the Tivoli Enterprise Portal but still fire situations and the agent logs are report that they are running

This error can occur if the agent names in the group identified contained embedded spaces. Agent names cannot contain embedded spaces. Edit the agent names to remove the spaces. The CTIRA_HOSTNAME environment variable on the agents must include a specific definition for correct agent host names.

The Tivoli Enterprise Portal displays erratic sorting behavior when removing more than one managed system simultaneously

The Tivoli Enterprise Portal display erratic sorting behavior when you remove multiple managed systems at the same time after clicking **Remove Offline Systems** menu item from the Managed System Status view. Allow the display to finish updating before attempting another operation.

Multiple events that occur at the same time are loaded too slowly

Manually set the variable KFW_CMW_EVENT_SLEEP in `cq.ini` on Linux or `kfwenv` on Windows to less than 10 seconds:

```
KFW_CMW_EVENT_SLEEP=5
```

Desktop client performs poorly after installing Language Packs for IBM Tivoli Monitoring V6.1

Some configuration settings for the IBM Tivoli Monitoring Warehouse database can cause performance degradation. Perform the following steps from a db2cmd prompt to correct the DB2 settings:

1. Check the Health Monitor configuration:
   ```
   db2 get dbm config | find /I "health"
   ```
2. Turn the Health Monitor off:
   ```
   db2 update dbm config using HEALTH_MON OFF
   ```
3. Determine what databases IBM Tivoli Monitoring connects to:
   ```
   db2 list application
   ```
4. Check system buffer pool settings on the Tivoli Enterprise Portal Server and PROXYWH databases:
   a. `db2 connect to TEPS db2 select * from SYSIBM.SYSBUFFERPOOLS`
   b. `db2 connect reset`
   c. `db2 connect to PROXYWH`
   d. `db2 select * from SYSIBM.SYSBUFFERPOOLS`

   (Must be a value of 250.)
5. Adjust buffer pool settings that are too high:

Note: You must be connected to that database.

```
db2 alter bufferpool ibmdefaultbp size 250
```

6. Disconnect all applications:

```
db2 force application all
```

7. Stop DB2:

```
db2stop
```

8. Start DB2:

```
db2start
```

9. Recycle Tivoli Enterprise Portal Server service.

Existing OMEGAMON product imagery displays after upgrading to IBM Tivoli Monitoring V6.1

Existing OMEGAMON product imagery displays after upgrading because there it was cached on the client browser. Use the following steps to correct the problem:

1. Close all browser instances.
2. Clear the browser cache.
3. Reload the Tivoli Enterprise Portal browser client.
4. Verify the correct images display.

The Warehouse Proxy Agent started, but does not appear in the Managed System Status list on the Tivoli Enterprise Portal

The database was either not created in UTF-8 or the DB2CODEPAGE was not setup in the environment as required for proper operation. You need to set the DB2CODEPAGE=1208 (no spaces after the 1208) on the system environment After you have done this, shutdown the Warehouse Proxy Agent, drop the UTF8TEST table from the database, and then restart the agent.

Cannot start or stop agents from the Navigator view

This feature is not supported in environments with a z/OS Tivoli Enterprise Monitoring Server.

Cannot load a ws_pres.css file in order to select a language other than English

The user.language parameter allows you to specify the language code. The portal client uses cascading style sheets to render the application text. If no localized version of a style sheet, such as `ws_press.css`, is available, the English version will be used.

Chapter 8. Tivoli Enterprise Portal Server troubleshooting

This chapter describes problems that might occur with the Tivoli Enterprise Portal Server. If you do find the resolution to a problem you experience with the Tivoli Enterprise Portal Server in this chapter, see Chapter 6, "Connectivity troubleshooting," on page 115.

Performance impacts of the HTTP and HTTPS protocols

Connection protocol options between the Tivoli Enterprise Portal client and the Tivoli Enterprise Portal Server include the default protocol, IIOP, as well as the HTTP and HTTPS protocols. Note, however, that you might encounter a response time impact when you use the HTTP and HTTPS protocols. Affected workspaces include the Linux Process workspace, Linux PAS workspace, and UNIX Process workspace. These workspace have longer response times when you use the HTTP Tivoli Enterprise Portal client instead of the CORBA/IIOP Tivoli Enterprise Portal client. In addition to the response time impact, you might encounter increased CPU consumption for the HTTP and HTTPS protocols.

Users who run the IBM HTTP Server do not have permission to the content directory

During configuration and startup of the Tivoli Enterprise Portal Server, the system attempts to confirm that the user running the IBM HTTP Server has permission to access the IBM HTTP Server content directory. If not, one of the following messages are displayed:

```
KCIIN2723W User who runs IHS (IBM HTTP Server) does not have proper permissions
 to IHS content directory. Do you want to continue?
```

or

```
KCIIN2724W User who runs IHS (IBM HTTP Server) does not have proper permissions
 to IHS content directory.
```

This error occurs when the IBM HTTP Server is running under a user that does not match the user specified in the *CANDLE_HOME/ARCH/iu/ihs/httpd.conf* file.

For the portal server to run correctly, the user who is running the IBM HTTP Server must have access to the IBM HTTP Server content directory.

tacmd exportWorkspaces or importWorkspaces receives an out of memory error

If you get an OutOfMemory Error when running this command, you can increase the maximum Java heap size for the tacmd java JVM by using the TACMD_JVM_MAX_MEMORY environment variable. This variable specifies the maximum java heap size (in megabytes) for the tacmd Java virtual system. Memory for tacmd is freed when the tacmd invocation finishes. Valid values are 256 through to 2048, inclusive.

For IBM Tivoli Monitoring v6.2.2 Fix Pack 2 or higher, you can set it in the command environment , using SET/export, or you can set it in the environment files (KUIENV on Windows systems, or the $CANDLEHOME/bin/tacmd shell script on UNIX and Linux systems).

The portal server and Warehouse Proxy Agent fail to connect to the database on a 64-bit Windows system

The ODBC control panel available in the Windows Start menu is for 64-bit ODBC configuration. Since the portal server and the Warehouse Proxy Agent are 32-bit applications the 32-bit ODBC control panel must be used. Launch the 32-bit ODBC window from C:\Windows\SysWOW64\odbccp32.cpl and manually create the "ITM Warehouse"/"TEPS" ODBC source by going to the System DSN tab and clicking **Add**.

Failed to log in as sysadmin with portal server LDAP enabled

When LDAP authentication is enabled for the monitoring server, the sysadmin ID must be defined in the LDAP server. However, when LDAP is enabled for the portal server, the sysadmin ID should exist in the monitoring server's local OS user registry, but should not be defined in the LDAP server, otherwise, the sysadmin ID will not be able to log in.

On AIX systems, newly created users with auto-expire passwords cause installation failures

When installing on AIX systems, security policies for newly created users auto-expire the password after the first use and require you to set a new (or same) password as a permanent password. The Tivoli Enterprise Portal Server configuration interface allows you to create a new user ID for the portal server and warehouse database, but using the interface always fails because the user password is not set and is expired. You must ssh/telnet into the same server, using the target user ID, and set the password appropriately.

Linux portal server unable to FTP catalog/attribute files

Linux portal server unable to FTP catalog/attribute files with Manage Tivoli Enterprise Monitoring Server. A monitoring server is needed along with the portal server (on the same system) to be able to seed a z/OS monitoring server.

Upgrading the Tivoli Enterprise Portal Server takes a long time

Performing a Tivoli Enterprise Portal Server upgrade, depending on the efficiency of the hardware platform, can take anywhere from 30 minutes to over an hour.

Running the Tivoli Management Services Discovery Library Adapter, results in a book that does not contain the fully qualified hostname

Edit the resulting xml file and change the shortname to the fully qualified hostname.

Tivoli Enterprise Portal Server performance is slow

If you want to increase the performance of your portal server and you are not concerned about security, you can disable Secure Socket Layer data encryption on the portal server. If you do not want to use Secure Socket Layer communication between IBM Tivoli Monitoring components and the Tivoli Enterprise Portal Server, use the following steps to disable it:

1. In Manage Tivoli Enterprise Monitoring Services, right-click **Tivoli Enterprise Portal Server**.
2. Click **Advanced > Edit ENV** file.
3. Find the following line:

   ```
   kfw_interface_cnps_ssl=Y
   ```

4. Change the `Y` to `N`.
5. Save the file and exit.
6. Click **Yes** when you are asked if you want to recycle the service.

Cannot create a Tivoli Enterprise Portal Server database

When using DB2 8.1 or 8.2, you must install the correct fix pack versions of DB2 in order to create a Tivoli Enterprise Portal Server database. These fix pack versions are:

- DB2 V8.1 with Fix Pack 10 or higher fix packs
- DB2 V8.2 with Fix Pack 3 or higher fix packs

Also, on AIX systems, a failure occurs when you attempt to install a Tivoli Enterprise Portal Server with a DB2 database. Using the db2 installation user ID (default is db2inst1), do the following:

1. Stop the DB2 server if not already stopped using the following command:

   ```
   cd /db2inst1/sqllib/adm
   db2stop
   ```

2. Issue the following configuration changes:

   ```
   export EXTSHM=ON
   db2set DB2ENVLIST=EXTSHM
   db2set -all
   ```

3. Using your preferred editor add the following lines to the `/db2inst1/sqllib/db2profile` file:

   ```
   EXTSHM=ON
   export EXTSHM
   ```

4. Restart the DB2 server using the following command:

   ```
   cd /db2inst1/sqllib/adm
   db2start
   ```

5. Restart the Tivoli Enterprise Portal Server using the following command:

   ```
   cd /opt/IBM/ITM/bin
   ./itmcmd agent start cq
   ```

For information on how to modify kernel parameters, see http://publib.boulder.ibm.com/infocenter/db2luw/v9/index.jsp?topic=/com.ibm.db2.udb.uprun.doc/doc/t0008238.htm

You receive a KFW error when a query is sent to more than 200 managed systems

You receive the following error when a query is sent to more than 200 managed systems:

```
KFWITM217E Request error: Request to xxx nodes exceeds the limit of 200.
Please specify a smaller distribution or increase the maximum.
```

There is a default limit of 200 nodes for any single query for a workspace view. If the following conditions exist in the query for a workspace view, you must increase the **KFW_REPORT_NODE_LIMIT** environment variable for the Tivoli Enterprise Portal server environment variable as described below:

- The query is assigned to a managed system list that contains more than 200 managed systems.

  OR
- More than 200 managed systems are explicitly assigned to a query in any workspace view.

Under these conditions, you must increase the following Tivoli Enterprise Portal server environment variable.

```
KFW_REPORT_NODE_LIMIT=xxx
```

where *xxx* is an integer that is equal to or greater than one of the following:

- The number of managed systems defined in a managed system list.

  OR
- Explicitly assigned to a query over 200 in a Tivoli Enterprise Portal workspace view.

You must add the **KFW_REPORT_NODE_LIMIT** environment variable or remove the comment marker (#) in the following Tivoli Enterprise Portal Server environment files, and restart the portal server.

- Windows systems: `\ibm\itm\cnps\kfwenv`
- Linux or AIX systems: `/opt/IBM/config/cq.ini`

After you change the **KFW_REPORT_NODE_LIMIT** variable, you might receive the following error:

```
KFWITM217E Request error: SQL1_CreateAccessPlan failed, rc=1.
```

Typically this problem is caused when too many explicitly defined managed systems are assigned to a query for a workspace view. The best practice for resolving this problem is as follows:

1. Create a managed system list that specifies the explicitly defined managed systems.
2. Remove the explicit assignments from the query.
3. Assign the managed system list to the query.

Alternatively, you can reduce the number of managed systems that you explicitly define in the query.

Non-hub situations are not associated at the Tivoli Enterprise Portal Server level

Only pure hub situations should be associated to the Tivoli Enterprise Portal Server. However, if you want non-hub situations to be associated at the Tivoli Enterprise Portal Server level, set the Tivoli Enterprise Portal Server environment variable: KFW_CMW_SPECIAL_HUB_ENTERPRISE=N.

When non-hub situations are associated at the Tivoli Enterprise Portal Server, they turn TRUE, meaning they are visible in the situation event console. Through the Situation editor, if you assign all the agents and managed systems lists from a situation, that situation event continues to appear in the situation event console.

Starting and stopping the Eclipse Help Server

The Tivoli Enterprise Portal Server depends on the Eclipse Help Server to display standalone help. The Eclipse Help Server is treated in the same way as Tivoli Enterprise Portal Server - as a server component (as opposed to IBM Tivoli Monitoring v6.1, where the Eclipse Help Server was treated as an agent).

This change necessitates that the Eclipse Help Server is started whenever the Tivoli Enterprise Portal Server is started (Eclipse Help Server start failure does not affect Tivoli Enterprise Portal Server startup). The UNIX command **itmcmd** agent stop or start all, does not stop or start the Eclipse Help Server now, since it does not also stop or start Tivoli Enterprise Portal Server. On Windows systems, starting or stopping of all components using kinconfg.exe still applies to all components without exceptions. The Eclipse Help Server, by default, cannot be stopped if the Tivoli Enterprise Portal Server is running. To stop the Eclipse Help Server, first stop the Tivoli Enterprise Portal Server. The UNIX command option [-f] itmcmd agent -f stop kf, allows you to stop the Eclipse Help Server unconditionally. On Windows systems, reconfiguration restarts all components. To reconfigure the Eclipse Help Server while the Tivoli Enterprise Portal Server is running, restart the Tivoli Enterprise Portal Server along with the Eclipse Help Server.

Non-root stopping or starting agents causes problems

You might experience issues while starting or stopping agents on servers, when using a non-root user ID. The following message might be received:

`KCIIN1191E Cannot execute` *`product_code`* `stop script.`

To avoid this situation, use the root account or an account with granted required permissions (itmuser group).

Root password is not accepted during non-root Tivoli Enterprise Portal Server configuration

While configuring the Tivoli Enterprise Portal Server, when using non-root user, the provided root password is not validated correctly. You should use root account or an account with granted required permissions (itmuser group).

Corba user exception is included in the Tivoli Enterprise Portal Server log when creating situations

When a user creates a new situation, the situation name must be unique. To verify that the new name is unique, the software attempts to access a situation by the new name. If the situation is found, then the name is already used and the user must select a new name. If the request fails, then the name is not already used. The failure to find the situation name is reflected in the log as the CORBA exception. The CORBA user exception indicates that the name is unique.

Stopping or starting the eWAS subcomponent of the Tivoli Enterprise Portal Server

The eWAS subcomponent of the Tivoli Enterprise Portal Server (TEPS), named Tivoli Enterprise Portal Server extension server (TEPS/e) is installed automatically with the Tivoli Enterprise Portal Server. If you need to start or stop the application server instance of eWAS on which the Tivoli Enterprise Portal Server is running, you must do it by starting or stopping the Tivoli Enterprise Portal Server. You cannot use the eWAS start and stop commands to control eWAS. Using the eWAS start and stop commands results in an internal error, indicated by `KFWITM392E Internal error occurred during login`. If you have already used the eWAS commands, see "Starting and stopping eWAS" in the *IBM Tivoli Monitorin Administrator's Guide* for recovery instructions.

Chapter 9. Tivoli Enterprise Monitoring Server troubleshooting

This section describes problems that might occur with the Tivoli Enterprise Monitoring Server and provides resolutions to recover from those problems. It includes the following sections:

Messages related to the index file are displayed when the agent fails back to a remote monitoring server

These messages indicate that the remote monitoring server was stopped forcefully (for example, when it crashes), but that the database is not corrupted. The messages help to ensure that even though the remote monitoring server stopped unexpectedly, no loss of data occurred, and that the database has been restored successfully.

A generic RPC communications error is received when issuing a long-running tacmd execute command

A generic RPC communications error is received when you issue a long-running **tacmd execute command** or **tacmd executeAction** command on an agent that is connected to a remote monitoring server. Agents directly attached to the hub monitoring server will not have this problem. When you run a **tacmd executecommand** or **tacmd executeAction** command on an agent that is attached to a remote monitoring server, and the command was issued with a the -t (timeout) option with a timeout value greater than 600 seconds (10 minutes), the command fails with a generic RPC communications error. The request does not incur a network or communication error, but is actually being terminated by the hub monitoring server when the response for the command is not returned within 600 seconds. However, the error returned to the TACMD indicates a communications error.

The default hub monitoring server behavior to timeout long-running remote requests is normally used to manage requests that have not returned within this time period, and also to indicate a network outage might have occurred, or that the remote monitoring server is down. However, this typical result is not the case for a long-running **tacmd executeAction** or **tacmd executecommand** where the command is still running at the endpoint, and the monitoring server is still online. If you intend to run commands that take longer than 600 seconds, you can set the KDS_SYNDRQ_TIMEOUT environment variable to run 60 seconds longer than the expected time for the command to complete. KDS_SYNDRQ_TIMEOUT is a monitoring server environment variable set only at the hub monitoring server. The variable can be set in the service console for dynamic update or in the monitoring server configuration file, which requires a hub recycle. This value can be set arbitrarily high.

Troubleshooting Tivoli Enterprise Monitoring Server problems on distributed systems

The problems described in this section might occur on distributed systems. For information about configuring the Tivoli Enterprise Monitoring Server, refer to the *IBM Tivoli Monitoring Installation and Setup Guide* .

The CT_GET request method fails in SOAP queries with a V6.2.3 hub monitoring server, a remote hub monitoring server earlier than V6.2.3, and an agent connected to a remote monitoring server

In an environment comprised of a V6.2.3 hub monitoring server, a remote monitoring server earlier than V6.2.3, and an agent connected to a remote monitoring server, the CT_GET request method fails in soap queries with the following error:

```
<xml version="1.0" encoding="UTF-8">
<SOAP-ENV:Envelope xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/"
 SOAP-ENV:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/">
<SOAP-ENV:Body>
<SOAP-ENV:Fault><faultcode>SOAP-ENV:Server</faultcode>
<faultstring>Unable to start request (67109066)</faultstring>
</SOAP-ENV:Fault></SOAP-ENV:Body></SOAP-ENV:Envelope>
```

To avoid this issue, install V6.2.3 application support files on the remote monitoring server. After you restart the remote monitoring server, the SOAP requests will work.

Exposure of passwords in the clear

Currently, all versions of IBM Tivoli Monitoring incorporating the IBM Tivoli Directory Server Client at the monitoring server are exposed to an unaudited security risk of exposure of passwords in the clear. To avoid displaying passwords in the clear when troubleshooting LDAP problems, use the following option:

```
LDAP_DEBUG=65519
```

Receive a seeding failed message

Before you seed a remote monitoring server, you must ensure that the hub monitoring server is running. However, if you receive this message, start the hub monitoring server, and then manually seed the support using the **itmcmd support** command.

High monitoring server CPU after restarting with Warehouse Proxy Agents configured

A remote monitoring server process incurs significant CPU utilization or percentage increases when any IBM Tivoli Monitoring Warehouse Proxy Agents have been started in the hub monitoring server environment. Due to an issue in the monitoring server KRANDREG module, the remote monitoring server can go into a loop making continuous calls to the IBM Tivoli Monitoring Global Location Broker facility. This loop can happen whenever the hub monitoring server Global Location Broker contains EXACTLY 50 entries relating to the IBM Tivoli Monitoring Warehouse Proxy Agent. The Global Location Broker is the hub monitoring server facility that shows which remote monitoring server or Warehouse Proxy Agents have been registered in this environment.

The total number of entries registered in the hub monitoring server Global Location Broker from the Warehouse Proxy Agent are a combination of the following amounts:

- The number of IBM Tivoli Monitoring network protocols configured for the Warehouse Proxy Agent (for example, IP.PIPE, IP.SPIPE).
- The number of network interface cards resident on any of the Warehouse Proxy Agent systems.
- The total number of Warehouse Proxy Agent that have been configured and connected to the hub monitoring server.

The following example of Global Location Broker entries for the Warehouse Proxy Agent is from a remote monitoring server RAS1 log when the remote monitoring server has the configuration parameters KDC_DEBUG=Y and KDE_DEBUG=Y set in its environment:

```
+4A8F0367.007D       object: 85f536a00000.02.0a.09.fe.31.00.00.00
+4A8F0367.007D         type: 85f532330000.02.0a.09.fe.31.00.00.00
+4A8F0367.007D    interface: 865fc14a0000.02.0a.09.fe.31.00.00.00
+4A8F0367.007D   annotation: Candle_Warehouse_Proxy
+4A8F0367.007D        flags: 0x2              addr-len: 16
+4A8F0367.007D        saddr: ip:#9.77.148.246[205]
```

In some cases, the "annotation" value of "Candle_Warehouse_Proxy" is not present, but the values for the object, type, and interface match those shown above. As an alternative to viewing the Global Location Broker entries using the RAS1 log, you can use the Manage Tivoli Enterprise Monitoring Servers workspace to view this information. After navigating to the Manage Tivoli Enterprise Monitoring Servers workspace, select the Protocols link for the hub monitoring server to view the global location broker entries. For further information about the Manage Tivoli Enterprise Monitoring Servers workspace, see the *IBM Tivoli Monitoring Tivoli Enterprise Portal User's Guide*.

Complete the following steps to address this issue:

1. Stop the hub monitoring server in your environment.
2. Make a configuration change that would alter the total number of Warehouse Proxy Agent Global Location Broker entries as described in items listed in the problem explanation. This might include the following steps:
   a. Stopping one of the running Warehouse Proxy Agents.
   b. Configuring and activating an additional Warehouse Proxy Agent.
   c. Adding or removing one or more network protocols (for example, IP.PIPE, IP) from a Warehouse Proxy Agent configuration.
3. Restart the hub monitoring server.
4. Restart the modified Warehouse Proxy Agents.

Upgrade inconsistency between the History and Object windows

The historical collections created in previous versions of IBM Tivoli Monitoring are not eligible to be members of a group in a later version of the software.

Attribute groups started for collection on the managed systems should not be available on the monitoring server list

Attribute groups can be started for collection on either the managed systems or the monitoring server, but not for both from the history collection configuration

window. When a collection setting that is started for collection on the managed system is grouped in a historical group, and then the historical group is distributed to a monitoring server, the collection is collected against the managed system and not the monitoring server.

Distribution to a monitoring server on the Object group editor is not equivalent to a monitoring server distribution in the historical collection configuration window.

To decrypt a password, KDS_VALIDATE_EXT='Y' is required

KDS_VALIDATE_EXT='Y' is required on a SLES 10 64-bit zLinux monitoring server to successfully decrypt a password sent by the portal server for validation. This operating system uses Pluggable Authentication Modules (PAM) and this monitoring server parameter for this purpose. For all other purposes, PAM is not supported by adding the parameter KDS_VALIDATE_EXT=Y to a monitoring server configuration.

Remote Tivoli Enterprise Monitoring Server consumes high CPU when large number of agents connect

In enterprise environments, a large number of agents can connect to a remote Tivoli Enterprise Monitoring Server in a short period of time. Examples of when this might occur are during startup of the Tivoli Enterprise Monitoring Server, or when agents failover from a primary to secondary Tivoli Enterprise Monitoring Server. In these cases, the amount of CPU processing is directly proportional to the total number of situations that have been distributed to agents connected to the remote Tivoli Enterprise Monitoring Server. For example, if there are 1000 agents connecting to the remote Tivoli Enterprise Monitoring Server, and each agent has an average of 20 situations distributed to it, the total number of situations distributed to agents connected to the remote Tivoli Enterprise Monitoring Server would be 20 thousand.

To minimize the amount of CPU processing when a large number of agents connect, consider reducing the total number of situations distributed by avoiding distribution of situations that are not being used. Some situations, including predefined situations, have the default distribution set as a managed system list. These situations are distributed to all managed systems in the managed system list, even if the situation is not being used. Limiting the distribution to only managed systems where the situation will be used minimizes the total number of situations distributed from the remote Tivoli Enterprise Monitoring Server, and minimizes the CPU processing when a large number of agents connect.

The distribution specification for a situation can be changed using the Situation editor or the **tacmd editsit** command.

Unable to start the Tivoli Enterprise Monitoring Server after the kdsmain process is terminated abnormally

When the kdsmain process is terminated abnormally, a stale cms process is left behind. This stale cms process prevents the proper startup of the Tivoli Enterprise Monitoring Server. The cms process should be killed first, and then a startup of the Tivoli Enterprise Monitoring Server should be retried for a successful startup. A restart of the Tivoli Enterprise Monitoring Server should be attempted only after verifying the `CMS.EXE` process is also terminated. A `CMS.EXE` left running in response to the earlier failure is likely to cause a subsequent start of Tivoli Enterprise Monitoring Server to fail.

THRESHOLDS.XML and Tivoli Enterprise Monitoring Server table not cleaned when managed system override is removed

Removing an existing managed system override definition by removing the managed system from a situation distribution list does not result in the override being removed from the Tivoli Enterprise Monitoring Server table and the `THRESHOLDS.xml` file on the agent.

You must first check to see if any override is associated with that particular managed system before removing it from the situation. If an override is found, remove it before the situation's distribution is modified.

Situations fail to trigger for attributes by applying group function

If you create a Situation with attributes (for example, 'Elapsed_Time' and 'Virtual Bytes for 'NT_PROCESS') and then apply the condition (MAX(Elapsed Time(Seconds))==*TRUE AND Virtual Bytes != 5, the created situation should be triggered and forwarded to Tivoli Enterprise Console server. However, the situation is not triggered. The Tivoli Enterprise Portal expects that the Tivoli Enterprise Monitoring Server should dynamically find the MAX row and then apply further conditions. This is not how column functions work

According to standard, grouping functions can only return the grouping function results and any columns used in the grouping. This predicate is looking for a single row, but a grouping function is an aggregate of the grouped rows.

Tivoli Enterprise Monitoring Server application support will complete all seeding functions but may crash as the program is exiting

The Tivoli Enterprise Monitoring Server seeding program that adds Tivoli Enterprise Monitoring Server application support completes all seeding functions, but may crash as the program is exiting. This crash has only been observed rarely during product testing. The IBM Tivoli Monitoring configuration tool checks the output produced by the seeding functions, and it reports that the Tivoli Enterprise Monitoring Server application support was added successfully. Since all seeding functions were completed, the Tivoli Enterprise Monitoring Server tables with application support are correct and not corrupted.

A core or dump file might be created during the program crash. Creation of a core or dump file usually depends on if the system has been configured to save crash information. However, even if the system is configured to save crash data, this particular crash might not produce a core or dump file.

The Tivoli Enterprise Monitoring Server seeding output files contains information about the crash. An operating system message indicates the condition that caused the crash. A sample crash message would be:

```
 signal 11(SIG1_SIGSEGV=29) 0B000000000000000100000000000000F84CD256887CAE56E8F
400570000000048010000EE5DB656B88B9655A4F700572200000022000000000000000D8F900572C
F800578C81C056ACEF0057C04DD256484DD2563EB4B656C04DD2560000000000F5005701
0000000000000020000000020000000879D8B558C81C056A8EF0057
```

The expected seeding completion messages will follow the crash message. The normal seeding messages are checked by the IBM Tivoli Monitoring configuration

tool for successful completion of all seeding functions. The crash message always appears in the Tivoli Enterprise Monitoring Server seeding output even if a core or dump file is not produced.

Tivoli Enterprise Monitoring Server seeding output files are stored in different files on UNIX and Windows systems.

UNIX examples:

```
$ITM_HOME/logs/Node_ci_query_Process_ID.log
    $ITM_HOME/logs/Node_ci_query_Process_ID.log
```

where :

Node The system host name

Process_ID
The program process ID

Windows example:

```
C:\IBM\ITM\CNPS\logs\seedApp.log
```

where:

App The 3-character product code, such as knt for the Monitoring Agent for Windows OS

The exact cause of the Tivoli Enterprise Monitoring Server seeding program crash has not been determined. The program has finished all seeding functions and is exiting. The crash has only occurred when only a few seeding changes are required. Seeding functions making many updates to the Tivoli Enterprise Monitoring Server tables have never resulted in this type of program crash. It is very possible that there is something unique about the system where this crash has been seen. The crash has only been observed on one internal test system, which was a Linux for AMD (Opteron) system.

tacmd login fails when monitoring server is configured with LDAP authentication

Set the monitoring server tracing and LDAP client-side tracing on the hub monitoring server:

```
KBB_RAS1=ERROR (UNIT:kdslg ALL) (UNIT:kdsvl ALL) (UNIT:kgllg ALL) (UNIT:kglld ALL)
```

UNIX or Linux systems

Run the following commands on the system hosting the UNIX or Linux hub monitoring server:

1. export LDAP_DEBUG=65535
2. export `LDAP_DEBUG_FILE=/opt/IBM/ITM/logs/ldaptrace.txt` (or whatever path/file you want)
3. rm `/opt/IBM/ITM/logs/ldaptrace.txt` (to remove the file before restarting the Hub)

Restart the hub monitoring server. Note that these LDAP-related trace settings remain active until the monitoring server is restarted from a shell session where the variables are not exported. If the monitoring server is restarted from the same session where these variables are still exported, then the settings will be active again after restart.

Reproduce the problem. As you reproduce it, any LDAP requests add trace content to that `ldaptrace.txt` file.

Retrieve that `ldaptrace.txt` file, and the hub monitoring server log files. The hub monitoring server logs will show any possible failures that occur leading up to the calls to the SOAP server. The `ldaptrace.txt` file will show any activity and possible failures occurring when it actually binds to the SOAP server and attempts to lookup users.

Windows Systems

Windows systems use the same KBB_RAS1 trace settings as UNIX and Linux systems, but enabling the additional LDAP trace requires a different procedure. From the Manage Tivoli Enterprise Monitoring Services (MTEMS) GUI, complete the following steps:

1. Stop the monitoring server.
2. Right-click the entry for the monitoring server, and select **Advanced... -> Edit Variables...**.
3. In the Override Local Variable Settings window that appears, click **Add**. Enter `LDAP_DEBUG` for the Variable, and `65535` for the value, and click **OK**.
4. Click **Add** again and enter `LDAP_DEBUG_FILE`for the Variable, and any path or file that you wish (for example, C:\temp\ldaptrace.txt). Then click **OK**.
5. Click **OK** to save the changes.
6. Start the monitoring server. New login and LDAP-related monitoring server activity is now logged in the LDAP_DEBUG_FILE.

When you are finished reproducing the problem and want to stop tracing, go back to the Manage Tivoli Enterprise Monitoring Services (MTEMS) GUI and complete the following steps:

1. Stop the monitoring server.
2. Right-click the entry for the monitoring server, and choose **Advanced...-->Edit Variables...**.
3. Highlight the variables and click **Delete** to delete both the LDAP_DEBUG and LDAP_DEBUG_FILE variables. Then click **OK** to save the changes.
4. Start the monitoring server.

Some agents are displayed in the Service Console list that are not accessible from that user interface

For instance, if you click **IBM Tivoli M5 Agent Service Interface**, a popup is displayed for the User Name and Password. There is no valid user name and password combination that will work, and you must click **Cancel** to get out of this page. Other agents do not have this problem.

tacmd login fails after hub monitoring server is recycled

The tacmd login process uses SOAP to interface with the hub monitoring server validation process. SOAP runs with the monitoring server process and also with the IBM Tivoli Monitoring internal web server. All usually run in the same process during a normal startup. The IBM Tivoli Monitoring internal web sever process runs on the first IBM Tivoli Monitoring process started up. If that first process stops, the web server swaps to another IBM Tivoli Monitoring process. The web server supports the service console and port forwarding logic as well as SOAP.

When the monitoring server is stopped, the internal web server swaps to another IBM Tivoli Monitoring process such as an OS Agent. When the monitoring server starts again, the monitoring server and SOAP are running, but the internal web server is not in the same process. You can determine which process is running the internal web server by starting a browser session to the service console http://server:1920. Ensure the browser View/Status is checked, and then move the cursor over each link. The port involved will be seen in the status line like this:

```
Service Point: cnp
-> IBM Tivoli Monitoring Service Console
-> IBM Tivoli Enterprise Portal Web Client
Service Point: nmp180_hd
-> IBM Tivoli Monitoring Service Console
```

In this case the cursor was on the service console link under "Service Point: nmp180_hd" and that was the process running the internal web server.

If a firewall rule is in place between the **tacmd login** process and the server running the hub monitoring server and SOAP, the **tacmd login** command might fail. The **tacmd** logic attempts to use the base port connected with the "IBM Tivoli Monitoring Web Services" link. If that is unavailable, it uses the 1920 port. That will fail if the 1920 process is not the same as the monitoring server process.

If this condition occurs, it can be resolved by stopping all IBM Tivoli Monitoring processes on that server, starting the hub monitoring server, and then starting up the rest of the IBM Tivoli Monitoring processes. When things are running again, the tacmd login begins to operate as expected.

tacmd and SOAP are not able to connect

If two instances of the Hub Tivoli Enterprise Monitoring Server are started under different user IDs (root plus one other), tacmd and SOAP are not able to connect. When the problem occurs, it is usually in the presence of another process such as the IBM Tivoli Monitoring Universal Agent or the Monitoring Agent for Unix OS. When the problem occurs, both instances of the Hub Tivoli Enterprise Monitoring Server are listed on the "IBM Tivoli Monitoring Service Index" web page that is produced on port 1920. The tacmd and SOAP interfaces use the service index as part of their communications, and the extra Hub Tivoli Enterprise Monitoring Server entry disrupts them from communicating at all.

When the problem occurs, make sure the Hub Tivoli Enterprise Monitoring Server started under the non-root login is not running. Then recycle whichever process shows up first on the Service Index page.

The system crashes when attempting a bulk import or export command

You might be attempting to import from a 0-byte XML file. Ensure that the XML file has content. Also, this can also occur if the file contents are corrupted (if some expected XML elements are missing).

The Tivoli Enterprise Monitoring Server fails to start, but then does after a reboot

When your Tivoli Enterprise Monitoring Server does not start up properly and you see the following messages in the Tivoli Enterprise Monitoring Server logs, you need to check if anything is using the location server/broker (default is port 1918):

```
(4703AF9A.002B-4:kdcsuse.c,99,"KDCS_UseFamily") status=1c010005,
"cant bind socket", ncs/KDC1_STC_CANT_BIND_SOCK
(4703AF9A.002C-4:kdebpap.c,125,"KDEBP_AssignPort")
ip.pipe bound to port 14206: base=1918, limit=1918 (4703B06C.0000-
4:kdcc1sr.c,562,"rpc__sar")
Endpoint unresponsive: "ip.pipe:#9.42.22.26:1918", 1C010001:1DE0000F, 210, 5(2),
FFFF/1, 1.1.1.9, d7273a (4703B06F.0000-4:kdcl0cl.c,129,"KDCL0_ClientLookup")
status=1c020006, "location server unavailable", ncs/KDC1_STC_SERVER_UNAVAILABLE
(4703B08F.0000-
4:kdcc1sr.c,562,"rpc__sar") Endpoint unresponsive: "ip:#9.42.22.26:1918",
1C010001:1DE0000F, 32, 5(2), FFFF/2, 1.1.1.9, d7273a
(4703B092.0000-4:kdcl0cl.c,129,"KDCL0_ClientLookup") status=1c020006,
"location server unavailable", ncs/KDC1_STC_SERVER_UNAVAILABLE
```

You can find out what is using that port, stop the process, and then configure your system to use another port. You can also reboot the system to clean up any stale IBM Tivoli Monitoring processes that might be bound to this port.

Remote Tivoli Enterprise Monitoring Server lost connection to the hub Tivoli Enterprise Monitoring Server and all agents display offline

Check the log for error messages in the RAS1 trace log that indicate timestamp problems such as `Ignoring invalid lastTimeStamp`. This error occurs because you synchronized the time on the hub and remote Tivoli Enterprise Monitoring Server with another time server. Restart the Tivoli Enterprise Monitoring Server experiencing the errors because timers and POSIX (timed waits, for example) depend on reliable system time.

After the set timeout, the Tivoli Enterprise Monitoring Server is still pending

When you attempt to stop or start the Tivoli Enterprise Monitoring Server service, after the set timeout, the Tivoli Enterprise Monitoring Server is still pending the start or stop. You will receive the following error:

```
TEMS service is still pending start/stop. Check ITM documentation for more details.
```

The default time for starting and stopping a Tivoli Enterprise Monitoring Server service is ten minutes. In the following two situations, this time can be ten times as long:

1. If you have a large or complicated infrastructure connected to the Tivoli Enterprise Monitoring Server.
2. If you have a remote Tivoli Enterprise Monitoring Server, but the hub Tivoli Enterprise Monitoring Server is offline.

In any other situation, call IBM Software Support.

Providing the wrong path to configuration files during LDAP configuration causes the Tivoli Enterprise Portal login window to hang

During Security and LDAP configuration at Tivoli Enterprise Monitoring Server, if you provide an incorrect path to the `key.kdb` and `key.sth` files, the Tivoli Enterprise Portal login window goes into an indefinite loop. This occurs after restarting the Tivoli Enterprise Monitoring Server and launching the Tivoli

Enterprise Portal client. Ensure that the provided paths are correct during configuration. The installer does not check if the file exists under the user-provided path.

Crash on Linux remote Tivoli Enterprise Monitoring Server during hub failover to Hot Standby

The monitoring server can use a large number of file descriptors, especially in a large environment. On UNIX and Linux systems, the maximum number of file descriptors available to a process is controlled by user limit parameters. To display the user limits, run the following command:

```
ulimit -a
```

The "nofiles" parameter is the number of file descriptors available to a process. For the monitoring server process (kdsmain), the "nofiles" parameter should be set larger than the maximum number of agents that will be connecting to the monitoring server. If the monitoring server is unable to get file descriptors when needed, unexpected behavior can occur, including program failures. Consider increasing the value to 1000 file descriptors or more.

There are other user limit parameters that control how much data, stack and memory are available to a process. For large environments, consider increasing these memory-related user limit parameters for the monitoring server (kdsmain) process.

Configuring the user limit parameters usually requires root access, and involves changing system startup files which are operating system specific. Consult the operating system manuals for information on how to configure the user limit parameters.

HUB Tivoli Enterprise Monitoring Server quiesce prevents the display of the data collected by the attached Tivoli Enterprise Monitoring Agents

A HUB Tivoli Enterprise Monitoring Server has been running. A shutdown of the Tivoli Enterprise Monitoring Server and Tivoli Enterprise Monitoring Agents on the remote systems is in process, but the shutdown takes awhile due to abends in the remote Tivoli Enterprise Monitoring Server. About 8 or 9 minutes go by before the HUB Tivoli Enterprise Monitoring Server quiesces. There are a lot of remote request communication messages in the HUB's RKLVLOG prior to the QUIESCE, but no other signs of errors until after the abend. You cannot restart the remote environments following the quiesce, until after the HUB environment is recycled.

The value of the MINIMUM parameter within the KDSSYSIN member of the RKANPARU library might need to be increased if the STGDEBUG(X) or STGDEBUG(Y) parameter is also supplied within KDSSYSIN. If the address space controlled by this KDSSYSIN member enters a "storage quiesce" state (indicated by a KLVxxxxx message stating that there is a storage shortage or quiesce in effect), you should increase the value of the MINIMUM parameter and restart the address space.

During installation of a remote Tivoli Enterprise Monitoring Server on a Windows system, the agent support is applied, but fails

In a multiple-level Tivoli Enterprise Monitoring Server environment, the remote Tivoli Enterprise Monitoring Servers obtain their agent support from the hub Tivoli Enterprise Monitoring Server. In order to apply agent support to a remote Tivoli Enterprise Monitoring Server, the hub Tivoli Enterprise Monitoring Server must be running and reachable by the remote Tivoli Enterprise Monitoring Server.

During installation of a remote Tivoli Enterprise Monitoring Server on a Windows system, the agent support is typically applied. This fails if the hub Tivoli Enterprise Monitoring Server is unreachable.

During remote Tivoli Enterprise Monitoring Server installation on the Windows platform, ensure the hub Tivoli Enterprise Monitoring Server is running.

Using a Deploy Group with addSystem or updateAgent commands

When using a deploy group with **addSystem** or **updateAgent** commands, remote deploy might fail to locate the existing Managed System Name for some hosts. Message received:

```
KDY0012E:  The target target_hostname is incorrect or is offline.
The command did not complete because the value for the
target is incorrect or the target is offline.
```

This message normally indicates that the OS agent is not online. If the agent is, in fact, online, cancel current operations to this node:

```
# tacmd cleardeploystatus  -h hostname
```

Then issue the operation directly by using the Managed System Name parameter (instead of the deploy group):

```
# tacmd updateAgent  -t product_code -n managed_OS
```

Tivoli Enterprise Monitoring Server requires restart if you issue itmcmd server stop/start commands when you are already logged on

When you are logged in but restart the Tivoli Enterprise Monitoring Server using **itmcmd server** stop or start commands, you receive the message: KUICLR099E: The command did not complete because of a system error. Refer to the log for details and contact the system administrator.

A new login solves the problem and enables the **tacmd listsystems** command.

Log indicates Hub Tivoli Enterprise Monitoring Servers are down when they are up

The statusPut process fails periodically, resulting in an incorrect hub status. This condition is harmless and does not cause any operational change by the software. The following is an example of the log:

```
Tue Jun 14 04:27:01 2005 KO41039    Error in request sqlRequest. Status= 1103.
Reason= 1103.
(42AEA2E5.0011-6:ko4sndrq.cpp,855,"IBInterface_sqlRequest") Distributed request
failed
```

```
(42AEA2E5.0012-6:ko4state.cpp,3519,"IBInterface_sendInsert") send insert has no
request handle error
(42AEA2E5.0013-6:ko4ibput.cpp,1407,"IBInterface:insertProcessing")
General error <1103>
(42AEA2E5.0014-6:ko4ibput.cpp,1657,"IBInterface::put_sList")
table put error <1103>
(42AEA2E5.0015-6:ko4ibstr.cpp,1139,"IBStream::insertDef") IB Err: 1103
(42AEA2E5.0016-6:ko4crtsq.cpp,5547,"IBInterface_refreshIB") Hub is not there
(42AEA2E5.0017-6:ko4crtsq.cpp,5547,"IBInterface_refreshIB") Hub is not there
(42AEA2E5.0018-6:ko4crtsq.cpp,5547,"IBInterface_refreshIB") Hub is not there
(42AEA2E5.0019-6:ko4crtsq.cpp,5547,"IBInterface_refreshIB") Hub is not there
(42AEA2E5.001A-6:ko4crtsq.cpp,5547,"IBInterface_refreshIB") Hub is not there
Tue Jun 14 04:27:01 2005 KO41034    Monitoring for situation UADVISOR_OMUNX_SP2OS
ended.
(42AEA2E5.001B-6:ko4crtsq.cpp,5547,"IBInterface_refreshIB") Hub is not there
Tue Jun 14 04:27:01 2005 KO41036    Monitoring for situation UADVISOR_OMUNX_SP2OS
started.
(42AEA3C3.0000-6:kdssqrun.c,2995,"Fetch") QueryRowset error. status 302
Tue Jun 14 04:30:43 2005 KO41039    Error in request Notify. Status= 1105.
Reason= 302.
(42AEA3C3.0001-6:ko4async.cpp,4744,"IBInterface::completeRequest") Close failed
request <55BE90>
(42AEA53C.0000-6:ko4ibstr.cpp,1090,"IBStream::insertDef")
Ret code 155 indicates hub connection lost.
  Attempting to switch hubs o
r reconnect.
(42AEA53C.0001-6:kdcgbin.c,118,"KDCG_Bind") Using GLB at ip:#9.48.157.26[1918]
(42AEA53D.0000-6:ko4crtsq.cpp,6456,"IBInterface::restartAllObjects")
No access list records changed
(42AEA53D.0001-6:ko4mxque.cpp,97,"MutexQueue::~MutexQueue") Reply store <FC0798B8>
still associated with request <503D98>: info.re
ply <FC0798B8> info.oType <5546> info.oName <INSERTO4SRV.TNODESTS> info.sitName
<*noname*>
info.reqState <-1> info.physicalIO <1>
info.logIt <0> info.reqGen <412>
Tue Jun 14 04:37:01 2005 KO41034    Monitoring for situation UADVISOR_OMUNX_SP2OS
 ended.
Tue Jun 14 04:37:02 2005 KO41036    Monitoring for situation UADVISOR_OMUNX_SP2OS
started.
(42AEA61B.0000-6:kdssqrun.c,2995,"Fetch") QueryRowset error. status 302
Tue Jun 14 04:40:43 2005 KO41039    Error in request Notify. Status= 1105.
Reason= 302.
(42AEA61B.0001-6:ko4async.cpp,4744,"IBInterface::completeRequest")
Close failed request <61D5E0>
```

The Platform view in the Manage Tivoli Enterprise Monitoring Services panel shows the Tivoli Enterprise Monitoring Server as running as a 32 bit application, but my agents are shown as running as 64 bit applications

The Tivoli Enterprise Monitoring Server is a 32 bit application that runs on both 32 and 64 bit operating systems.

Tivoli Enterprise Monitoring Server does not release memory after running a large SQL query

Running a query for data beyond a 24-hour period consumes high CPU and memory because the data is not stored on the server and must be retrieved from the endpoints. All users might experience low system performance while a large amount of data is retrieved from endpoints.

SQL queries with more than 200 OR predicates do not complete

If an SQL query to the hub monitoring server contains more than 200 OR predicates, a limit is reached and the query does not complete. An example of this is if the **tacmd listSystems** command is run specifying a remote monitoring server that contains universal agents that contain more than 200 subnodes, the query will OR together all of the subnodes.

Tivoli Enterprise Monitoring Server aborts unexpectedly when exiting the telnet session used to start it

A UNIX-based systems Tivoli Enterprise Monitoring Server aborts unexpectedly when exiting the telnet session used to start it, either from the client or the command line. If you start the Tivoli Enterprise Monitoring Server from a Bourne shell, the Tivoli Enterprise Monitoring Server session terminates when you exit the telnet session. Do the following so you can exit the telnet session without shutting down the Tivoli Enterprise Monitoring Server.

1. Enter the Korn shell (ksh).
2. Start Tivoli Enterprise Monitoring Server.

KCIIN0084E Timeout appears while waiting for Tivoli Enterprise Monitoring Server to start on AIX 5.3

After installation the Tivoli Enterprise Monitoring Server and Remote Tivoli Enterprise Monitoring Server performance is very slow.

Confirm that the prerequisite software has been installed. The C libraries are critical for the Tivoli Enterprise Monitoring Server performance at start and stop times and are important for communication between Tivoli Enterprise Monitoring Server and Tivoli Enterprise Portal Server.

The installation should check the prerequisites and show information in one of the logs, such as the candle installation log or the Tivoli Enterprise Monitoring Server log. If one of the prerequisites is missing the installation will not continue automatically.

Troubleshooting Tivoli Enterprise Monitoring Server problems on z/OS systems

This section includes describes problems you might experience with Tivoli Enterprise Monitoring Server on z/OS and provides resolutions. It covers problems that occur during run-time that you can resolve with the Installation and Configuration Assistance Tool (ICAT). For more information about configuring the Tivoli Enterprise Monitoring Server on z/OS, refer to the *Configuring Tivoli Enterprise Monitoring Server on z/OS* manual.

Receive Program KDFCINIT and Program FAXCMON messages

"Program KDFCINIT with task id 8 ended" and "Program FAXCMON with task id 7 ended" messages are generated in the IBM Tivoli Monitoring z/OS Tivoli Enterprise Monitoring Server RKLVLOG if either or both IBM Tivoli OMEGAMON XE on z/OS and OMEGAMON XE for Storage on z/OS are running in the

monitoring server address space. These are informational messages that report on internal task terminations which in turn help identify non-terminating internal tasks. These messages are benign.

The Tivoli Enterprise Monitoring Server start task (CANSDSST default) encountered error message 'KLVST044 LOADLIST MEMBER NOT FOUND IN RKANPAR DATASET (KDSLLIST) KppLLIST KLVST001 CANDLE ENGINE INITIALIZATION ERROR(S), ABEND U0012' in the RKLVLOG at startup

The Tivoli Enterprise Monitoring Server start task (CANSDSST default) encountered error message "KLVST044 LOADLIST MEMBER NOT FOUND IN RKANPAR DATASET (KDSLLIST) KppLLIST KLVST001 CANDLE ENGINE INITIALIZATION ERROR(S), ABEND U0012" in the RKLVLOG at startup. Ensure the following conditions:

- The pp#2xxxx RTE Load job ran successfully for this RTE:
  1. To perform the RTE Load, place the L option next to the RTE on the KCIPRTE RTE main menu. The Configuration tool generates the pp#2xxxx RTE Load job.
  2. Submit the RTE Load job. The RTE Load job populates the &rhilev.&RTE.RK* runtime libraries by copying required elements from the SMP/E target high-level qualifiers (&thilev.TK*).
- If the RTE Load job was performed, then the job references the &thilev.TK* SMP/E target datasets from where the members are copied. Ensure the datasets are correct SMP/E target datasets where &svhilev.CSI is installed.
- If the RTE Load job does not reference any &thilev.TK* SMP/E target datasets or generates an incomplete RTE Load job, then ensure that the Configuration tool references the correct SMP/E target high-level qualifiers. The Configuration tool only generates appropriate IEBCOPY TK*-->RK* steps for SMP/E target datasets that it can access.

Use the following steps to ensure that the Configuration tool references the correct SMP/E target high-level qualifiers:

1. From the Configuration tool main menu, select **Install products or maintenance** > **Set up product or maintenance environment** >**Specify environment information**.
2. Verify that the values for the high-level qualifiers are correct. If the high level qualifiers values are not the correct, use the following steps to unlock the SMP/E high-level qualifiers:
   a. Run &shilev.INSTLIB.
   b. On the Installation tool main menu, select **Services and utilities** > **Unlock SMP/E high-level qualifiers**.
   c. Specify **Y** on the **Unlock SMP/E high-level qualifiers?** field.
   d. Edit the high-level qualifier modifications on the **Specify installation environment information** panel.
3. Go to the RTE main menu and regenerate the RTE Load job.

If the zOS CT/Engine stops, the Tivoli Enterprise Monitoring Server must be recycled

If anything causes the zOS CT/Engine to stop, then the Tivoli Enterprise Monitoring Server must be recycled. The problem that caused the stoppage also needs to be addressed.

KDS Parameters not generated from the batch parm deck

If you try to clone an RTE through Create Batch Mode parameters processing KDS variables (for example, KDS_CMS_TYP) are not generated in the output. A possible workaround is to manually add the missing parameters.

The problem is that the KCITVARS ISPF table is out of order. The procedure to sort the table is:

1. Back-up INSTDATA.
2. In TKANCUS, create a CLIST called XSORT. The contents will be as follows:

```
====================================================
PROC 0
SET SORTLIST = &STR(CIGPRF,C,A,CIGPRD,C,A,CIGVAR,C,A)
  ISPEXEC TBOPEN KCITVARS WRITE SHARE  ISPEXEC TBSORT KCITVARS FIELDS(&SORTLIST)
  ISPEXEC TBCLOSE KCITVARS PAD(30)  EXIT CODE(0)
  ====================================================
```

3. Invoke ICAT.
4. On the ICAT main menu, select **Configure products->Services and utilities->Execute a CLIST in the TKANCUS library** option.
5. On the next panel, specify XSORT as the Name. Ensure that the panel displays a "Completion Code = 0" message after this CLIST is invoked.
6. Navigate to the RTE main menu and regenerate the batch parameter member for RTE=SYP1. Ensure that all the applications are now generated.

Cannot encrypt text. A call to CSNBSYE failed. Cannot encrypt contents of keyfile

On the **Specify configuration values** option on the "Configure the Tivoli Enterprise Monitoring Server main menu, you can provide the Integrated Cryptographic Service Facility (ICSF)-related values for password encryption. These values generate the KAES256 step in the Tivoli Enterprise Monitoring Server "Create runtime members" job. To create the encryption key file (KAES256) in the &rte.RKANPAR library. If within this step, the error occurs, this message indicates that ICSF is not configured correctly in your system. Consult with your system administrator. Refer to the *Configuring Tivoli Enterprise Monitoring Server on z/OS* manual for more information about configuring a z/OS Tivoli Enterprise Monitoring Server and the security-related information.

The error "KLVST005 MVS JOBSTEP AUTHORIZATION REQUIRED KLVST001 CANDLE ENGINE INITIALIZATION ERROR(S), ABEND U0012 CSV019I - Required module KLVSTWTO not accessed, it is not APF Authorized (RKANMODL) CSV028I - ABEND 306-0C" occurs in the z/OS Tivoli Enterprise Monitoring Server RKLVLOG during startup

Ensure that the load libraries, including RKANMOD and RKANMODL are correctly APF-authorized. Additionally, in the Configuration tool **Complete the configuration** step, specify that any runtime libraries concatenated in the STEPLIB

DDNAME and in the RKANMODL DDNAME of the Tivoli Enterprise Monitoring Server started task must be APF-authorized.

The error "KLVSQ000 carved mode in effect for extended storage" occurred in the RKLVLOG during startup

You can increase the MINIMUM() storage settings in the &rhilev.&rte. RKANPAR(KDSSYNSIN) member if IBM Support personnel instructs you to do so. The default value for the MINIMUM() parameter is MINIMUM(150000,X). Use the following steps to increase this value or any other storage-related parameters:

1. On the **Configure the Tivoli Enterprise Monitoring Server** main menu, select the **Specify configuration values** option.
2. On the next panel, navigate to the **F5=Advanced** key.
3. Do the following on the **Specify Advanced Configuration Values**:
   - Edit the **Minimum extended storage** field to 300000 K.
   - Edit the **Maximum storage request size** fields to 16 (Primary) and 23 (Extended).
4. On the **Configure the Tivoli Enterprise Monitoring Server** main menu, select the **Create runtime members** option to generate the DS#3xxxx Create runtime members job. Submit the job and verify good condition codes.
5. Recycle the Tivoli Enterprise Monitoring Server.

Error message 'KDSMA013 OPEN VTAM for VDM1APPL failed with status 8' occurs in the Tivoli Enterprise Monitoring Server start task (CANSDSST default)

Error message "KDSMA013 and the task ends in "ABEND=S000 U0200 REASON=00000000 KDSMA003 Tivoli Enterprise Monitoring Server data collection server ended successfully". Ensure the following:

1. The KDS_VTAMID= parameter exists in the &rhilev.&rte.RKANPAR(KDSENV) member. If it does not exist, then ensure that the Tivoli Enterprise Monitoring Server is configured correctly. Refer to the "*Configuring Tivoli Enterprise Monitoring Server on z/OS* manual for more information about configuring a z/OS Tivoli Enterprise Monitoring Server.
2. If the KDS_VTAMID= VTAM APPLID exists, ensure that the Tivoli Enterprise Monitoring Server VTAM major node is activated correctly.

For more information, review the **Complete the configuration** option on the **Configure the Tivoli Enterprise Monitoring Server** main menu.

Chapter 10. Monitoring agent troubleshooting

This chapter describes problems you might experience with the monitoring agent deploy tool and monitoring agents. If you do not find the resolution to a problem you experience with a monitoring agent, refer to the agent-specific user guide listed in"IBM Tivoli Monitoring library" on page 291 section of this book.

Memory leak on Solaris OS during khdxprtj process causes applications to hang

The Oracle JDBC driver version V10.2.0.3.0 causes an application to hang when it tries to acquire a connection to the database. The most common symptoms affecting the Summarization and Pruning agent or Warehouse Proxy Agent are:

- lack of Tivoli Enterprise Portal responsiveness
- agent upload failures for Warehouse Proxy Agent
- increased memory usage over time
- rejecting a shutdown command

To resolve this issue, upgrade the JDBC driver to a newer level (at least V10.2.0.5.0 or later).

Local history migration tools move the agent operation logs to multiple agent history locations

If you upgrade your TEMS and TEPS after configuring historical data collection in your previous environment, the local history migration tools move the agent operation logs, OPLOG and OPLOG.hdr, into multiple agent history locations. The following files are common files and may appear in multiple directories: khdexp.cfg, OPLOG, OPLOG.hdr, KRAMESG, and KRAMESG.hdr. Only the agent that records into the specific directory will record history into the file. The other agents will record history information into their respective directories.

Unreadable tool tip information for Available EIF Receivers list of the Situation editor

When you select the **EIF** tab of the Situation editor, you might notice an unreadable tool tip in the Available EIF Receivers list. The problem is caused by bad data in the TEXT column of the EVNTSERVER table. The problem has been corrected. However, you might still experience this problem if the default event destination (id=0) on the zOS TEMS has not been updated since the problem was fixed.

To correct the problem, delete the default event destination entry (for example, id=0) and recycle the hub TEMS. This will cause the Event Forwarder to rebuild the default event destination entry in the EVNTSERVER table and the tool tip will display correctly.

Unable to configure the Warehouse Proxy agent with modified parameters from the Tivoli Enterprise Portal GUI

In an environment with an OS agent and the Warehouse Proxy agent, your attempt to modify the Warehouse Proxy agent parameters from the Tivoli Enterprise Portal GUI might result in the following message:

```
KDY1024E: The agent failed to respond to the command command did
not start or stop agent.
```

This message indicates that the configuration attempt failed. For example, after you specify "Run As User" for an agent, this value cannot be cleared back to not having "Run As User" because the code that triggers updates is based on a value being set for a property. In this case, you are trying to unset a property by not passing a value. To avoid this issue, supply the same user name for the WPA agent as you have for the OS agent (typically, root or Administrator).

Self-describing agent overwrites most recent manually installed z/OS TEMS support

An older version of a self-describing agent might overwrite the most recent version of TEMS application support that is manually installed on z/OS TEMS. The most recent version of the TEMS application support is not installed through the self-describing mechanism . To resolve this issue, disable self-describing mode on the agent side with the older application support and reseed the z/OS TEMS with the most recent version of application support or use self-describing mechanism to install the new TEMS support across your environment.

32-bit Agent Builder agent will not start on 64-bit Windows with System Monitor Agent-installed OS Agent

A System Monitor Agent must not be installed into a system where existing IBM Tivoli Monitoring components (including other monitoring agents) are already installed, with this exception: Agents built with Agent Builder V6.2.2 or subsequent may be installed alongside a System Monitor Agent, provided they run in the same mode as the Windows System Monitor Agent. If the Windows agent runs in 32-bit mode, only 32-bit Agent Builder agents are supported; if the Windows agent runs in 64-bit mode, only 64-bit Agent Builder agents are supported. 32-bit Agent Builder agents can be regenerated using Agent Builder to create 64-bit Windows binaries that you can install with the 64-bit Windows System Monitor Agent.

Unable to locate the file name of an exported situation that begins with numerals

Situations created with a name starting with a numeral are stored with a full name based on your input and a situation name generated by the system. The situation name is comprised of the letter Z followed by numerals. When you export situations using the **bulkexport sit** command, the situations are exported by situation name. The full name is stored inside the xml exported file. To avoid losing track of your exported situations, do no use numerals to begin situation names.

Tivoli Enterprise Portal data for UNIX OS and Linux OS agents is not updated after stopping the disk

For the UNIX OS and Linux OS agents, the Tivoli Enterprise Portal data is not updated after stopping the disk. The Tivoli Enterprise Portal Server provides GPFS data gathered by AIX OS *df* command. Data gathered by the *mmdf* command might conflict with the data displayed within a Tivoli Enterprise Portal view.

Unable to view data for a default query in a workspace

A default query should display data when it is assigned to the view on the workspace. However, if this is a view that has links, a link must be selected in order to see the data in the workspace.

Testing the connection to the Tivoli Data Warehouse database is valid even with an invalid password

A test of the connection shows that the connection to the Tivoli Data Warehouse database as valid even if the password is incorrect. The first *N* characters of the password entered in the Warehouse Proxy Agent and the Summarization and Pruning Agent configuration are actually used, where *N* is the password length defined in the operating system. Any trailing characters are ignored, even though the password is incorrect.

This behavior is true for ODBC, JDBC, and for DB2, using an OS user. This behavior is not true for MSSQL or Oracle, not using an OS user, but rather a DB user.

Linux OS agent fails to start

On some Linux systems (SUSE 10, Linux Itanium) there is a problem with OS Agent operation after deployment. The current workaround is to use the -o KDYRXA.AUTOCLEAN=NO option when executing the **tacmd createnode** command to deploy the OS agent to a remote node. This option places the transferred installation image in the system temporary directory on the remote node.

Configured non-root user agent starts up as root

After configuring the agent to run as non-root, whenever it is restarted, the agent restarts as root. This is a present issue with the Solaris operating system.

Large historical collections slow monitoring agents

If historical collection is turned on for an attribute group, it can produce a large volume of data. Either turn off historical collection for the attribute group, or set the pruning for the attribute group to 1 hour to avoid long-term problems.

Unable to access History Collection Configuration for any agent

You are unable to access History Collection Configuration from the Tivoli Enterprise Portal for any agent, and you receive the following message:

```
Cannot Load Product Configuration Data
```

If you find that the Tivoli Data Warehouse database does not contain a WAREHOUSEPRUNE table, and if in the portal server database the KFWWHISTDATA table has been renamed KFWWHISTDATABAK, rename the KFWHISTDATABAK table to KFWWHISTDA in the portal server, and then reconfigure the warehouse. The WAREHOUSEPRUNE table will then be in the Tivoli Data Warehouse database, and the issue will be resolved.

Agent names and icons are displayed incorrectly

When installing portal server support from images older than v6.2.2, the support installation might fail with no symptom, leading to names and icons related to the agent being displayed incorrectly in the Tivoli Enterprise Portal. If this occurs, reconfigure the portal server in the Manage Tivoli Enterprise Monitoring Services window by right-clicking the portal server entry, and then clicking **Reconfigure**.

64 bit monitoring agents are not started

If a monitoring agent is installed as an "Agent Template," an instance needs to be created before the agent can be started. For instance, you install and start a v6.2.2 Fix Pack 1, 64-bit monitoring agent and perform a local installation of a pre-v6.2.2 Fix Pack 1 agent template, for example the v6.2 Agentless Monitoring for Windows Operating Systems. After the installation ends, the 64-bit monitoring agent is not running. There is no trace of the monitoring agent attempting to start in the main installation log.

The following conditions will bring about this issue:

- installations are performed locally
- v6.2.2 Fix Pack 1 monitoring agents are 64-bit
- pre-v6.2.2 Fix Pack 1 monitoring agents are a template

To ensure that these monitoring agents are started, manually start them from Manage Tivoli Monitoring Services.

Examples of monitoring agents from before v6.2.2 Fix Pack 1 for which the issue can appear:

- DB2 Agent
- Oracle Agent
- Microsoft SQL Server Agent
- Sybase Server Agent
- Microsoft Exchange Server Agent
- Lotus Domino Agent
- VMWare VI Agent
- Microsoft BizTalk Server Agent
- Microsoft Cluster Server Agent
- Microsoft Exchange Server Agent
- Microsoft SQL Server Agent
- mySAP Agent
- Siebel Agent

Errors in the configuration xml file

If a tag error occurs in an XML definition file, it is displayed in the LG0 log (for example, misspelling the tag in the *pc*_eventdest.xml file). In the following example, Srv should be Server:

```
<EventDest>
          <Destination id="0" type="T" default="y" >
              <Srv location="xx.xx.xx.xx" port="5529" />
          </Destination>
      </EventDest>
```

You will see the following in the *LG0 log file:

```
1090918140248857KRAX002I  XML begin tag Srv unrecognized XML Parser
1090918140323448KRAX003I  XML end tag Srv unrecognized XML Parser
```

If you have a problem with the value in the xml file, you need to check the agent log file. For example, if you misspell the value in the *pc*_eventmap.map file as follows:

```
<itmEventMapping:agent
    xmlns:itmEventMapping="http://www.ibm.com/tivoli/itm/agentEventMapping"
    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
    xsi:schemaLocation="http://www.ibm.com/tivoli/itm/agentEventMapping
    agentEventMap.xsd">
    <idUD/id>
    <version>6.2.0</version>
    <event_mapping>
         <situation name="UDB_Buff_Used_Pct_Warn_pr">
             <class name="ITM_KUDINFO00"/>
             <slot slotName1="msg">
                 <mappedAttribute name="Incorrect slotName"/>
             </slot>
    </event_mapping>
```

You will see the following errors in the agent log:

```
(4AB91AF5.0005-2:kraaeevx.cpp,686,"process_Slot_Tag") <slotName> attribute
not specified for element <slot>
(4AB91AF5.0006-2:kraaeevx.cpp,192,"IRA_EIF_endXMLElement") Null Emb
<110A05EB0> or Esb <NULL> processing slot end element.
(4AB91AF5.0007-2:kraaeevm.cpp,788,"processMapFile") Event map parsing error.
Map entries from file
 </data/achan/private_situation/ud_eventmap.map> not added.
```

Subnode Limitations for autonomous function

The Service Interface has the following limitations when working with subnode agents:

- The Queries Link has been removed and is not supported for subnode agents.
- The Situations Link only shows situations from the agent instance level. While situations can be distributed to run on specific subnodes, the Situations page does not filter by subnode, so all situations for all subnodes defined in the agent instance are shown.
- The History views show metrics for all subnodes combined in a single table. Currently, the service interface does not allow filtering by subnode.

SNMP alerts sent from the monitoring agent have some limitations when working with subnodes. Currently, the monitoring agent does not support situation attribute atomization. This means that for a situation that returns multiple rows from a table, an SNMP alert is only sent for the first row returned. For example, a

situation called Low_Disk_Space will trigger if available_disk_space *LE 20% might be true for more than 1 disk at a time. An enterprise situation would define the disk name as the display item so a separate situation alert would be displayed for each disk with less than 20% free space available.

The monitoring agent does not support the displayname/atomization, so the SNMP alert emitter will only emit an SNMP alert for the first row in the disk table where the situation is true. This limitation applies to subnodes as well. An instance of a subnode agent collects metrics for all subnodes in one table. These metrics are filtered by subnode when displayed in the Tivoli Enterprise Portal, but situations running against multiple subnodes in an instance are running against a single table. If a situation becomes True for 1 subnode, an SNMP alert defined for that situation will be emitted, but no SNMP alerts will be emitted for any other subnodes for that situation, since no further rows are processed in the table.

Binary Path attribute of the Windows OS agent does not show a value

On 64 bit systems with an installed 32 bit Windows OS agent, the value of the Binary Path attribute of the NT_Process attribute group is null if the process is running as 64 bit native.

Installing pre-v6.2.1 Monitoring Agent for Windows OS onto a v6.2.1 or later monitoring server inadvertently unconfigures the monitoring server

When a pre-v6.2.1 Monitoring Agent for Windows OS is installed onto a system that has a v6.2.1 or later monitoring server, the agent installation inadvertently unconfigures the monitoring server. This results in the monitoring server being left in a stopped state. Settings for the monitoring server remain preserved in the monitoring server ini and env files. Attempts to manually start the monitoring server fail with the message:

```
Unable to start tems service. Check the event log.
```

Monitoring Agents for Windows OS that are v6.2.1 and higher can be installed onto a monitoring server with no adverse side effects. IBM Tivoli Monitoring Application Agents regardless of version can also be installed onto a monitoring server with no adverse side effects.

If this issue is encountered, the monitoring server should be re-configured and restarted from Manage Tivoli Enterprise Monitoring Server or through the CLI. Settings for the monitoring server from before the installation (preserved in the monitoring server ini and env files) will automatically be used.

The tacmd executeaction command fails for certain take actions

For certain action commands, the **tacmd ExecuteAction** command fails with the following error message:

```
KUICXA029E: The execution of the take action ActionName failed in all
 the managed systems.
```

This failure occurs when the following ExecuteAction options are specified:

- -e | --stderr
- -o | --stdout
- -r | --returncode

- -l | --layout
- -p | --path

Certain action commands must be handled by specialized agent command handler functions. These include all action commands that are prefixed by a combination of the associated agent's two character product code (pc) and a colon (:) (for example, UX:). These take actions must never be run with any of the listed ExecuteAction options, otherwise the **tacmd ExecuteAction** command fails.

To understand if an action has a prefix, run the **tacmd viewaction** command and view the action's Command details. For example, the UNIX AMS Stop Agent take action command has a UX: prefix.

```
tacmd viewaction -n "AMS Stop Agent" -t ux

Action Name: AMS Stop Agent
Action Type: UNIX OS
Description: Kux:KUX6065
Command    : UX:AMS_Stop_Agent
"&KCA_UX_Agent_Active_Runtime_Status.PAS_Agent_Name"
"&KCA_UX_Agent_Active_Runtime_Status.Process_Name"
&KCA_UX_Agent_Active_Runtime_Status.Process_IDKey
: KUX_1212721981813
```

OS agent restarted unexpectedly on heavily loaded systems

When Agent Management Services has a high workload, the OS agent is restarted automatically. At this point the OS agent is stopped, and its workspace on the Tivoli Enterprise Portal is grayed out, then the monitoring agent starts automatically by Agent Management Services in several seconds. When the OS agent is started, refresh workspace, you find only the Watchdog's management status workspace as "managed", all of the other agents'workspaces' status display "Not managed."

On a heavily loaded system, increase the command time out parameter (KCA_CMD_TIMEOUT) in the OS agent's ini file from its default value to something larger, up to 120 seconds. Also, you may need to increase the checkFrequency value in the OS agent's availability checking policy file to a larger value. See the IBM Tivoli Monitoring Administration Guide's chapter on Tivoli Agent Management Services for information on how to change the parameters of this file.

Calendar entries overlap

After an upgrade, the calendar entries for PrimeShift and NonPrimeShift might have overlaps for hours 8 and 17. The default PrimeShift and NonPrimeShift calendar entries should look as follows:

```
Name: NonPrimeShift
Type: CRON
Data: * 0,1,2,3,4,5,6,7,17,18,19,20,21,22,23 * * 1-5

Name: PrimeShift
Type: CRON
Data: * 8-16 * * 1-5
```

To correct the problem, use the **tacmd editcalendarentry** command to correct the calendar overlaps so that the calendar entries look as shown above.

Receive an error when deploying an System Service Monitor agent

When deploying a System Service Monitor agent using a hub monitoring server outside a firewall through a remote monitoring server inside the firewall to a client inside the firewall, this error occurs:

```
KDY3010E: The SNMP command installSSM timed out with an SNMP return code of 0.
The SNMP command timed out because there was a network error, or the agent
was stopped, or the specified SNMP community/user does not have write and
create privileges.
```

This happens because the SNMPPORT is not available to use. The default SNMPPORT is 161. You should try to specify a different SNMPPORT to use when deploying the agent. Here is an example command:

```
tacmd createNode -h smb://target_endpoint_hostname -p snmpport=4567
server=RTEM_hostname -u user_id -w password -t ssm
```

Attributes differ between the situation action commands and what is displayed in the Tivoli Enterprise Portal

The raw data delivered by an monitoring agent is a string or number. The Tivoli Enterprise Portal has format information to control the display. When an attribute is used in a system command in the Situation Action tab, the raw data from the agent is substituted. For example, if a situation had an action command to send an email, it could look like this in the Situation editor:

```
some_command Warning too many processes &{System.Load_Average_1_Min}
options
```

If the average was actually 6.99 as displayed in the Portal client, the command would be executed as:

```
some_command Warning too many processes 699
options
```

&{xx.yy} is the best way to specify an attribute because there is no uncertainty about what attribute is being used. It allows adding characters to the command without spaces, such as a forward slash or backward slash.

If the data in the action command must be transformed from the raw data to some other format, that must be accomplished using shell commands. In Windows or Linux and UNIX that could be a shell command like Perl or REXX or ksh and in zOS that would be a REXX command which is STARTed. The shell command would transform the raw data into a display format and issue the command actually desired. If a shell command is already being used, it could simply take the needed formatting into account in its logic.

Events can also be sent through a Workflow Policy activity SNMP emitter or action command. That data will also be unscaled.

Large difference in attribute values between the Tivoli Enterprise Portal and Perfmon

On Windows 2008 systems, when viewing attributes there is a very large difference in their values between the Tivoli Enterprise Portal and Perfmon.

The Agent Service Interface is not globalized

This window is only displayed in English. There is not a workaround for this issue.

OS agent installation does not detect System Monitor agents

Any agent released with IBM Tivoli Monitoring v6.2.2 or before, other than agents built with the latest Agent Builder tool, should not be installed on top of the IBM Tivoli Monitoring v6.2.2 System Monitor agents.

Some attribute group names are unintelligible from the History Collection Configuration window

If you have configured historical collection for the monitoring agents and upgraded to IBM Tivoli Monitoring v6.2.2, you might notice that the names listed for attribute groups are now unintelligible.

In some cases, these names are not friendly and hovering over the item on the navigation tree shows the attribute group to which it belongs. You can alter the name of these collections by editing the historical collection and modifying only the name.

History collection fails to display the most recent 24 hours of data

When requesting a display of the historical availability for beyond 24 hours, the most recent 24 hours of data was not displayed, only the 48 hours (previous to the current 24) was displayed. This seems to be a case where data is retrieved correctly from the long-term store in the warehouse but is not retrieving data from the local short term history.

There can be a variety of factors that lead to a failed history collection:

- The size of the history data file affects the amount of time it takes the agent to read the file.
- The amount of data the agent is trying to send to the monitoring server.
- The bandwidth of the communications (for example, a slow data rate).

Situations with attributes from more than 1 group not supported with autonomous agent

When using autonomous agent in Manage Connected Mode, creating situations with AND and OR logic, and using values from two different attribute groups, the traps do not list the predicates in an expected way.

If you have defined a situation that attempts to combine attributes across more than 1 attribute group, this is not currently supported by any autonomous agent processing mode or private situations. The monitoring server performs the evaluation of situations having combined attribute groups. This can be either from embedded situations, or two or more attribute groups in the same predicate, for example, WHERE USER=abc AND LOCALTIME=today.

Failure when importing situation xml file edited with WordPad

If you edit an xml file for a situation using WordPad, and then import the situation (**tacmd createsit-i** *xml*), the command fails. If you edit the xml file using Notepad, it works correctly. Use Notepad to edit situation `xml` files.

Printer details of another system are displayed on the Tivoli Enterprise Portal

When connecting to a system remotely, printers on that local system can be seen from the Tivoli Enterprise Portal on the remote system. You should be aware that by using a remote desktop, printer information might be displayed in the Tivoli Enterprise Portal and shared with others.

CTIRA_MAX_RECONNECT_TRIES environment variable is now obsolete

The agent now attempts communication with a monitoring server until a connection is successfully established. There is no longer a limit on the number of connection attempts. If the CTIRA_MAX_RECONNECT_TRIES environment variable is specified, it is accepted, and results in the agent reverting to the previous behavior of there being a limit on connection attempts. A trace message is also produced, indicating that this variable is obsolete.

If you specify this variable and the number of connection attempts to the monitoring server exceeds CTIRA_MAX_RECONNECT_TRIES, the agent attempts to shutdown. If the Agent Management Services Watchdog is running, it immediately restarts the agent. If you want the agent to shutdown when CTIRA_MAX_RECONNECT_TRIES is exceeded, this Watchdog process must be disabled. Use the AMS Stop Management action to disable this watchdog process.

Agent goes offline after removing history path

Deleting the directory where historical collection occurs is not supported. If this is done, the directory must be manually recreated.

Override button is not present for a situation

A situation cannot be overridden if it contains repeated combinations of attributes or operators.

Agent's Management Definition View columns are not showing data

There will be no data shown in any columns for which an element in the corresponding CAP file is empty. An element is left empty when it is not needed to manage a particular agent by Agent Management Services. For monitoring agents, for example, the following columns are left empty:

- Startup Script
- Stop Script
- Configuration Script
- Operating System Version
- Operating System Name
- Dependencies

There is a situation distribution discrepancy if there is a hub monitoring server outage when one or more remote monitoring servers remain active

Run the itmsuper tool following the hub monitoring server recycle and take note of any distribution discrepancy between any of the remote monitoring servers and the hub monitoring servers that the tool reports on. For the situations involved in the distribution discrepancy, an undistribute followed by a redistribute of situations rectifies the problem by causing proactive notifications to occur where the agents are currently reporting.

Installing v6.2.2 agent application support on a monitoring server for a prior release causes agents to fail

Do not install agent application support for the current release on a Tivoli Enterprise Monitoring Server for a prior release (for example, do not install V6.2.2 agent application support on a V6.2 monitoring server). Doing so could cause agents to fail. If you see the 208 return code at the Tivoli Enterprise Portal Server console, you have installed application support for v6.2.2 on a back level Tivoli Enterprise Monitoring Server.

Installing backlevel Windows OS agent on existing environment causes Tivoli Enterprise Monitoring Server not to start

Due to packaging optimizations in v6.2.1, installing a backlevel Windows OS Agent into an existing 6.2.1 environment is not supported, and the Tivoli Enterprise Monitoring Server cannot start. If this is the desired deployment, the backlevel Windows OS Agent should be installed first.

The link to an OS agent workspace is pointing to a superseded version of the workspace

Links point to specific object names and are not automatically updated to return the latest version of a workspace. A link from an external agent pointing into the OS agent must be updated to point to the current release. If the current version of the agent is not truly "versioned" using the VRF appendage to the object name, but is a different object name to facilitate 64-bit data workspace exposure, the external anchor should have two links associated with it: one pointing to the existing version of the workspace and a second pointing to the new 64-bit enabled workspace. Non-OS agents should not expect a specific version of the workspace to be available unless their respective agent requires that base version. In this case, it might not be feasible to update agents until the next required release.

SNMP trap Sendto fails

An agent running on an IPv4 or dual stack IPv4/IPv6 system tries to emit an SNMP trap to an IPv6 destination address defined in the `trapcnfg` XML file, but the trap is not received on the destination system. In the agent log file, there is an error message stating that the SNMP trap Sendto failed with rc=-1.

Ensure that the system sending SNMP traps to IPv6 destinations can resolve its own IPv6 address. The system where the trap emitting-agent is running must have a valid IPv6 address associated with its own local hostname. If the DNS

configuration has not been updated for IPv6, then it is necessary to modify the `\etc\hosts` file or `/etc/resolv.conf` file on the agent system in order to associate the local hostname with a valid local IPv6 address, for example, not a loopback or link-local address.

Situation overrides cannot be used to disable situations on specific systems at specific times

Dynamic thresholding has a restriction on the override of situations with calendar entries. Situation overrides can be used to change the conditions under which situations run on specific systems at specific times. However, they cannot be used to disable a situation on specific systems at specific times. To override the time a specific situation runs, the situation must include a time attribute, for example, Local_Time.Day_Of_Week, and then you can use an override to change the value of the time attribute that causes the situation to run.

Situation or calendar name in thresholds.xml file appears incorrect

If situation and calendar overrides are created with names that do not conform to the naming convention, the names will be a randomly generated name and be displayed in the xml file as such. The naming convention includes the following conditions:

- Must start with an alphabetical character (a-z, A-Z)
- Can contain 1-30 additional alphanumeric characters (a-z, A-Z, 0-9)
- Can also contain the following special character (_)
- Must end with an alphanumeric character

BAROC file is missing for IBM Tivoli Monitoring 5.x Endpoint situations

A BAROC file does not exist for the IBM Tivoli Monitoring 5.x Integration Agent that defines the class definitions for the following situations:

- KTM_Health_Indication
- KTM_Missing_Metadata
- KTM_Resource_Model_Statu

As a result, when any of these situations are triggered, the forwarded situation events are not successfully processed by the EIF receiver.

The BAROC file for the Integration Agent is no longer supplied with IBM Tivoli Monitoring. Generate the BAROC files as needed by using the BAROC file generator tool found here:

`http://catalog.lotus.com/topal?NavCode=1TW10TM43`

The target hostname, platform, and version information is not displayed for the deploy status in the CLI or the workspace

Target hostname, platform, and version information is not displayed for the deploy status in the CLI or the workspace. For group commands, the target hostname, platform, and version information are not displayed. However, the transaction ID for the grouping command can be used to query all the transactions started by this group command.

Here is an example of a group with one member:

```
@echo "Creating DEPLOY Group Window"
tacmd creategroup -g Window -t DEPLOY -d "Windows Deploy Group"

@echo "Adding ACHAN1 to Window DEPLOY group"
tacmd addgroupmember -g Window -t DEPLOY -m achan1.raleigh.ibm.com
 -p KDYRXA.RXAusername=achan KDYRXA.RXApassword=xxxxx
KDYRXA.installDir=C:\data

@echo "Issuing group DEPLOY of Windows OS agent"
tacmd createNode -g Window

Transaction ID : 12227825422970000000015724
Command        : CREATENODE
Status         : SUCCESS
Retries        : 0
TEMS Name      : HUB_ACHAN2
Target Hostname:
Platform       :
Product        : ITM
Version        :
Error Message  : KDY0028I: Request completed successfully.
Deployment request was processed successfully and is now completed.

Transaction ID : 12227825422970000000015724
Command        : CREATENODE
Status         : SUCCESS
Retries        : 0
TEMS Name      : HUB_ACHAN2
Target Hostname: achan1.raleigh.ibm.com
Platform       : WINNT
Product        : NT
Version        : 062100000
Error Message  : KDY2065I: The node creation operation was a success.
Old Component: deploy
New Component: itm_scn_ID
```

A workspace view is showing an error

It is possible that the workspace definition was saved incorrectly. An example workspace would be the IBM Tivoli Monitoring for Databases: Oracle Agent's SQL Text workspace.

To solve this problem, replace the view and save the workspace.

Agent upgrade and restart using non-root

The monitoring agent can run using a non-root user ID on UNIX and Linux systems. This can be done by running the **itmcmd agent start** command while logged in as a non-root user, and this can be done remotely by deploying the agent using the **Run As** option on the GUI or using the **_UNIX_STARTUP_.Username** option on the **tacmd addSystem** command line. If the agent is running using a non-root user ID, and then the agent is upgraded, restarted remotely, restarted as a result of a system reboot, or the **itmcmd agent start** is run using the root user ID, then the monitoring agent subsequently runs as the root user. To confirm the user ID that the monitoring agent is using, run the following command:

```
itm_install/bin/cinfo -r
```

If the installation is not permissioned properly, then you might be unable to restart the agent as a non-root user ID after it has been run as the root user ID. To prevent this problem, ensure that the **secureMain lock** command with the -g option has

been previously run. See the "Securing your IBM Tivoli Monitoring installation on Linux or UNIX" appendix in the *IBM Tivoli Monitoring Installation and Setup Guide* for further details.

If the agent is running as root, and that is not the desired user ID, then use the following steps to restart the agent:

1. Log in as root.
2. Run the **itmcmd agent stop** command.
3. Log in (or 'su') to the user ID that you want the agent to run as.
4. Run the **itmcmd agent start** command.

If the agent was running as root because of a system reboot, then complete the following steps so that the appropriate user ID is used the next time the system is rebooted. Editing the startup file is no longer supported. Instead you must modify the `config/kcirunas.cfg` file and then run `bin/UpdateAutoRun.sh`:

1. Edit *install_dir*`/config/kcirunas.cfg`.
2. Add a section, after the `agent` line, to specify the agent or agent instance that you want to start as a specific user ID. To specify the user ID to start a non-instance agent, or to start all instances of an agent, use the following syntax:

```
<productCode>product_code</productCode>
<default>
   <user>user_name</user>
</default>
```

   To specify different user IDs to start different instances of an agent, use the following syntax:

```
<productCode>product_code</productCode>
<instance>
   <name>instance_name1</name>
   <user>user_name</user>
</instance>
<instance>
   <name>instance_name2</name>
   <user>user_name</user>
</instance>
```

   Where:

   product_code
   2-character product code for the agent, for example, *ux* for the Unix OS monitoring agent.

   user_name
   Name of the user to run the agent as.

   instance_name1
   Name of an instance.

   instance_name2
   Name of another instance.

   Examples:

   For the Unix OS monitoring agent, to run as itmuser:

```
<productCode>ux</productCode>
<default>
   <user>itmuser</user>
</default>
```

For the DB2 monitoring agent instances to run as the instance owner IDs:

```
<productCode>ud</productCode>
<instance>
   <name>db2inst1</name>
   <user>db2inst1</user>
</instance>
<instance>
   <name>db2inst2</name>
   <user>db2inst2</user>
</instance>
```

For the Websphere MQ monitoring agent instances to all run as the mqm user ID, and for the default instance to not be started:

```
<productCode>mq</productCode>
<default>
   <user>mqm</user>
</default>
<instance>
   <name>None</name>
   <autoStart>no</autoStart>
</instance>
```

3. Repeat step 2 for each agent or agent instance that you want to start as a specific user ID.
4. Save the file.
5. Run *install_dir*/bin/UpdateAutoRun.sh as root user.

After installing and configuring a monitoring agent, it fails to start

If the SecureMode file is in the registry directory, SecureMain was run in environment. This does not allow the monitoring agent to start if you try to start it without root privileges. See the *IBM Tivoli Monitoring Installation and Setup Guide* for instructions on how to have monitoring agents work properly with SecureMain in place.

situation_fullname slot missing for delete events

If you create a situation that has a long name (longer than 32 characters), distribute the situation to an agent, and then delete it after the situation's associated event is displayed in Tivoli Enterprise Console, the situation_fullname slot is missing.

The expected result would be that, for the deleted event, the situation status is set to 'D".

Events do not reflect the long names if the definition is deleted, and the Tivoli Enterprise Monitoring Server logs also do not reflect the long name.

Logs are using the situation ID string instead of the display name

Situations have both a display name (up to 256 bytes in length, UTF8 enabled) and an ID string (up to 32 bytes in length). For example, a situation display name can be "don't let the pigeon drive the bus !" or 100 characters of Japanese text. The associated ID string will be of the form 000000000000008D723DE7DFED450F. If the Tivoli Enterprise Portal Server Universal Message Console and the Tivoli Enterprise Monitoring Server RKLVLOG cannot display the situation display name, the ID string is displayed instead.

To ensure that your situations are displayed using the display name instead of the display ID, make sure that your situation names do not exceed 31 characters in length, and that they do not contain any special characters.

If a managed system list is removed for a situation, the situation stops

If a managed system list is removed for a situation, the situation stops. At this point, you see a message in the Message Log that the situation has been stopped and deleted for the Remote Tivoli Enterprise Monitoring Server, and events do not appear for any remaining managed system list that is in the distribution list for the situation. Manually restart the situation after the managed system list has been removed.

Descriptions are not displayed for default situations

If you use the command to view any default situation, for example, when inputting **/tacmd viewsit -s UNIX_User_CPU_Critical** , the following is displayed:

```
Name                    : UNIX_User_CPU_Critical
Full Name               :
Description             : Kux:KUX3736
Type                    : UNIX OS
```

This is a limitation of the current product.

Agent configuration failed on remote deploy while using single quotes for configuration properties

You cannot provide a deployment or configuration property with single quote characters embedded within the properties. For paths with spaces in them, wrap the entire property in single or double quotes. The following examples are valid:

```
DBSETTINGS.SYBASE=/data/sybase
'DBSETTINGS.SYBASE=/data/sybase'
"DBSETTINGS.SYBASE=/data/sybase"
```

Whereas this example is NOT valid:

```
DBSETTINGS.SYBASE='/data/sybase'
```

New attributes missing

When viewing a workspace, not all of the attribute group's attributes are displayed in a table view. To see the new attributes in a table, you must create a new query to retrieve the new attributes, and you must create a new workspace to use the new query.

Unable to receive summarized data for the last hour in the Tivoli Enterprise Portal

The Summarization and Pruning Agent does not run continuously. It is scheduled to run at some frequency or on a fixed schedule. Data for the last hour likely will not be available until this agent has just finished running and has had enough data to compute the last hour summary, which a data sample exists for the following hour.

The Summarization and Pruning Agent does not summarize hour *X* until at least one sample for hour *X*+1 is available in the Tivoli Data Warehouse at the time the summarization is started for that agent.

Summarization for CCC logs is not allowed

You cannot set summarization for CCC logs. If summarization is set up for CCC logs, it can be undone again using the command-line interface.

Receive errors when modifying the JAVA HEAP SIZE for the Summarization and Pruning Agent

On 32-bit Windows systems with 4 GB of RAM, there is a maximum heap-size limit of approximately 1.6 GB. You might need to add the /3GB switch to the `boot.ini` file. Determine the max heap size in MBs by testing when setting KSZ_JAVA_ARGS=-Xms256M -XmxSIZEM in the `KSYENV` file. If the -Xmx value is too large, the agent fails with an error.

When associating situations, they fire, but cannot be viewed

When a situation association is done at a specific node level on the navigator tree, the situation fires when true, and the event is then associated to the navigator item. The situation is not associated with that navigator item if the navigator item or node is not part of its distribution.

The Summarization and Pruning agent fails when processing an index created in a previous release of the product

If a database insert fails while running the Summarization and Pruning Agent, and the message indicates the insert has failed because the maximum index size has been exceeded, complete the following steps to correct this issue:

1. Stop the Summarization and Pruning Agent.
2. Drop the index causing the failure.
3. Run the Schema Publication Tool in configured mode:
   ```
   KSY_PRODUCT_SELECT = configured
   ```
4. Open the `tdw_schema_index.sql` file and find the index that was deleted in step 1.
5. Edit out all statements except the index you want to recreate.
6. Run the create index statement.
7. Start the Summarization and Pruning Agent.

Summarization and Pruning agent schedule not affected by daylight saving time

If after starting the Summarization and Pruning agent you allow daylight savings time to be reached, the agent start time is now 1 hour later than the time before the time change. The agent does not seem to be aware of the time change.

The agent is respecting flexible scheduling in this case. That it appears to be running one hour later is an artifact of the time change. The number of minutes for the run remains the same.

Attribute names must be kept under 28 characters long

Attribute names must be kept under 28 characters long due to the Summarization and Pruning Agent adding suffixes to the attribute names. There are also limits in how long the column name can be for some of the DBMS' that are supported by Tivoli Data Warehouse.

Agent deploy operations are not completing before the TIMEOUT expires

When running agent deploy operations, TIMEOUTs can occur because of slow network connections or slow hardware. The agent deploy operations can complete if you increase the TIMEOUT value. Some operations can complete even after a timeout is returned.

Table 39. Resolutions for agent deploy operations that TIMEOUT

Problem	Resolution
KDY0014E message	Increase the Tivoli Enterprise Monitoring Server timeout value to 1200 seconds (`TIMEOUT=1200`). The default is 600 seconds. On Windows: *`installation_dir`*`\CMS\KBBENV`. On UNIX-based systems: *installation_dir*/config/*host_name*_ms_*Tivoli_Enterprise_Monitoring_Server_ID*.config.
KDY1009E KDY1017E KDY1018E KDY1022E KDY1025E KDY1030E KDY1033E	Increase the OS agent timeout to 600 seconds (`TIMEOUT=600`). The default is 300 seconds. On Windows: *`installation_dir`*`\CMS\KNTENV`. On UNIX-based systems: *`installation_dir`*`/ux.ini`. On Linux, set it in *`installation_dir`*`/lz.ini`. The value must be set in seconds:
A system error occurs when running a tacmd command.	Increase the timeout for the tacmd setting environment variable to 3600 seconds. On Windows: Enter the following command: `set timeout=3600` **Note:** Be aware that this command does not affect the TACMD_TIMEOUT in the `KUIRAS1.log`, but it does indeed change the timeout period. Another solution is to change the TACMD_TIMEOUT environment variable in the `itm_home/bin/tacmd` file on GNU/Linux and UNIX systems or the `itm_home/bin/KUIENV` file on Windows systems. The TACMD_TIMEOUT in these files must be in minutes. You can also change the environment variable in the `kui.env` file on Windows systems and the tacmd shell script on non-Windows systems. Both of these files can be found in the CANDLEHOME/logs directory.
A failure occurs when deploying an agent from the Tivoli Enterprise Portal.	The Tivoli Enterprise Portal Server times out waiting for deployment action to complete. The default timeout is 600 seconds. You can change the timeout setting to KFW_SQL1_ASYNC_NOTIFY_MAX_WAIT in kfwenv: `KFW_SQL1_ASYNC_NOTIFY_MAX_WAIT=1000`

Table 39. Resolutions for agent deploy operations that TIMEOUT (continued)

Problem	Resolution
KUICCN068E error when running tacmd createnode.	Increase the timeout value in seconds by adding "-o TIMEOUT=3600" to the **createnode** command.

Deploy cannot tell if the install failed

When installing an OS Agent on an endpoint that already has an OS Agent, the installation program does not write out a `C:\IBM\ITM\InstallITM\Abort IBM Tivoli Monitoring 20070924 1319.log` in the **createNode** specified directory. It writes messages to the existing `C:\data\itm61_oqv_ga2_koy\InstallITM\IBM Tivoli Monitoring 20070924 1319.log` log file and reports the error in that log file.

An agent does not display in the Tivoli Enterprise Portal or in the output from the listSystems command

If you have multiple instances of a monitoring agent, you must decide how to name the monitoring agents. This name is intended to uniquely identify that monitoring agent. The agent's default name is composed of three qualifiers:

- Optional instance name
- Machine network hostname
- Agent product node type

An agent name truncation problem can occur when the network domain name is included in the network hostname portion of the agent name. For example, instead of just the hostname myhost1 being used, the resulting hostname might be myhost1.acme.north.prod.com. Inclusion of the network domain name causes the agent name in the example above to expand to SERVER1:myhost1.acme.north.prod.com:KXX. This resulting name is 39 characters long. It is truncated to 32 characters resulting in the name SERVER1:myhost1.acme.north.prod.

The agent name truncation is only a problem if there is more than one monitoring agent on the same system. In this case, the agent name truncation can result in collisions between agent products attempting to register using the same truncated name value. When truncated agent names collide on the same system, this can lead to Tivoli Enterprise Monitoring Server problems with corrupted EIB tables. The agent name collision in the Tivoli Enterprise Monitoring Server might cause a registered name to be associated with the wrong product.

In general, create names that are short but meaningful within your environment. Use the following guidelines:

- Each name must be unique. One name cannot match another monitoring agent name exactly.
- Each name must begin with an alpha character.
- Do not use blanks or special characters, including $, #, and @.
- Each name must be between 2 and 32 characters in length.
- Monitoring agent naming is case-sensitive on all operating systems.

Create the names by completing the following steps:

1. Open the configuration file for the monitoring agent, which is located in the following path:
   - **On Windows:** *&install_dir;*\tmaitm6\K*product_code*CMA.INI. For example, the product code for the Monitoring Agent for Windows OS is NT and the file name is KNTCMA.INI.
   - **On UNIX and Linux:** *install_dir*/config/*product_code*.ini and *product_code*.config. For example, the file names for the Monitoring Agent for UNIX OS are ux.ini and ux.config.
2. Find the line the begins with **CTIRA_HOSTNAME=**.
3. Type a new name for host name that is a unique, shorter name for the host computer. The final concatenated name including the subsystem name, new host name, and AGENT_CODE, cannot be longer than 32 characters.

   Note: You must ensure that the resulting name is unique with respect to any existing monitoring component that was previously registered with the Tivoli Enterprise Monitoring Server.
4. Save the file.
5. Restart the agent.
6. If you do not find the files mentioned in Step 1, perform the workarounds listed in the next paragraph.

If you do not find the files mentioned in the preceding steps, perform the following workarounds:

1. Change **CTIRA_HOSTNAME** environment variable in the configuration file of the monitoring agent.
   - Find the KAGENT_CODEENV file in the same path mentioned in the preceding row.
   - For z/OS agents, find the **RKANPAR** library.
   - For i5/OS agents, find the **QAUTOTMP/KMSPARM** library in member **KBBENV**.
2. If you cannot find the **CTIRA_HOSTNAME** environment variable, you must add it to the configuration file of the monitoring agent:
   - **On Windows:** Use the **Advanced > Edit Variables** option.
   - **On UNIX and Linux:** Add the variable to the config/*product_code*.ini and to config/*product_code*.config files.
   - **On z/OS:** Add the variable to the **RKANPAR** library, member K*product_code*ENV.
   - **On i5/OS:** Add the variable to the **QAUTOTMP/KMSPARM** library in member **KBBENV**.
3. Some monitoring agents (for example, the monitoring agent for MQ Series) do not reference the **CTIRA_HOSTNAME** environment variable to generate component names. Check the documentation for the monitoring agent that you are using for information on name generation. If necessary, contact IBM Software Support.

Other symptoms that can be observed when multiple instances of a monitoring agent with the same managed system name attempt to connect to a Tivoli Enterprise Monitoring Server include the following:

- A managed system name's status toggles ON and OFF line constantly as one agent heartbeat overlays the other's information.

- High CPU usage is observed that is caused by a constant thrashing of the Tivoli Enterprise Portal Server or Tivoli Enterprise Monitoring Server.
- Situation distribution, Tivoli Enterprise Monitoring Server table relationship updates, Tivoli Enterprise Portal Server topology view updates; all could be initiated as each agent heartbeat registers its changing properties.

Other solutions besides ensuring that each managed system name is unique are the following:

- Detect and stop the agent process that is running improperly. This can be done by checking the Tivoli Enterprise Portal Server Managed System Status network address of the managed system name that seems to toggle ON and OFF line. Go to the system indicated in the network address and check for multiple running monitoring agents.
- If the agents running on the same system are the same product, stop or kill the unintended agent process.
- Delete the faulty agent managed system name from the enterprise managed system status so that the new managed system name can register properly with the Tivoli Enterprise Monitoring Server. You might need to stop the correct agent process so that it is OFF line.

One monitoring agent's workspaces are listed under another agent node on the Tivoli Enterprise Portal

This problem has been seen in ira-based agents that exist on the same system. Set the CTIRA_HOSTNAME environment variable configuration file for the monitoring agent as follows:

1. Open the configuration file for the monitoring agent, which is located in the following path:
   - **On Windows:** *install_dir*\tmaitm6\K*product_code*CMA.INI. For example, the product code for the Monitoring Agent for Windows OS is NT file name for is KNTCMA.INI.
   - **On UNIX and Linux:** *install_dir*/config/*product_code*.ini. For example, the file name for the Monitoring Agent for UNIX OS is ux.ini.
2. Find the line the begins with **CTIRA_HOSTNAME=**.
3. Type a new name for host name that is a unique, shorter name for the host computer. The final concatenated name including the subsystem name, new host name, and AGENT_CODE, cannot be longer than 32 characters.

   Note: You must ensure that the resulting name is unique with respect to any existing monitoring component that was previously registered with the Tivoli Enterprise Monitoring Server.
4. Save the file.
5. Restart the agent.

Issues with starting and stopping an agent as a non-Administrator user

You might experience issues with starting and stopping an agent as a non-Administrator user. This issue is caused because of improper permissions set for the *hostname_pc*.run file.

That file is created or modified every time an instance is started or stopped. All instances must use the same user ID.

UNIX-based systems Log agent was deployed, configured, and started but returns the KFWITM290E error

The Tivoli Enterprise Monitoring Server is timing out waiting for deployment action to complete. The default timeout is 600 seconds. You can change the timeout setting to KFW_SQL1_ASYNC_NOTIFY_MAX_WAIT in `kfwenv`.

```
KFW_SQL1_ASYNC_NOTIFY_MAX_WAIT=1000
```

KDY1024E error displays when configuring the run-as user name for an agent

The error message KDY1024E displays when configuring the run-as user name for an agent when the UNIX-based systems monitoring agent was installed as a non-root user. For UNIX-based systems, you can only configure the run-as user name if the UNIX-based systems/UNIX-based systems monitoring agent was installed using the root user. In this case, leave the entry for the run-as user blank or set the run-as user to the same user ID used to install the UNIX-based systems monitoring agent.

Interface unknown messages in ras1 logs

Interface unknown messages appear in the ras1 log. For example:

```
(46CB65C1.0001-F:kdcsdrq.c,466,"do_request") Interface unknown
684152a852f9.02.c6.d2.2d.fd.00.00.00,
activity c638270e4738.22.02.09.2a.15.06.28.a2,
7509.0
```

These are issued to alert you that some set components are driving RPC requests to a server that is not setup to handle that request. Often, this occurs when the Warehouse Proxy Agent is not setup on a fixed port number. For information on how to setup the Warehouse Proxy Agent, see the IBM Tivoli Monitoring Installation and Setup Guide.

When upgrading a System Service Monitors agent from 3.2.1 to 4.0, receive KDY3008E message

The previous agent is still running and using the port that is needed for the upgraded agent. Stop the agent before the upgrade. Once the agent is stopped, the upgrade is successful.

The Tivoli Data Warehouse fails and you either lose data or have memory problems

On distributed systems, the data is written to the local file system. When the Warehouse Proxy Agent receives the data, it copies the data to the Tivoli Data Warehouse. If the Tivoli Data Warehouse is not available, the collected data could take up a significant amount of memory.

On z/OS systems, the data is written to the persistent datastore. Maintenance procedures must be installed and workable to handle cases other then simply saving copies of the data. These procedures are used to recover corrupted datasets

and to handle migration issues. When the persistent datastore is started, it looks at the status of a dataset and determines if it has corrupted data. If there is corruption, it launches maintenance with the options to export the data, reallocate and initialize the dataset, and then restore the exported data. Also when the persistent datastore is started, it compares the information in the dataset against the current configuration to see if any table structures have changed. When it detects a change, it goes through the same process that effectively does a database REORG. If you do not have the maintenance procedures installed and usable, the datasets might become unusable, and therefore there might be a loss of data.

If maintenance is set-up so that the data is rolled-over, the data that would have been copied to the Tivoli Data Warehouse is copied over after a set period of time. You can set maintenance to roll off the data. For more information on rolling of this data so that it is backed up, see the *IBM Tivoli Monitoring Configuring Tivoli Enterprise Monitoring Server on z/OS Guide*.

If maintenance is not performed, then the agent stops writing to the Tivoli Data Warehouse until initialization is performed. Because the agent has stopped writing, the data is there "forever" until you re-initialize and start again writing from the top of the first dataset.

If persistent datastore maintenance is allowed to proceed automatically as it is intended, then the agent starts writing from the top of the first persistent datastore, therefore wrapping occurs.

The persistent datastore is set up to allow for 24 by 7 data collection even if maintenance is not specified when configuring the product in ICAT. There are typically 3 datasets, though having more is allowed.

The minimum of 3 datasets allows for continuous collection, the normal case is that one dataset is empty, one or more are full, and one is active. When an active dataset becomes full, the empty dataset is activated for continued writing. When the persistent datastore detects that there are no empty datasets left, it finds the one with the oldest data and maintains it. If the BACKUP or EXPORT options are not specified, maintenance is done within the persistent datastore to initialize the dataset so that its status changes from full to empty. If BACKUP or EXPORT are specified, a job runs to save the data, then the dataset is initialized and marked as empty. If the BACKUP or EXPORT was specified, but the maintenance jobs fail to do their job, the recording would stop in the persistent datastore. In this case, datasets are taken off-line until there are no more available datasets for reading or writing.

Note: If you allocate persistent datastores that fit more than 24 hours worth. The agent initializes and writes as much data as it can fit in the persistent datastores, 24 hours or more. The Tivoli Enterprise Portal, for short term history display, only pulls up 24 hours worth of data. The warehouse can archive ALL the data in the persistent datastores, regardless if it has been 24 hours or more worth of data.

If you create a Tivoli Enterprise Portal query that is over 24 hours, then the warehouse fulfills that request regardless if the data is in the online persistent datastores.

Also, because the agent or Tivoli Enterprise Monitoring Server reads the entire persistent datastores at initialization time, you should not allocate very large persistent datastores to potentially store more than 24 hours. That increases the

Tivoli Enterprise Monitoring Server and agent startup time. As mentioned above, the agent writes to it, but the Tivoli Enterprise Portal only displays 24 hours from it. The warehouse processing reads all the data in the persistent datastores (24 hours or more), but there is a trade-off in Tivoli Enterprise Monitoring Server and agent startup time. It is always best to calculate space for 24 hours as best as possible.

As far as the potential of losing historical data, if the warehouse is down over 24 hours, that is a potential problem, assuming the persistent datastore's backup processing is functioning and, therefore, the agent does not stop writing to the persistent datastores.

Since you have the choice of collecting history data at the Tivoli Enterprise Monitoring Server or the Tivoli Enterprise Monitoring Agent, the persistent datastore should be defined in both places. If you are 100% sure that you will always collect at the Tivoli Enterprise Monitoring Agent or always collect at the Tivoli Enterprise Monitoring Server then you can optionally define the persistent datastore in only one location. Note that many configuration issues occur because the person installing the product selects one location for the persistent datastore and sometime later someone else enables history collection for the other location.

Error list appears in warehouse logs

The following error list appears in the warehouse logs:

```
== 25 t=Thread-1 com.ibm.db2.jcc.c.DisconnectException:
A communication error has been detected.
 Communication protocol being used: T4Agent.sendRequest().
Communication API being used: OutputStream.flush().
Location where the error was detected:
There is no process to read data written to a pipe.
Communication function detecting the error: *. Protocol specific error codes(s)
TCP/IP SOCKETS   DB2ConnectionCorrelator: G92A17E8.C3D2.071018074633
 at com.ibm.db2.jcc.b.a.a(a.java:373)
 at com.ibm.db2.jcc.b.a.y(a.java:346)
 at com.ibm.db2.jcc.b.a.l(a.java:298)
 at com.ibm.db2.jcc.c.j.c(j.java:234)
 at com.ibm.db2.jcc.c.uf.lb(uf.java:1934)
 at com.ibm.db2.jcc.c.uf.addBatch(uf.java:1348)
 at com.tivoli.twh.khd.khdxjdbc.addBatch(khdxjdbc.java:1290)
```

Check the ethernet adapter settings on both the client and server. There are problems if the adapter is set to Auto and the switch is set to 100/Full Duplex.

When configuring the Monitoring Agent for Sybase and the Warehouse Proxy Agent, receive message to use CandleManage

The **CandleManage** command has been deprecated. The message should reference the **./itmcmd manage** command.

listSit command with the type option fails with a KUIC02001E message on Japanese Systems

Edit the `kuilistsitVld.xml` file to replace the following text:

```
<Type    arg1="-t"  arg2="--type"  Type ="String" ValidationRegExp=
"[-A-Za-z0-9 _/()\&%.]" Required="Y"/>
```

with the following text:

```
<Type    arg1="-t"  arg2="--type"  Type ="String" ValidationRegExp=
"[-A-Za-z0-9 _/()\%.]" Required="Y"/>
```

Take Action command names do not accept non-English characters

There is not a workaround at the present time.

Creating a situation from a group member does not copy the distribution list

The indirect assignments coming from the group are due to the original situation's membership within that group. When you create another situation from one of these member situations, that operation does not allow for the new situation being part of that same group. Copy only the distributions that are directly assigned.

A changed situation name does not show up

If you change the name of a situation, the Tivoli Enterprise Portal and the **listsit** command does not show the name change. Once the situation is created, it has to be referenced by its original name.

New agents do not display in the Tivoli Enterprise Portal navigator

The Tivoli Enterprise Portal navigator does not update automatically when an agent is installed to or uninstalled from the managed system. You must refresh the navigator to display changes. Do the following to refresh the navigator from the Tivoli Enterprise Portal menu:

- Press the F5 key on your keyboard.

  –OR–
- Click **View** > **Refresh**.

An agent displays unavailable in the Tivoli Enterprise Portal

The agent is not online. Do the following to ensure the agent is online:

- Check the agent log for data communication errors.
- Check the managed system status in the Tivoli Enterprise Portal.
- Ensure that the agent process started.
- Check the Tivoli Enterprise Monitoring Server `kfwras1.log` for errors.
- Check the Tivoli Enterprise Monitoring Server `kfwras1.log`.

CTIRA_HOSTNAME has no effect on log file names

Setting CTIRA_HOSTNAME with the virtual hostname shows the agent on the workspace as one entity no matter the node on which it is running. However, the setting has no effect on the log file names. These names still use the local nodename instead of the virtual hostname.

The Summarization and Pruning Agent and the Warehouse Proxy Agent do not work with DB2 9.1 Fix Pack 2

Do not try to use these agents with this version of DB2.

An error of 'can bind a LONG value only for insert' appears

The following message appears in the Warehouse Proxy Agent:

```
ORA-01461: can bind a LONG value only for insert into a LONG column
```

Upgrade to Oracle 10.1.0.5 or later.

Errors in either the Warehouse Proxy Agent or Summarization and Pruning Agent logs

You receive the following error in either the Warehouse Proxy Agent or Summarization and Pruning Agent logs:

```
DB2 SQL error: SQLCODE: -964, SQLSTATE: 57011, SQLERRMC: null
```

The solution is to increate the DB2 logging for the warehouse database. See the *IBM Tivoli Monitoring for Databases: DB2 Agent User's Guide* for more information.

Receive a message saying that the statement parameter can only be a single select or a single stored procedure

You receive the following message when connecting to a Microsoft SQL Server 2000 database on a Windows 2000 system from a Warehouse Proxy Agent on a Linux system using Microsoft SQL Server 2005 JDBC driver 1.2 April 2007.

```
SSQL error: Exception message: sp_cursoropen/sp_cursorprepare:
The statement parameter can only be a single select
or a single stored procedure.
```

This was fixed by not adding by default the selectMethod=cursor string in a Microsoft SQL Server URL, but you also must remove the string selectMethod=cursor that comes by default when choosing the Microsoft SQL Server database in the Warehouse Proxy Agent configuration panel on UNIX systems.

Custom defined workspace views do not handle symbol substitution as expected

Symbol references in the header and footer regions of custom defined workspace views do not resolve as expected in the Tivoli Enterprise Portal. Symbol references in Header and Footer expressions set through the view Properties window will only be substituted if the workspace is reached as the target of a link. Verify that the custom workspace for which the expression is being specified is being reached through a link rather than being selected directly from a navigator node or the Workspaces menu. Otherwise, the symbols will evaluate as an empty string.

For best results, also ensure that the expression is assigned to the Header or Footer target workspace property through the Link Wizard rather than by editing the Title text field for the Header or Footer region on the Style panel of the Properties Dialog. Whatever expression is assigned to the target workspace property through the Link Wizard will override the Title text entered in the Style panel when the workspace is reached through the link. This problem was reported against Tivoli Management Portal v1.9.6 but also applies to the Tivoli Enterprise Portal v6.1.0, v6.2.0, v6.1.1, and v6.2.2.

Unresolved variables in custom queries

Whenever you assign a custom query containing $-delimited symbol references to a view through the Properties window, a popup appears asking for values for all symbol references for which a value cannot be found. The values provided through this window are used to parameterize the query issued to fill the Preview pane of the Properties window. The values provided will NOT be saved in the workspace state although they will remain defined from when the Properties window is dismissed until the workspace is refreshed.

The reason for the prompt for values is to allow the author of the query/workspace to test whether or not the query returns the expected result set for the provided values. The values are optional and need not be provided in order to complete the assignment of the query to the view. The only impact of not providing values is that the query triggers a syntax error when executed by the Properties window Preview pane and the view is empty. In order for the query to work correctly in the workspace, values must be provided for all the referenced symbols through the execution environment. Typically, this is done by reaching the workspace through a link that either explicitly or implicitly assigns values to the symbols. It can also be done through special controls like the Timespan window, but these must be built into the product.

Custom query processing differs from 'standard' query processing in that, for custom queries, a value must be provided for every symbol reference while, for 'standard' queries, the system discards segments of the WHERE clause involving symbols for which a non-null value cannot be found. In order to support historical queries against summarized data, various agent groups distribute product-provided custom queries that reference symbols that are meant to be provided by the Timespan window when the 'Use summarized data' option is selected. These queries are used with the product-provided 'Historical Summarized ...' workspaces available from the Workspaces menu of the Operating System summary workspaces like 'Windows Systems'.

In order for the queries to return data, the Warehouse Proxy and Summarization and Pruning agents must be configured and have been running long enough to collect and summarize the data being viewed. The queries reference a number of symbols. Following are some of the commonly referenced symbols and example values:

KFW_USER: Name of the summarized database schema owner. Default is ITMUSER but it can be any value assigned by the customer during installation.

SHIFTPERIOD: Indicator of shifts to include. -1 = AllShifts, 1 = OffPeak, 2 = Peak

VACATIONPERIOD: Indicator of vacation days to include. -1 = AllDays, 0 = WorkDays, 1 = VacationDays

TIMESPAN: Set of values captured by the Timespan window. It is not practical to construct this directly.

SUMMARY_DAY: Day to select. A string in the format YYYY/MM/DD. The following is an example link wizard expression that can build such a string value from the a TEP 16 character timestamp attribute value (assuming years in the 20yy range):

dt = $knt.Processor:ATTRIBUTE.NTPROCSSR_H.WRITETIME$; yyyy = "20" + STR(dt, 2, 2); mm = STR(dt, 4, 2); dd = STR(dt, 6, 2); yyyy + "/" + mm + "/" + dd

SUMMARY_WEEK: First day of week to select. A string in the format YYYY/MM/DD

Because of the open-ended nature of the custom queries and their provision by multiple agent groups, it is possible that other symbols might also be used. One way to understand what values are required is to save a copy of the query and edit it to remove clauses involving the symbols. When the modified query is assigned to a view (assuming any syntax errors are overcome), it should return an unfiltered view of the table. The values in the table, in conjunction with close examination of the query text, can be used as a guide to what to provide as filter values.

Another symbol that has been specifically asked about is $Server_Name$. This is the name of the server of interest. If the workspace is below the agent level in the navigator tree, $NODE$ will usually return an appropriate value. If the value is being provided through a link, it can often be picked from the Server Name attribute of the link source row. When in doubt, examining a display of the unfiltered table can help determine what is expected.

In summary, it should be emphasized that the product-provided workspaces based on these queries should be used whenever possible.

A message appears after accepting the license

UNIX only During installation of the Monitoring Agent, immediately after accepting the license agreement, a message similar to the `lslpp:` message shown below may be displayed:

```
Press Enter to continue viewing the license
agreement, or enter "1" to accept the
agreement, "2" to decline it, "3" to print it,
"4" to read non-IBM terms, or "99" to
go back to the previous screen.
1
lslpp: Fileset gsksa.rte not installed.
```

This message is harmless and is associated with verifying the versions of the gskit component installed by IBM Tivoli Monitoring. The message is displayed at a point where the UNIX install normally pauses for a number of seconds, causing a tendency to think the install has failed, although this is not the case.

Do not interrupt or cancel the installation process at this point, wait for the installation prompts to continue after the message is displayed and proceed to finish the installation as you normally would.

Adding agent help files requires a restart of the Eclipse Help Server and the Tivoli Enterprise Portal Server

When an agent's online help files are added to the eclipse server, they are not available until the eclipse help server is restarted. This also requires a restart of the Tivoli Enterprise Portal Server.

Unable to create historical collection directory for ud:db2inst1

If you receive the following message, check if the IBM Tivoli Monitoring environment is in SecureMode.

```
db2inst1@amsnt148d:/opt/IBM/ITM/bin> ./itmcmd agent -o db2inst1 start ud
Sourcing db2profile for user db2inst1
Starting Monitoring Agent for DB2 ...
KCIIN0174E Unable to create historical collection directory for ud:db2inst1
```

There are two possible fixes for this problem. Either manually set the file permission to history dir, or add the db2 instance user to the root group. See the *IBM Tivoli Monitoring Installation and Setup Guide* for instructions on how to have monitoring agents work properly with SecureMain in place.

Receive a large amount of data back from the warehouse for a baseline command

The variable, TACMD_JVM_MAX_MEMORY must be more than 256 and less than 2048. The command defaults to 256 megabytes of heap space for the JVM.

Chapter 11. IBM Tivoli Performance Analyzer troubleshooting

This chapter describes problems you might experience with the IBM Tivoli Performance Analyzer.

Enabling logging

Enable logging to collect information about problems that might occur. You can then send the information to the IBM support team, or use it to determine the cause of the problem.

About this task

Two areas within the Performance Analyzer are logged: the agent and the portal plug-in.

Enabling logging for the agent

If you experience any problems with the Performance Analyzer agent, you can turn on detailed logging with debugging to discover the cause.

About this task

Note: Logging with debugging has a significant impact on performance of the agent. Use logging with debugging turned on only when solving a problem, and switch it off afterwards.

The log files for the agent are created in the `$ITMinstall_dir\TMAITM6\logs` (Windows) or `$ITMinstall_dir/logs` (other platforms) directory.

Procedure

1. Stop the Performance Analyzer agent.
   - On Windows platforms, click **Start** > **Programs** > **IBM Tivoli Monitoring** > **Manage Tivoli Monitoring Services**, then right-click on **Performance Analyzer** and select **Stop**.
   - On other platforms, enter the `itmcmd agent stop pa` command.
2. Open the `init.cfg` file. Depending on your operating system, the file is located in the following directory:

   Windows
   `$ITMinstall_dir\TMAITM6\config`

   Linux `$ITMinstall_dir/li6263/pa/config`

   AIX `$ITMinstall_dir/aix533/pa/config`

   Solaris
   `$ITMinstall_dir/sol283/pa/config`
3. Update the **LogLevel** and **LogSize** parameters:

   ```
   LogLevel=Debug
   LogSize=10000000
   ```
4. Start the Performance Analyzer agent.

- On Windows platforms, click **Start** > **Programs** > **IBM Tivoli Monitoring** > **Manage Tivoli Monitoring Services**, then right-click on **Performance Analyzer** and select **Start**.
- On other platforms, enter the `itmcmd agent start pa` command.

Logging with debugging is enabled for the agent.

5. Wait until the `Waiting for a period of 60000` message appears in the `kpacma.log` file. The message means that the processing cycle of the agent is over.
6. If you want to send the log files to support, stop the agent, compress the *kpacma*.log* files to `itpa_agent_log1.zip` and send it.
7. Restore the default values to the **LogLevel** and **LogSize** parameters:

```
LogLevel=Warning
LogSize=1000000
```

8. Restart the agent.

Enabling logging for the portal

You can turn on logging to discover the cause of any problems with the Performance Analyzer UI in TEP.

Procedure

1. Stop the Performance Analyzer agent.
   - On Windows platforms, click **Start** > **Programs** > **IBM Tivoli Monitoring** > **Manage Tivoli Monitoring Services**, then right-click on **Performance Analyzer** and select **Stop**.
   - On other platforms, enter the `itmcmd agent stop pa` command.
2. Open the `logging.properties` file, located in the *<home_directory>*`/IBM/Java142/jre/lib` directory.
3. Comment out the `handlers= java.util.logging.ConsoleHandler`:

```
#handlers= java.util.logging.ConsoleHandler
```

line

4. Uncomment the `#handlers= java.util.logging.FileHandler, java.util.logging.ConsoleHandler`:

```
handlers= java.util.logging.FileHandler, java.util.logging.ConsoleHandler
```

line

5. Edit the values of the `java.util.logging.FileHandler.limit` and `java.util.logging.FileHandler.count` properties in the following way:

```
java.util.logging.FileHandler.limit = 5000000
java.util.logging.FileHandler.count = 1
```

6. Add the

```
com.ibm.tivoli.pa.config.level = FINEST
```

line

7. Verify that the value of the `java.util.logging.FileHandler.pattern` property is set to `%h/java%u.log`, where *%h* is the path to your home directory. This property determines the location where log files are created.
8. Save and close the file.

Results

Detailed logging has been enabled.

What to do next

If you want to send the log files to IBM Software Support, start the TEP desktop client and perform steps to reproduce the error, and then go to the user home directory, where *java*.log.** files are created. Compress the files to `itpa_agent_log1.zip` and send it to IBM Software Support.

Troubleshooting the installation

If you are experiencing difficulties after installing and configuring Tivoli Performance Analyzer , first review the following information:

After upgrading, the previous version of the Performance Analyzer is shown in the Performance Analyzer Configuration window, and task names are not displayed correctly

The problem occurs on Windows platforms, when Tivoli Enterprise Portal was running during the upgrade process.

To resolve this issue, you should upgrade Tivoli Performance Analyzer again, making sure that Tivoli Enterprise Portal is not running.

After upgrading, the names of workspace groups in the Performance Analyzer Warehouse Agent node in the Navigator view are not displayed correctly

The problem occurs on Windows platforms, when Tivoli Enterprise Portal was running during the upgrade process.

To resolve this issue, you should upgrade Tivoli Performance Analyzer again, making sure that Tivoli Enterprise Portal is not running.

Tivoli Performance Analyzer graphical user interface for Tivoli Enterprise Portal fails when downloading tasks list

If your Tivoli Enterprise Portal Server database runs DB2 on an AIX system, and the Tivoli Performance Analyzer graphical user interface in Tivoli Enterprise Portal fails while loading the tasks list, look in the Tivoli Enterprise Portal Server log for the following message from the command-line interface driver with a code of SQL1224N:

```
 [IBM][CLI Driver] SQL1224N A database agent could not be started to
service  a request, or was terminated as a result of a database
system shutdown or a  force command.  SQLSTATE=55032b
```

This message indicates that DB2 has exhausted all available shared memory segments. To resolve this problem, you must configure your DB2 server to support extended shared memory. To enable this support, complete the following steps:

1. From DB2 command prompt, run the following command:

```
export EXTSHM=ON
db2set DB2ENVLIST=EXTSHM
db2set –all
```

2. Edit `cq.ini` file in `<itm_dir>/config/` and at the end of the file add this line:
   ```
   EXTSHM=ON
   ```
3. Restart TEPS and DB2.

When tasks are started and when you should see data in the workspaces

Tasks are run when the Analytic Agent starts and during each time period specified for the task. Depending on your data collection size and database server performance, you can expect to see data within 5 - 30 minutes. However, if you have not previously activated the Summarization and Pruning Agent and you use the default daily schedule of 2 a.m., you might need to run the agent overnight before summary tables are created and workspaces populated.

No data is displayed in the workspaces

If after running Analytic Agent overnight, you do not have any data, confirm the answers to following questions:

- Check the Performance Analyzer Agent Statistics workspace. Have all tasks completed successfully? If not, read the error messages to identify the source of the problem.
- Is the Summarization and Pruning Agent active? This agent is required by Tivoli Performance Analyzer.
- After installing Tivoli Performance Analyzer, did you configure historical data collection? For more information, see the "Configuring historical data collection for the Performance Analyzer warehouse agent" section in the *IBM Tivoli Monitoring: Installation and Setup Guide*.

If the agent is active and historical data collection is configured, your configuration may be wrong. Confirm the answers to following questions:

- Is the connection configuration information for the Tivoli Enterprise Portal Server and Tivoli Data Warehouse correct?
- Is the Performance Analyzer Warehouse agent running?
- If you installed on a distributed system did you install the correct support files on each workstation?

The Tivoli Performance Analyzer workspaces are not available or not displayed

If the workspaces are not visible at all, the connection to the Tivoli Enterprise Monitoring Server is not configured correctly.

If the workspaces are visible but unavailable, the Analytic Agent ran in the past but conditions have changed: either the agent is no longer running or the connection configuration for Tivoli Enterprise Monitoring Server has changed.

No chart is visible on the Forecast Details workspace

Configure historical data collection for Tivoli Performance Analyzer attribute groups. For more information, see the "Configuring historical data collection for the Performance Analyzer warehouse agent" section in the *IBM Tivoli Monitoring: Installation and Setup Guide*.

The Performance Analyzer Agent Statistics workspace shows database errors indicating that some tables or views are missing

Try the following solutions:

- See the "Configuring historical data collection for the Performance Analyzer warehouse agent" section in the *IBM Tivoli Monitoring: Installation and Setup Guide*.
- Check if the database schema for Tivoli Data Warehouse is the same as the username used by Summarization and Pruning Agent.
- Verify that the user specified during the Tivoli Performance Analyzer configuration has the appropriate rights to select data from tables and views in the database schema where Tivoli Data Warehouse tables and views are created.

The Tivoli Enterprise Monitoring Server does not restart after installation of Domain Support

This problem may occur on Windows because of a corrupted Tivoli Enterprise Monitoring Server catalog database after you install or upgrade Tivoli Performance Analyzer and then launch the domain support tool. If the monitoring server cannot be started, complete the following steps:

1. Copy the two files: `QA1CDSCA.DB` and `QA1CDSCA.IDX` from `<itm>\BACKUP\<latest timestamp>\CMS` to `<itm>\CMS`
2. Start Tivoli Enterprise Monitoring Server.

After completing these two steps, the catalog database is restored and the monitoring server works correctly. No data is lost in the process.

Chapter 12. Command troubleshooting

This chapter describes problems you might experience with commands.

On Solaris 8 operating systems, checkprereq processes do not complete

If a prerequisite check is executed for an agent on a UNIX or Linux endpoint, either with the **tacmd checkprereq** command or the **tacmd createnode** command with the *-o EXECPREREQCHECK=Y* command-line option, certain processes might not complete. If you supply a Windows-syntax installation directory (for example, *C:\IBM\ITM*) with either the **-d | --directory** flag or the group deployment property (*KDY.INSTALLDIR=C:\IBM\ITM*), the execution of the prerequisite check on the endpoint might hang some processes on UNIX or Linux operating systems. However, if you observe this situation in your enviroment, you can end those processes without causing additional problems. To avoid this issue, provide the prerequisite check with the appropriate directory syntax for UNIX and Linux (for example, */opt/IBM/ITM*).

Situations deleted from the CLI are still listed on Tivoli Enterprise Portal Situation editor

If you stop your hub Tivoli Enterprise Monitoring Server (TEMS) and then delete situations using tacmd deletesit, the situations are deleted from the CLI, but are still listed on the Tivoli Enterprise Portal (TEP) Situation editor. To avoid this issue, delete situations from the CLI while the TEMS is running. As appropriate, the situations do not display on the Situation editor.

The tacmd addBundles command returns an unexpected KUICAB010E error message

Using the **tacmd addBundles** command results in an unexpected error message:

```
KUICAB010E: The addBundles command did not complete.
Refer to the following returned error: ERRORTEXT
```

The **tacmd addBundles** command is used to add one or more deployment bundles to the local agent deployment depot. By default, this command also adds all deployment bundles that are prerequisites of the deployment bundle being added, if the prerequisite bundles do not already exist in the depot. The **tacmd addBundles** command requires double the size of the bundle disk space free in the depot (including the agent and all prerequisite bundles). The kdyjava.log file in the system temp directory provides additional information about the problem.

tacmd removeBundles command returns unnexpected KUICRB010E error message

Using the **tacmd removeBundles** command results in an unexpected error message:

```
KUICRB010E: The removeBundles command did not complete.
Refer to the following returned error: ERRORTEXT
```

The **tacmd removeBundles** command is used to remove one or more deployment bundles from the local agent deployment depot. The **tacmd removeBundles** command requires double the size of the bundle disk space free in the depot. The kdyjava.log file in the system temp directory provides additional information about the problem.

tacmd executecommand command run against subnode fails

Subnodes are not enabled for the **tacmd executecommand** command to execute the system command provided in the given command. The subnode might be registered to run on a system or environment different from that of the the agent. In this case, the monitoring agent does not track where the subnode is running, or how to execute a command on that specific system or environment.

By not enabling the enhanced command execution for subnodes, you can avoid this issue. Instead, you can use the **tacmd executecommand** command against a subnode manager agent that controls the subnode.

The krarloff command returns an error message

The krarloff rolloff program can be run either at the Tivoli Enterprise Monitoring Server or in the directory where the monitoring agent is running, from the directory in which the history files are stored. For more information about the krarloff command, see "Converting files using the krarloff program" in the *IBM Tivoli Monitoring V6.2.2 Administator's Guide*: http://publib.boulder.ibm.com/infocenter/tivihelp/v15r1/index.jsp?topic=/com.ibm.itm.doc_6.2.2/history_krarloffwindows.htm.

Unexpected KUIC02013E error message

When running on an operating system that is configured for locales that do not conform to the Language_Locale convention, the tacmd command returns the following message:

```
KUIC02013E: The software did not run the command because of a
internal system error. Contact the system administrator.
```

The IBM Tivoli Monitoring command line environment expects the system to be running in the Language_Locale convention, and is currently limited from understanding other conventions. You can verify this problem by viewing the kuiras1 log and looking for entries similar to the following:

```
(4C765377.008E-1:nls2.c,491,"NLS2_GetLocale") Entry
(4C765377.008F-1:nls2.c,494,"NLS2_GetLocale") Input parameters: languageId 0,
codepage 0, options 0.
(4C765377.0090-1:nls2.c,507,"NLS2_GetLocale") Zero language Id and codepage
defined.
(4C765377.0091-1:nls2.c,3888,"NLS2_allocateLocale") Entry
(4C765377.0092-1:nls2.c,3907,"NLS2_allocateLocale") Preparing to initialize
Locale structure.
(4C765377.0093-1:nls2.c,3980,"NLS2_initLocaleObject") Entry
(4C765377.0094-1:nls2.c,3983,"NLS2_initLocaleObject") Get the current native
locale.
(4C765377.0095-1:nls2.c,3991,"NLS2_initLocaleObject") Locale returned is
turkish.
(4C765377.0096-1:nls2.c,4000,"NLS2_initLocaleObject") Getting the locale
basename.
(4C765377.0097-1:nls2.c,4022,"NLS2_initLocaleObject") Locale basename is
turkish.
(4C765377.0098-1:nls2.c,4024,"NLS2_initLocaleObject") Locate locale basename in
table.
```

```
(4C765377.0099-1:nls2.c,4042,"NLS2_initLocaleObject") Basename not found in table.
Not valid Locale name.
(4C765377.009A-1:nls2.c,4043,"NLS2_initLocaleObject") Exit: 0x25
```

To solve this problem, convert your system to the equivalent Language_Locale convention. In the example above, use the tr_TR locale.

Missing options for login -stdin results in unexpected behavior

For both the **tacmd login** and the **tacmd tepslogin** commands, if the -stdin option is used, and an echo is used to pass the options, then all the mandatory options need to be passed in the echo. For example, the following options are allowed:

```
echo "-s localhost -u .... -p ..." | tacmd login -stdin
```

And, the following options are not allowed:

```
echo "-s localhost" | tacmd login -stdin
```

A system error occurs with the tacmd editsystemlist -e command

You receive the following message:

```
KUIC02013E: The software did not run the command because of a internal system error.
 Contact the system administrator.
```

Edit the .xml file to be well formed. For example, when running the **tacmd viewsystemlist -l** *mslname* **-e** *filename* command, the command produces a `testmsl.xml` with these contents:

```
<TABLE>
<ROW>
<NODELIST>testmsl</NODELIST>
<AFFINITIES>0008000000000000000000000000000000000000</AFFINITIES>
<NODE>Primary:CLISOAP:NT</NODE>
</ROW>
</TABLE>
```

Then if you run the **tacmd editsystemlist -e testmsl.xml -a** *managed_system_name* command, the command runs as expected, producing a new `testmsl.xml` file that contains the *managed_system_name*:

```
<TABLE>
<ROW>
<NODELIST>testmsl</NODELIST>
<AFFINITIES>0008000000000000000000000000000000000000</AFFINITIES>
<NODE>Primary:CLISOAP:NT,Primary:managed_system_name</NODE>
</ROW>
</TABLE>
```

Problem running the tacmd listsystemlist -d command on Linux systems

When running the **tacmd listsystemlist -d** command with any of the semicolon (;), asterisk (*), number sign (#), or tilde (~) characters, you receive the following message:

```
KUIC02002E: The argument for the -d option is missing.
```

Change the delimiter to another character or escape these characters with a backslash (\). The following example escapes a semicolon (;):

```
./tacmd listsystemlist -d \;
```

Commands with embedded single quotation marks fail

The commands executeaction and executecommand fail if they contain single quotation marks. Also, commands that contain embedded single quotation marks and a right curly brace also fail.

There is no workaround at this time.

tacmd exportnavigator -o not behaving correctly

This option should export only the custom navigator view. Workspaces, queries, and situation associations referenced within the custom navigator view should not be exported. However, if you reimport the navigator view using the xml generated using the -o option, the customizations showed up on the custom navigator view in the Tivoli Enterprise Portal. This behavior occurs because this option does not delete the customizations from the portal server database.

TACMD xxxxAction commands fail on Japanese systems

The following commands fail on Japanese systems:

- tacmd createAction
- tacmd viewAction
- tacmd editAction
- tacmd executeAction

Run the command with LANG=C or LANG=Ja_JP.UTF-8. Edit the kuixxxxactionVld.xml, removing the dash (-). For example, change the following:

```
<ActionName arg1="-n" arg2="--name" Type="String"
ValidationRegExp="[A-Za-z0-9 _:.\-()/]" Required="Y"/>
```

to:

```
<ActionName     arg1="-n"  arg2="--name" Type="String"
ValidationRegExp="[A-Za-z0-9 _:.\()/]" Required="Y"/>
```

Overrides set against an agent cannot be deleted from the command line

It appears as though the override does not exist when deleting, however it allows you to list (**listOverride**) and even modify (**setOverride**) the override. If you use the **setOverride** command, using a predicate of 99, for example, the agent applies this value as 99.0. If you then try the **deleteOverride** command using 99 rather than 99.0, the command does not find a matching override, and it fails. If you read the **listOverrides** command output and use the reported values to run the **deleteOverride** command, the override is deleted.

tacmd listsit -m UX *Managed System* gives no result

The **tacmd listsit** command on AIX systems gives no results as shown below:

```
-------------------------------------------------------
tacmd listsit -m UX Managed System gives no result.
Return code = 255.
-------------------------------------------------------
```

This behavior might be caused by an OUT OF MEMORY condition on the AIX system where the command is issued due to specific AIX memory management. This problem can be solved by setting the environment variable, LDR_CNTRL=MAXDATA=0x80000000, to be exported in the shell from which the tacmd command is issued:

```
export LDR_CNTRL=MAXDATA=0x80000000
```

Receive a busy monitoring server message when using the getfile, putfile, or executecommand commands

If you receive a busy monitoring server message, there are too many file transfers in progress. Wait until some of the transfers complete, and then retry your command. The following error messages are received for the respective commands:

For the getfile command:

```
KUIGTF111E: Monitoring server is too busy.
```

For the putfile command:

```
KUIPTF111E: Monitoring server is too busy.
```

For the executecommand command:

```
KUIPTF111E: Monitoring server is too busy.
```

Reconfiguring an agent and then getting the deploy status yields a port number message

When reconfiguring an agent by running the **tacmd configuresystem** command, a subsequent **tacmd GetDeployStatus** command yields a message like the following:

```
KDY0030E: lookupUAPort failed. Operation to determine the port number used by
Universal Agent agent was not successful.
```

If installing from images on an NFS mount, the NFS mounts need world execute permissions to be accessible by the process doing the distribution.

tacmd getfile or putfile command is failing

On UNIX and Linux systems, either of these commands fail if the requested file's size is larger than the user limit file size defined by the ulimit command. When using the **tacmd getfile** command, ensure that the local system's ulimit -f setting can accommodate the requested file's size. When using the **tacmd putfile** command, ensure that the remote system's ulimit -f setting can accommodate the specified file's size.

Temporary files remain when tacmd getfile or putfile is interrupted

When issuing a **tacmd getfile** command or **tacmd putfile** command, the file is copied as a temporary file to the directory location as specified by the -d|–destination option. If the command is interrupted (for example, if the session is closed), this temporary file is left in the specified directory location. On Windows systems, the temporary file name is prefixed with 'cxm' followed by random characters and has a '.tmp' filetype (for example, cxm1C.tmp). On UNIX systems, the temporary file name is prefixed with 'cxp' followed by alphanumeric characters (for example, cxp5pYmUa.) Over time, this presence of potentially large temporary files could present problems that ultimately result in future **getfile**

command or **putfile** command failures due to lack of space. As a result, any temporary files should be deleted periodically.

Receive an OutOfMemory exception when using the import or export commands

Edit the environment variable "TACMD_JVM_MAX_MEMORY" and override the default maximum JVM memory value size of 256 MB. You can edit the value to be between 256 and 2048, inclusive. Incorrect values or values out of range are disregarded, with an error written to the `kuiras1` trace log.

The suggestbaseline or acceptbaseline commands fail

You receive the following type of error:

```
KUICAC014E The command failed because the Tivoli Data Warehouse did not contain any
historical data for the managed system(s) for attribute
"NT_Process_64.%_Processor_Time" for the specified time period.
```

The warehouse did not contain any historical data from the managed system for the specified situation attribute during the specified time period. The time period is established by the start time and end time, and is further constrained by the calendar entries you specified. In addition, historical data collection must be configured and enabled for the attribute group, and the warehouse proxy agent must be configured and running on the same host as the managed system.

Verify that historical data collection is enabled for the appropriate attribute group and that the warehouse proxy agent is installed and running on the same host(s) as the specified managed system or managed systems.

Problems with Take Action commands and curly brackets

Take Action commands that are created with curly brackets, {}, are not recorded and cannot be selected from the Tivoli Enterprise Portal. This happens only for "}" and not for "{", and only when the backward curly brace is embedded with single quotes.

There has been a change in syntax where attributes that are enclosed in curly brackets, {}, no longer are required to have quotes. See the following example:

```
&{grp1.atr1}.&{grp2.atr2}
```

When configuring the Monitoring Agent for Sybase and the Warehouse Proxy Agent, receive message to use CandleManage

The **CandleManage** command has been deprecated. The message should reference the **./itmcmd manage** command.

listSit command with the type option fails with a KUIC02001E message on Japanese Systems

Edit the `kuilistsitVld.xml` file to replace the following text:

```
<Type    arg1="-t"  arg2="--type"  Type ="String" ValidationRegExp=
"[-A-Za-z0-9 _/()\&%.]" Required="Y"/>
```

with the following text:

```
<Type    arg1="-t"  arg2="--type"  Type ="String" ValidationRegExp=
"[-A-Za-z0-9 _/()\%.]" Required="Y"/>
```

Take Action command names do not accept non-English characters

There is not a workaround at the present time.

addBundles command times out

When using the **addBundles**command to add bundles to a depot, the command might time out. The default timeout is 600 seconds (10 minutes). The following message is returned after successful execution:

```
KUICAB022I: The following bundles were successfully added to the
C:\IBM\ITM\CMS\depot\depot
```

If the **addBundles** command times out, this message is not returned. Set the TIMEOUT environment variable to more than 600 before running the **addBundles** command. For example:

```
#set TIMEOUT=1800
```

You can also reset the TIMEOUT after the command times out. Then run the **addBundle**s command.

You can also change the LAN linkspeed and duplex setting from auto detect to 100Mbps/Full Duplex. Then re-start the addbundle process.

createNode command fails

Table 40 on page 209 provides information to help you recover when the **createNode** command fails.

Table 40. createNode command fails

Symptom	Resolution
The **createNode** command fails on a Windows OS agent from a UNIX or Linux host when using the "-d" option and "\" as the path separator.	Because tacmd on UNIX and Linux is a wrapper script for the createNode command, the character "\" is removed from the command. Specify the path with the "-d" option using either "/" or "\\\\" when you deploy a Windows OS agent from a UNIX/Linux host. The following examples display the correct usage to install the Windows OS agent in the path `C:\ITM61\WIN\OSAgent`: **Windows** C:/ITM61/Win/OSAgent **UNIX or Linux** `c:\\\\ITM61\\\\Win\\\\OSAgent`

tacmd suggestbaseline minimum, maximum, and average function values are ignored

One or more function values entered for either the minimum, maximum, or average parameter is not valid, so these incorrect values are ignored.

tacmd suggestbaseline command receives an error

When using this command, you receive this message:

```
" The specified managed system is not overrideable because it does not have the
appropriate affinity feature bit enabled."
```

The **tacmd suggestbaseline** command does not support pre-IBM Tivoli Monitoring v6.2.1 agents.

When using the listSystems command, the last two digits for the version appear as 'XX'

Extended version information for every agent might not always be available. When this happens, the last two digits of the version displayed are represented as "XX". This occurs for subnode agents or when agents are not enabled for Agent Deploy support.

The command tacmd restartAgent fails if the agent is already stopped

If the **tacmd restartAgent** command is issued against an agent that is stopped, it will generate an error message:

```
# /opt/IBM/ITM/bin/tacmd restartagent -n zpmaix13:KUX -t ul

KUICRA006I: Are you sure you want to restart the UL agent(s) that manage
zpmaix13:KUL?

Enter Y for yes or N for no: Y

KUICRA007I: Restarting UL agent(s).

KUICRA009E: A problem occurred while restarting UL - refer to the following error
returned from the server:

The monitoring server encountered an error while restarting the managed system.

If the error information returned from the server is not sufficient to help you
resolve the error, contact IBM Software Support.

The command /opt/IBM/ITM/bin/CandleAgent  -h /opt/IBM/ITM -c stop ul did not start
or stop agent.
The command returned a return code.

Enable Deployment trace logging on the agent machine. Contact Customer Service
for details on this procedure. Collect the following log files
        On Windows the log kdsmain.msg log is located in the {CANDLEHOME}\CMS
directory and {hostname}_ms_{timestamp}-XX.log files are located in
CANDLEHOME\logs directory.
        On Unix-Based systems the logs {hostname}_{timestamp}.log and
{hostname}_ms_{timestamp}-XX.log is located in the {CANDLEHOME}/logs directory.
On the target Managed System Node machine collect the following log files.
        On Windows the logs kdyproc_ras1_{timestamp}.log and {hostname}_nt_kntcma_
{timestamp}-XX.log are located in the {CANDLEHOME}\tmaitm6\logs directory.
        On Unix systems the logs kdyproc_ras1_{timestamp}.log and {hostname}_
ux_kuxagent_{timestamp}-XX.log is located in the {CANDLEHOME}/logs directory.
        On Linux systems the logs kdyproc_ras1_{timestamp}.log and {hostname}_
lz_klzagent_{timestamp}-XX.log is located in the {CANDLEHOME}/logs directory.
Refer to IBM Tivoli Monitoring v 6.2 Problem Determination Guide
for more information.
```

The user can verify the agent is stopped by running **tacmd listSystems**:

```
# /opt/IBM/ITM/bin/tacmd listsystems
Managed System Name             Product Code Version     Status
zpmaix13:KUL                    UL           06.20.00.00 N
```

```
zpmaix13:08                       08          06.20.00.00 Y
amshp16.tivlab.raleigh.ibm.com:K UX           06.20.00.00 Y
TEMS_zpmaix13                     EM          06.20.00.00 Y
```

To start the agent, user can issue **tacmd startAgent**:

```
/opt/IBM/ITM/bin/tacmd startagent -n zpmaix13:KUX -t ul
```

Using the kinconfig command and remotely starting, stopping or recycling agents fails on Windows 2000 systems

If the endpoint is a Windows 2000 systems, you must reboot the system after the Monitoring Agent for Windows is installed to allow environment variables that have been set by the OS Agent's installation to take effect for other processes to use these variables.

You receive a message when using a tacmd command related to agents

You receive the following message:

```
KDY0010E: The agent bundle product_code was not found in the agent bundle depot on
TivoliEnterpiseMonitoringServer_Name. The agent bundle specified for deployment
is not installed on the agent bundle depot for the target
operating system.
```

This occurs when using a tacmd command related to agents like **tacmd getdeploystatus** or **tacmd addsystem**.

Ensure that you are using the right format for the product code. It must be a 2 digit product code, as in 'um' for the Universal Agent, and not 'kum'.

You receive a message when trying to use the tacmd maintagent command

The **tacmd maintAgent** command is disabled for the IBM Tivoli Monitoring v6.2.2 release. The command stops and starts situations on individual agents without notifying the Tivoli Enterprise Portal Server or Tivoli Enterprise Monitoring Server, therefore the Tivoli Enterprise Portal Server or the Tivoli Enterprise Monitoring Server can potentially lose track of the state of the situation on the agent. After running the **maintAgent** command, the only way to check if the situation is running is to look at the agent's startup log.

Endpoint fails to connect to monitoring server when running createnode from a monitoring server in a different domain

When running the **tacmd createnode** command from a hub or remote monitoring server to an endpoint that is in a different domain than the connecting monitoring server, the endpoint might fail to connect back to the monitoring server. If the failure occurs, it could be due to the fact that the endpoint cannot resolve the provided hostname to the fully-qualified hostname for example, the hostname is itmserver and the fully-qualified hostname is itmserver.raleigh.ibm.com).

Either update the systems host tables and correctly setup the DNS domain search so that the link between itmserver and itmserver.raleigh.ibm.com can be made, or supply the monitoring server fully-qualified hostname during the createnode deployment using the SERVER=itmserver.raleigh.ibm.com property.

Take Action commands do not work if unrequired values are left blank

The predefined Take Action commands work if None is provided in the keyword and the value fields after at least one database (manager) configuration parameter config-keyword value that you wish to update has been provided.

Take Action commands do not display messages when run from a Navigator Item or from a workspace view

Take Action commands do not display messages when run from a Navigator Item or from a workspace view for return codes 0, -1, or 4. The destination and return code is displayed, but not the message for the return code.

Corrupted tacmd responses are displayed in the command-line interface

With the default code page setting, some systems might display corrupted characters for the following tacmd commands:

- histconfiguregroups
- histcreatecollection
- histdeletecollection
- histeditcollection
- histlistattributegroups
- histlistcollections
- histlistproduct
- histstartcollection
- histstopcollection
- histunconfiguregroups
- histviewattributegroup
- histviewcollection
- exportcalendarentries
- importcalendarentries
- createsitassociation
- deletesitassociation
- listSitAssociations
- exportsitassociations
- importSitAssociations
- createsysassignment
- deletesysassignment
- listsysassignments
- exportsysassignments
- importsysassignments
- suggestBaseline
- acceptBaseline
- setOverride
- listOverrides
- deleteOverride

This problem has to do with your locale and system configuration, and can be fixed by performing the following procedure:

1. Open the command prompt.
2. Change the command prompt locale according to the following table:
3.

Country	Code Page Default Setting	New Code Page Value
Latin 1 - Brazilian Portuguese, French, German, Italian, Spanish	850	1252
Latin 2- Czech, Hungarian, Polish	852	1250
Russian	866	1251

a. To change the locale in the command prompt, type `chcp ****` in the command prompt, where **** is the new value for your code page, and press enter. For example, if your system locale is Latin 2, type `chcp 1250` in the command prompt.
b. To check the results of this change, type `chcp` and press enter. The command prompt will display the following message:

   ```
   Active code page: ****
   ```

   If the value displayed after `Active code page` is the same as the value you just entered, then you have successfully changed the settings. For example, if your system locale is Latin 2, the command prompt should display the message:

   ```
   Active code page: 1250
   ```

4. Change the font displayed within the command prompt.
   a. You can do this by right-clicking the title bar and clicking **Properties** from the drop-down menu.
   b. Click the Font tab and select `Lucida Console` from the list of fonts in the window.
   c. Click **OK**.
   d. A window will appear, allowing you to select the windows to apply the font change to. Select **Modify shortcut that started this window** and click **OK**.
5. You should no longer see corrupted characters in the CLI.

The listSystems command consumes high CPU in enterprise environments

In enterprise environments with many managed systems, high CPU consumption is expected behavior for the **listSytems** command.

Improving tacmd command response time when using VMWare

If you experience slow response time when invoking the tacmd command while running on a VMWare ESX system, consider disabling virtualization of the Time Stamp Counter (TSC). To make this change, add the following setting in the .vmx configuration file for the virtual system where the tacmd command is being invoked.

```
monitor_control.virtual_rdtsc = false
```

This parameter is described in the "Timekeeping in VMWare Virtual Machines" paper on the VMWare Web site at http://www.vmware.com/pdf/vmware_timekeeping.pdf. Measurement experience has shown that this setting can significantly improve the tacmd command response time on VMWare ESX systems.

The addSystem command fails with error message KUICCR099E

The KUICCR099E error occurs when at least one incorrect parameter was specified. When adding managed systems with the addSystem command, ensure that you

- Specify the correct product code.
- Specify a correct node that is online. You can run the **listsSystems** command to verify that the node is online.
- Specify correct properties.

```
tacmd addSystem {-t|--type} TYPE
[{{-n|--node} MANAGED-OS} |
{{-d|--dir|--directory} NODEDIR}}} ]
[{-i|--imagePath} IMAGEPATH]
[{-p|--property|--properties} NAME=VALUE ...]
```

where:

-t | --type
Specifies the type of managed system to add to the monitoring system. You can specify a managed system type name or its associated two-character code. Use **viewDepot** to display a list of correct managed system types.

-n | --node
Specifies the node to start. A node is identified by the managed operating system that it contains.

MANAGED-OS
Specifies a correct managed operating systems.

-d | --dir | --directory} NODEDIR
Specified the correct name of the directory that contains the node components, including the OS agent. This syntax is only correct when the node is on the local system.

-i | --imagePath
Specified the correct directory that contains agent install images.

-p | --property | --properties
Specifies one or more NAME=VALUE pairs that identify configuration properties of the new system and their values. Run the **describeSystemType** command to determine correct values for the properties.

The tacmd getdeploystatus command is not returning status return codes

At this time, there is not a workaround for this issue.

tacmd createSit does not send errors if you mistype the name of an attribute

The tacmd createSit command enables you to create situations without using the Tivoli Enterprise Portal. However, if you mistype the name of an attribute when using this command, you do not receive an error. The situation is created, skipping the attribute that you meant to type in the command. If the created situation had, for example, 6 attributes to monitor, the new created situation has only 5 if you made a mistake in typing 1 of the attribute names in the command.

If you are using the IBM Tivoli Monitoring command line tacmd createSit function for situation creation, you can use the Situation editor in the Tivoli Enterprise Portal to validate your specified attributes.

wsadmin commands' output indicates the wrong server name

When the wsadmin commands are run, the output indicates to restart server1, which is the default name for WAS server. However, the eWAS server for IBM Tivoli Monitoring is called ITMServer.

```
C:\ibm\ITM\CNPSJ\profiles\ITMProfile\bin>wsadmin -connType NONE
WASX7357I: By request, this scripting client is not connected to any server process.
C TEPSEWASBundle loaded.
WASX7029I: For help, enter: "$Help help"
wsadmin>securityoff
LOCAL OS security is off now but you need to restart server1 to make it affected.
```

Restart the server by its correct name whether that is the default name or not.

When using the viewuser command, you receive a message that an option is repeating

The -v, -p -a, and -o options for this command are mutually exclusive. If you enter more than one, you will receive a message that the second option entered is repeating. For example:

```
C:\IBM\ITM\bin>tacmd viewuser -u sysadmin -w mypassword -a -v

   KUIC02022E: The command did not complete because -v option is repeating.
```

Commands fail when a situation name consists of characters

When using the **"** character while executing commands, you must use the escape character \. This is a general command line restriction. For example:

```
[root@vger ksh]# tacmd createsit -s abc\"123 -b Linux_Process_High_Cpu
```

tacmd addSystem fails if agent already exists

When using the command **tacmd addSystem** to install an existing instance of the agent. The expected result would be a message saying that the agent is already installed. The actual results are that a message does not appear, and the installation does not overwrite the existing agent.

Installing an exported agent bundle using install.sh causes an error

Attempting to execute the interactive `install.sh` script found within the output directory of the **tacmd exportBundle -o LOCAL** command results in the following error message:

```
[root@sdogoff ud_062000000_li6263]# ./install.sh
INSTALL

Enter the name of the IBM Tivoli Monitoring directory
[ default = /opt/IBM/ITM ]:

ITM home directory "/opt/IBM/ITM" already exists.
OK to use it [ 1-yes, 2-no; "1" is default ]?

Select one of the following:
```

```
1) Install products to the local host.
2) Install products to depot for remote deployment (requires TEMS).
3) Install TEMS support for remote seeding
4) Exit install.

Please enter a valid number:  1

Initializing ...

Do you agree to the terms of the license in file LICENSE.TXT on the CD?
1-yes, 2-no, 3- to read the agreement now.
(choosing "2" exits the installation process) (1/2/3): 1
You are not entitled to install from this media. Setup will not proceed.
[root@sdogoff ud_062000000_li6263]#
```

Many interactive elements have been removed from the agent bundle output of the **tacmd exportBundle -o LOCAL** command in order to optimize it for remote transmission and silent execution using software distribution technologies. In order to install the exported agent bundle, the `silentInstall.sh` or `silentInstall.bat` script available in the destination directory should be run instead.

The addbundles command fails

You receive a message that says that an error occurred attempting to add the specified bundle to the depot.

You should upgrade the monitoring server before upgrading agents.

The exportBundles command does not work for patches

This command should not be used to install patches.

Chapter 13. Universal Agent troubleshooting

This chapter describes problems that might occur with the Universal Agent.

Preliminary Universal Agent troubleshooting

Correct operation of the IBM Tivoli Monitoring requires correct application data definitions, environment variables, and Tivoli Enterprise Monitoring Server and Tivoli Enterprise Portal configuration. Many problems are caused by incorrectly formatted data or data interpretation. Therefore, begin Universal Agent troubleshooting with the data provider.

Review the following list of fundamental Universal Agent troubleshooting tasks.

- Validate the metafiles using the console command VALIDATE. Review the validation messages and report. Resolve all identified errors and warnings. Because the IBM Tivoli Monitoring calls the same validation subroutines when it loads a metafile, it encounters the same problems as the KUMPCON VALIDATE program.
- Verify that the first three characters of the application name defined in the APPL statement of the metafile are unique throughout the enterprise.
- Verify that the sequence of data fields on the data record matches the listed sequence of attributes in the metafile. In addition, ensure that the attribute type and the maximum data value size correspond to the actual application data values.
- Verify that the actual data fields are delimited exactly as specified in the delimiter specification of the ATTRIBUTES statement. If the delimiter is specified as NONE, ensure that defined attribute value sizes exactly match the data values on the application data record.
- For FILE Data Providers, verify that only one file source (SOURCE FILE statement) is specified for each attribute group (NAME statement) or that you used ManagedSystemName to distinguish the sources.
- For SOCK Data Providers, verify that you have the correct socket source host name (SOURCE SOCK) specified for the application.
- Examine the UAGENT DPLOG report in Tivoli Enterprise Portal. It might include messages that provide clear indications concerning data provider operation and the data source disposition.

Universal Agent does not start

The Universal Agent did not allocate its DCH port 1919 for one of the following reasons:

Table 41. Universal Agent does not start

Problem	Explanation
Another Universal Agent process is running on the same system and the other Universal Agent was not shut down.	The following are the last messages that display in the Universal Agent RAS1 log. `kum0sock.c,110,"KUM0_OpenLocalSocket") bind failed for local address UDP socket 512, port=1919, = error=10048 kum0sock.c,110, "KUM0_OpenLocalSocket") bind failed for local address TCP socket 512, port=1919, error=10048 kumdsock.cpp,964, "ipcSock::allocateDCHport") Error: Could not open TCP/UDP sockets bound to universal agent DCH port 1919 kumdsock.cpp,965,"ipcSock::allocateDCHport") Determine if another copy of Universal Agent is already active on this system. Exiting...`  **Note:** In the RAS1 log above, the Winsock error code 10048 indicates the "Address is in use". On UNIX-based systems platforms, the equivalent "Address in use" error code is usually 125. Run `netstat –a` for more information about port usage on the local system.Stop the other process if it is not required. If the other process is required, set KUMA_DCH_PORT=nnnnn in the `KUMENV` or `um.ini` file. The environment variable causes the Universal Agent to allocate a different DCH port during startup.
There is a non-Universal Agent process running on the same system and the Universal Agent was not shut down.	

The agent fails, but events are still seen as active

It is possible for a situation to remain open for almost four times the sample period before the event closes. For example if a situation had a sample period of 15 minutes the following could occur:

```
The first sample true - 00:00
- sample true - no change in status 15:00
- agent crashes - 15:01
- proxy sends last sample - 30:01
- proxy sends last sample - 45:01
- proxy ends. return no sample 60:00
```

Previously defined situations display in the Tivoli Enterprise Portal with a Problem or Error status

Situations with a problem or error status are most likely the result of running um_cleanup, which deletes the Tivoli Enterprise Portal Server catalog and attribute files and the Tivoli Enterprise Portal Server ODI files for all Universal Agent applications. When the Tivoli Enterprise Portal Server and Tivoli Enterprise Portal server are recycled, they detect situations with no corresponding definition files. These situations are flagged as a problem until the application definition files are regenerated and uploaded again to the Tivoli Enterprise Portal Server and Tivoli Enterprise Portal Server.

All Universal Agent-emitted traps display with the same severity

Many different policy-generated traps are sent by Universal Agent to a 3rd party SNMP Manager product, but all the traps show up with the same severity and it's not the severity specified in the policy definition. Turn on the Universal Agent environment variable KUMP_TRAP_USE_POLICY_SEVERITY:

```
KUMP_TRAP_USE_POLICY_SEVERITY=Y
```

The Managed system version suffix increases

Each time the Universal Agent is restarted, the managed system version suffix for an application is incremented even though the metafile has not changed. There are two metafiles activated that have the same three-character application prefix. If the metafiles are activated one after the other, the Universal Agent determines that the three-character application was modified and registers a new version suffix and upload new CAT, ATR, and ODI files.

Tivoli Enterprise Portal column headings are missing for a Universal Agent application

A Universal Agent application is online to Tivoli Enterprise Portal but all of its column headings are missing in the application workspace.

The Universal Agent-generated CAT, ATR, and ODI files were not uploaded to the Tivoli Enterprise Portal Server and Tivoli Enterprise Portal Server directories. The most current and accurate copies of these definition files are in Universal Agent's work directory. If necessary, you can copy or FTP these files from the work directory to the appropriate Tivoli Enterprise Portal Server and Tivoli Enterprise Portal Server directories.

A variation of this problem is that some of the column headings display but not all of them, or the column headings are incorrect. This could indicate old or out-of-synch CAT, ATR, and ODI files in the Tivoli Enterprise Portal Server and Tivoli Enterprise Portal Server directories. Again, you can always synchronize these files by copying them from the Universal Agent work directory and recycling the Tivoli Enterprise Portal Server and Tivoli Enterprise Portal Server.

Another possible explanation is that Universal Agent is connected to a remote Tivoli Enterprise Portal Server, and the Universal Agent-generated CAT and ATR files for the application didn't get propagated to the hub Tivoli Enterprise Portal Server. Tivoli Enterprise Portal Server only queries the hub Tivoli Enterprise Portal Server, so it's unable to retrieve the data rows. Copy or FTP the Universal Agent-generated CAT and ATR files from the remote Tivoli Enterprise Portal Server to the hub Tivoli Enterprise Portal Server.

Historical data collection for new columns fails for a Universal Agent application

If you update the definition of a Universal Agent application definition by adding new columns, new metafiles are created (the ATR file, in particular). To change the historical data collection to include the new columns, you must recycle the Universal Agent.

Tivoli Enterprise Portal charts and graphs do not work for numeric data

Tivoli Enterprise Portal charts and graphs for a Universal Agent application are empty even though the attributes are defined as "N" in the Universal Agent metafile. The Universal Agent "N" attribute type means DisplayNumeric. It is a string representation of a numeric attribute that can include non-numeric

characters, such as a floating point number or a large number with comma separators. A DisplayNumeric attribute is a string in the ODI file and is not eligible for Tivoli Enterprise Portal charting and graphing. If you want to use a Universal Agent attribute in a chart or graph, define the attribute in the metafile as a true numeric attribute, for example:

- C for Counter
- G for Gauge

kumstrap and kumsnetd processes do not start

After running **itmcmd agent start um** on UNIX-based systems, the following error messages display:

```
elsun02% itmcmd agent start um
itmcmd agent  : installer level 350 / 552.
itmcmd agent  : running sol25 jre.
Starting agent  . . .
Note: Universal agent process kumsnetd did not start.
NOte: UNiversal agent process kumstrap did not start.
Agent Started . . .
```

When you check the Universal Agent RAS1 log file, the following messages display at the bottom:

```
-16:kum0sock.c,132,"KUM0_OpenLocalSocket") bind failed for local address
UDP socket 71, port=162, error=13
-F:kumsrcfg.c,73,"KUMS_ReadNetConfigFromExt")
Network configuration file /control1/dbisk/
candleUa410/sol276/um/work/KUMSNETS open failed,
ErrorText <No such file or directory>. \
Load network configuration bypassed
-18:kbbssge.c,52,"BSS1_GetEnv") KUMP_SNMP_NET_DISCOVER_ENTERPRISE="N"
Network configuration discovery tasks started.
-17:kumsrcfg.c,267,"KUMS_ReadRouterConfigFromExt") Router configuration
file /control1/dbisk/ candleUa410/sol276/um/work/KUMSROUT open failed,
ErrorText <No such file or directory>. \
Load router configuration bypassed 17:kumsrcfg.c,294,
"KUMS_ReadRouterConfigFromExt") 0 router record(s) loaded from router
configuration file /control1/dbisk/candleUa410/sol276/um/work/KUMSROUT
-19:kbbssge.c,52,"BSS1_GetEnv") KUMP_SNMP_MANAGE_LOCAL_NETWORK="N"
-16:kumsplst.c,167,"KUMS_PrepareListenSNMPtrap") *****
Unable to open SNMP trap listen port
-16:kumsplst.c,193,"KUMS_PrepareListenSNMPtrap")
Note: Determine if another SNMP Manager \
process is active on this system.
Monitoring of SNMP traps disabled. No trap receiving port or API available.
Insufficient process authority for executing ICMP procedures.
-17:kum0sock.c,132,"KUM0_OpenLocalSocket") bind failed for local address
 UDP socket 71, port=520, error=13
-17:kumslrtu.c,148,"KUMS_ListenRouterUpdates")
***** unable to open socket with router \
well-known port-17:kum0sock.c,132,"KUM0_OpenLocalSocket")
bind failed for local address UDP socket 73, \
port=520, error=13
-17:kumslrtu.c,148,"KUMS_ListenRouterUpdates")
***** unable to open socket with router well-known port
```

The `error=13` indicates a permission failure. The Universal Agent was not started with a root ID so the trap receiving and router/network discovery processes did not acquire the low-numbered ports needed. The kuma610 continues to run without those two processes.

Note: The kumstrap and kumsnetd processes are required only if you configured the SNMP data provider on a UNIX-based system with the following environment variables specified:

- KUMP_SNMP_MONITOR_TRAP=Y
- KUMP_SNMP_NET_DISCOVERY=Y

You can correct the authorization problem either by doing one of the following:

- Start the Universal Agent with a root ID.

  –OR–

- Use the SetPerm script in the `/bin` directory to grant root access to the kumstrap and kumsnetd binaries.

  If you use the SetPerm script to grant root access to kumstrap and kumsnetd, you do not need to start Universal Agent with a root ID for the two processes to start successfully. Because the kumsnetd process has the necessary root authority to acquire port 520, you can ignore the following error messages in the Universal Agent RAS1 log file:

  ```
  kum0sock.c,134,"KUM0_OpenLocalSocket") bind failed for local address UDP
  socket 67, port=520, errno=13
  kumslrtu.c,148,"KUMS_ListenRouterUpdates") ***** unable to open socket with
  router well-known port
  ```

The Universal Agent stops functioning if the system IP address changes while it is running

If a network connection failure occurs and the UA system is assigned a different IP address after the reconnection, UA will stop processing new input data because of socket bind failures. Recycle the Universal Agent so that it uses the new IP address.

'Unable to get attribute name for tablename/column' error occurs in the Tivoli Enterprise Monitoring Server log after creating a situation

After creating a situation for Universal Data Provider to fire event, the following error occurs in the Tivoli Enterprise Monitoring Server log file:

```
(4320916A.0049-F60:kfaottev.c,1572,"Translate_ResultBuffer")
Unable to get attribute name for tablename/column <UAG524400.UA4>. Ignored.
```

The Tivoli Enterprise Monitoring Server log messages are harmless for Universal Agent applications because of the time lag between the issuing of the messages and when the Universal Agent-uploaded attribute files are stored at the Tivoli Enterprise Monitoring Server. However, if these messages occur for other agent applications, they can indicate that the agent attribute files were not installed on the Tivoli Enterprise Monitoring Server.

SNMP data provider problems

This section describes symptoms and tips for diagnosing SNMP data provider problems.

SNMP-MANAGER Trap workspace is unavailable in many columns

Every Independent Software Vendor (ISV) product that emits a trap to the SNMP DP must have a Type 2 and Type 3 record with a unique enterprise OID defined in

Universal Agent `trapcnfg` file in Universal Agent `work` directory. When a trap is received, the SNMP data provider looks up the trap enterprise OID value, generic trap number, and specific trap number in the `trapcnfg`. The trap definition values received by the SNMP data provider must match the definitions in the `trapcnfg` file. If the SNMP data provider does not find a match for the values in the `trapcnfg`, it sets the status of the trap as "Unavailable" in the SNMP-MANAGER Trap table attributes. Although the traps are received, they display the "Unavailable" status in the SNMP-MANAGER Trap workspace.

The following example shows an intelliWatch trap definition:

```
intelliWatch-Monitor {1.3.6.1.4.1.1983.1.1}
    (Type 2)
criticalAlarm {1.3.6.1.4.1.1983.1.1} 6 1 A 1 0 "Status Events" (Type 3)
```

where:

1983 Specifies the Enterprise OID.

6 Specifies generic trap number.

1 Specifies the specific trap number.

Define the correct traps values in the `trapcnfg` file in the Universal Agent `work` directory.

The TRAP workspace does not display expected traps

For the SNMP to receive traps from SNMP agents, the trap destination list of the monitoring agent must include the host name or IP address of the host on which the Data Provider resides. Configuration of SNMP agents varies from monitoring agent to monitoring agent. Refer to your SNMP monitoring agent documentation.

If you are not receiving traps ensure that:

- SNMP is in the list of data providers being started
- The host of the SNMP Data Provider is configured to receive traps
- Agents are configured to send traps to the host of the SNMP data provider.
- That the trap listener started successfully by checking the UAGENT DPLOG workspace for the SNMP Data Provider
- KUMP_SNMP_MONITOR_TRAP is not set to N
- You add the trap description data to the file `trapcnfg` if a trap field shows UNAVAILABLE,

SNMP metafiles are imported but MIB data collection is not working

The MIB application workspaces are empty after initiating MIB data collection (**Take Action** > **Monitor Start**).

Table 42. MIB data collection is not working

Problem	Resolution
The community name was not specified correctly for the SNMP agent.	Use an MIB browser or freeware utility such as snmputil to retrieve MIB variables from this SNMP agent to determine the source of the problem.
The SNMP agent is not responding to any SNMP Get requests.	
The MIB OIDs on the SNMP agent host do not match the OIDs specified in the Universal Agent metafile.	

Table 42. MIB data collection is not working (continued)

Problem	Resolution
The agent does not respond to basic SNMP Get requests from Universal Agent.	All SNMP agents support the MIB2 OIDs such as SysName and SysLocation. Use the `rfc1213` metafile to establish a baseline of functionality. Use the Universal Agent RFC1213_mib-2.mdl to collect MIB-2 data from the agent to verify that the SNMP agent responds to basic SNMP Get requests from Universal Agent.

Universal Agent-emitted traps are not received by third-party SNMP Manager

The policies are configured to emit SNMP traps, but the traps do not display in the receiving system console. Use the following table to determine the source of this problem.

Table 43. Universal Agent-emitted traps are not received by third-party SNMP Manager

Symptom	Explanation

There are error messages in the Universal Agent RAS1 log in the kumaeagt.cpp module.	Error messages indicate why the policy is not being driven, for example:
	`kumaeagt.cpp,154,"kum_kumact_agent::TakeSample")`
	`Error: could not find terminator in`
	`<Local_Time.Day_Of_Week> = '02' AND Local_Time.Day_Of_Week <= '06' AND Local_Time.`
	`Time>= '053000' AND Local_Time.Hours <= '21' AND`
	`Queue_Statistics.Current_Depth >= 12800 \`
	`AND STRSCAN(QMQUEUES.QNAME, 'ACK') = 0;> tok1 @NULL tok2 @NULL tok3 @NULL attrValTemp <>`
	
	The kumaeagt.cpp module implements Universal Agent's Alert Emitter probe. Any error messages in this module might indicate that the policy request never got to the Universal Agent module that sends the traps.

There are no error messages in the Universal Agent RAS1 log but the traps are not received.	If the Universal Agent RAS1 log has no error messages, check whether there are error messages in the Tivoli Enterprise Monitoring Server log. If there are errors that report a duplicate CAT and ATR files, there might be a name conflict with other installed IBM Tivoli Monitoring emitters.
Search for errors showing policies ending with a "cmd failed" reason code.	In an MVS-based Tivoli Enterprise Portal Server, a "cmd failed" reason code indicates the `KUMATR` and `KUMCAT` files are missing from RKANDATV.
If the Universal Agent RAS1 log contains "SNMP trap emitted to destinations(s) ..." messages, but the traps do not display on the 3rd party SNMP Manager console.	A firewall might prevent communication between the system where Universal Agent is running and the system where the SNMP Manager product is running.
	Security rules might filter, block, or divert SNMP traps.
	Configuration steps might be required on the SNMP Manager product so that it can receive and display the Universal Agent traps.
	The SNMP Manager product might have a log file that indicates whether it receives or rejects the Universal Agent traps.
	If the host name of the Universal Agent SNMP Data Provider is added as a trap destination, the Universal Agent Emitter traps do not display in the SNMP-MANAGER Trap workspace.

The NETWORK workspace is empty

Ensure the following:

- The host where the SNMP Data Provider is running is TCP/IP configured.
- You can ping the default router/gateway from the host of the SNMP Data Provider.
- You have initiated network discovery using **Take Action > Manage Start**.

A MIB workspace is not showing expected data

For MIB workspaces to display data, you must initiate data collection using the **Monitor Start** option of the **Take Action** feature. If you are still not receiving data:

- Ensure that the correct metafile was loaded.
- Confirm that the correct target monitoring agent nodes were specified in the **Monitor Start** window, separated by commas.
- Confirm that the node and correct community name were entered in brackets. The following example displays correct formatting if the SNMP community name of the target is not the default (public) nor specified by KUMP_SNMP_NET_COMMUNITY, and there is no entry in the `KUMSCOMM` file:

  ```
  {athens IBM}
  ```

Take Action > Manage Start or Take Action > Manage Stop is not working

Ensure the following for the Manage Start and Manage Stop Take Action to work:

- The address is correct if you entered the network address manually (rather than selecting it in the NETSUMMARY workspace).
- The destination managed system you specified when distributing the action is *host name*:SNMP-MANAGER*NN*.

The SNMP Data Provider does not start with IBM Tivoli Universal Agent

Ensure you included SNMP as a value for environment variable KUMA_STARTUP_DP.

You do not see the TakeAction options

Seed the Tivoli Enterprise Monitoring Server with KUM.SQL and restart the Tivoli Enterprise Monitoring Server and Tivoli Enterprise Portal sessions.

A managed system for a MIB application does not come online as expected

Ensure that you imported the application metafile either through the console command IMPORT or updating your `KUMPCNFG` file. Check your DPLOG workspace in the application UAGENT for error messages regarding the importing of the metafile.

The NETSUMMARY workspace does not show expected data

Ensure that you can ping the default gateway or router from the host running the SNMP Data Provider.

A MIB workspace displays empty when you expect to see data

A MIB workspace displays empty if the community name used for the SNMP query was not the correct one for a particular SNMP monitoring agent.

To determine that a MIB workspace is empty as a result of an incorrect community name, monitor for the Authentication failure trap from the SNMP monitoring agent. Assuming the SNMP monitoring agent is configured to generate traps to the host running the SNMP DP, you can browse your SNMP-MANAGER TRAP workspace to look for Authentication failure traps (Generic trap number 4).

Chapter 14. Database troubleshooting

This chapter provides information you need to solve problems you might experience with the database. It covers data loss prevention information and descriptions of common problems and appropriate resolutions. It also addresses issues you might experience with the Tivoli data warehouse and Warehouse Proxy agent.

Data loss prevention

This section provides information about utilities you can use to back up and restore Tivoli Enterprise Portal Server databases.

Backing up the database for recovery purposes

You can use the following utilities to back up the database:

Table 44. Utilities for backing up the database

migrate-export.bat	The `migrate-export.bat` utility backs up the entire database by writing its contents as insert statements to a flat file called `saveexport.sql` located in *`install_dir`*`\cnps\sqllib`. It can also be used to move the contents of the database from one database instance to another. You might use this utility to move the contents of the database from one windows server to another.
migrate-import.bat	This utility is used to read the contents of the `saveexport .sql` file created in the migrate-export process and insert them back into the database. This utility can be used to recover the database. It reads the contents in the *`install_dir`*`\cnps\sqllib\saveexport.sql` and rebuilds the database tables and contents. You can also use the `migrate-import.bat` to move the contents of the database to another windows server running the database. 1. Run `migrate-export.bat`. 2. Copy the `saveexport.sql` file from the old Tivoli Enterprise Portal Server to the new Tivoli Enterprise Portal Server into the *`install_dir`*`\cnps\sqllib` directory. 3. Run `migrate-import.bat` to read and build the database tables and contents on the new system.

Restoring the original database contents

The migrate-clean.bat utility cleans the contents of the database. Use the `migrate-clean.bat` file with caution. You must backup the database before running the `migrate-clean.bat` file or you lose all customization of the database. When you restart the Tivoli Enterprise Monitoring Server, the database is restored to its original state after installation. This is a quick way to reset the database back to its original state. After running this bat file and restarting the Tivoli Enterprise Monitoring Server server, the original content provided by IBM Tivoli Monitoring is restored to the database.

If you modify your password or if it expires

The database requires the following user IDs:

db2admin
This ID is added when you install the database and is required by the product installer when you configure the Tivoli Enterprise Portal Server data source.

TEPS This ID is added during installation for creating the Tivoli Enterprise Portal Server data source.

If the Windows Local Security Settings are enabled for long or complex passwords, ensure your password meets those syntax requirements for these IDs. If your Windows environment requires you to change passwords regularly do the following to change the Tivoli Enterprise Portal Server database user account password.

Note: The following instructions do not apply in UNIX-based systems.

1. On the computer where the Tivoli Enterprise Portal Server is installed, be sure you are logged on to Windows with an ID having administrator authority.
2. From your Windows desktop, select **Start > Programs > Tivoli Monitoring Services > Manage Tivoli Enterprise Monitoring Services**.
3. Right-click the Tivoli Enterprise Portal Server and select **Advanced > Utilities > Build Tivoli Enterprise Portal Server Database** from the menu.
4. Click **DB2** to open the Tivoli Enterprise Portal Server Data Source Config Parameters window.
5. Enter the Admin Password.
6. Enter the new Database Password for the Tivoli Enterprise Portal Server Database user ID.

Receive First Steps error at the end of a DB2 installation

At the end of my DB2 install, I received an error that First Steps could not initialize because a supported browser was not present on my system. Here is the link to the full procedure on how to resolve this problem: http://publib.boulder.ibm.com/infocenter/db2luw/v9/topic/com.ibm.db2.udb.pd.doc/doc/c0025020.htm?resultof=%22%66%69%72%73%74%22%20%22%73%74%65%70%73%22%20%22%73%74%65%70%22%20%22%62%72%6f%77%73%65%72%22%20

Tivoli Enterprise Portal Server cannot connect to the database

If an error message displays indicating the connection failed for security reasons, the end user is logged in to the server with a userid with administrator authority, but is logged into the local domain instead of locally on the system. The user does not have authority to create a data source and register with windows, or the authority to create a windows user account. Continue installing the software, using the following steps to resolve the error:

1. When the install completes, log off the current Windows user session and log in with using the db2admin userid.
2. Run *install_dir*\installITM\DB2DataSource.exe from Windows Explorer or a command prompt. You can run this program again, even if one or more of the tasks completed the first time it ran.
3. Start the Tivoli Enterprise Monitoring Server after the software indicates the Tivoli Enterprise Portal Server configuration was successful.

If the Tivoli Enterprise Portal installation is complete but it does not start, the data source might not be defined. Go to the *install_dir*\cnps\kfwras1.log file. If error messages similar to the following are present in the log, the data source was not defined.

```
[IBM][ODBC Driver Manager]
Data source name not found and no default driver specified.
```

Use the follow steps verify whether or not the data source was created and resolve the problem:

1. Open the ODBC datasource window: **Start** > **Settings** > **Control Panel** > **Administrative tools** and double-click the **Data Sources** (ODBC) .
2. Verify that the Tivoli Enterprise Monitoring Server **IBM DB2 ODBC DRIVER** datasource is defined.
3. If the **IBM DB2 ODBC DRIVER** data source is not present, run the *install_dir*\installITM\DB2DataSource.exe file.
4. Read the error messages after running the program.
5. If the error is security related or mentions incorrect user IDs or passwords, log in to the windows server with the db2admin user account and run the db2datasource program.

If the password for db2admin changes, the logon information for the services must also change, otherwise the Tivoli Enterprise Portal Server database does not start because the DB2 processes cannot logon. Use the following steps to resolve this problem:

1. From a Windows desktop, select **Start** > **Control Panel** > **Administrative Tools** > **Services**
2. Scan the column on the right for the value .\db2admin
3. Do the following for each .\db2admin value:
   a. Open the **Properties** window.
   b. Select the **Log On** tab.
   c. Type the new password for the user.

For information on how to modify kernel parameters, see http://publib.boulder.ibm.com/infocenter/db2luw/v9/index.jsp?topic=/com.ibm.db2.udb.uprun.doc/doc/t0008238.htm

Oracle problem with JDBC drivers prior to 11.1.0.7

You receive an error like the following on the Summarization and Pruning java log when using Oracle:

```
== 509 t=work1 java.lang.ArrayIndexOutOfBoundsException
        at oracle.jdbc.driver.OraclePreparedStatement.setupBindBuffers
(OraclePreparedStatement.java:2673)
        at oracle.jdbc.driver.OraclePreparedStatement.executeBatch
(OraclePreparedStatement.java:10689)
        at com.tivoli.twh.ksy.agg.BatchManager.executeBatch(BatchManager.java:381)
        at com.tivoli.twh.ksy.agg.BatchManager.commit(BatchManager.java:488)
        at com.tivoli.twh.ksy.agg.BatchManager.checkCommit(BatchManager.java:575)
        at com.tivoli.twh.ksy.agg.RawTable.aggregateData(RawTable.java:2356)
        at com.tivoli.twh.ksy.agg.Originnode.aggregateDataForNode
(Originnode.java:180)
        at com.tivoli.twh.ksy.agg.RawTable.createAggregatesAndPrune
(RawTable.java:3286)
        at com.tivoli.twh.ksy.agg.Worker.run(Worker.java:98)
```

Use a smaller number of rows per database transaction.

Data did not migrate from the Microsoft SQL Server database to the DB2 Universal Database™

You can run the movefrom-m2i.bat located in the *install_dir*\cnps directory to recover the contents of the Universal Database. The movefrom-m2i.bat utility creates a flat file from the SQL server database contents and imports into the Universal Database. The movefrom-m2i.bat utility runs during the installation of the Tivoli Enterprise Portal when the option to migrate from Microsoft SQL Server to the Universal Database is selected but can also be used after installation or routine Tivoli Enterprise Portal usage. This migration utility can fail if the Tivoli Enterprise Portal userid and password do not have the correct authority to connect to the Tivoli Enterprise Monitoring Server Universal Database. The movefrom-m2i.bat requires that the Microsoft SQL server database is on the same Windows platform as the Tivoli Enterprise Monitoring Server and the new Universal Database installation. Use this utility only after migration problems and before customizing Tivoli Enterprise Monitoring Server. The `movefrom-m2i.bat` is only used to migrate the contents of Microsoft SQL Server to Universal Database.

Database contents are incorrect after installation

You can run the `movefrom-m2i.bat` located in the *install_dir*\cnps directory to recover the contents of the database. The movefrom-m2i.bat utility creates a flat file from the SQL server database contents and imports into the Universal Database. The movefrom-m2i.bat utility runs during the installation of the Tivoli Enterprise Portal when the option to migrate from Microsoft SQL Server to the Universal Database is selected but can also be used after installation or routine Tivoli Enterprise Portal usage. This migration utility can fail if the Tivoli Enterprise Portal userid and password do not have the correct authority to connect to the Tivoli Enterprise Monitoring Server Universal Database. The movefrom-m2i.bat requires that the Microsoft SQL server database is on the same Windows platform as the Tivoli Enterprise Monitoring Server server and the new Universal Database installation. Use this utility only after migration problems and before customizing Tivoli Enterprise Monitoring Server. The `movefrom-m2i.bat` is only used to migrate the contents of Microsoft SQL Server to Universal Database.

The error SQL0443N with 'SYSIBM:CLI:-805' occurs after upgrading to DB2 UDB Version 8.1 Fix Pack 10

An error occurs with the SQLTables if the database was created before applying IBM DB2 V8.1 Fix Pack 10 (also known as Version 8.2 Fix Pack 3), you encounter an SQL0443N error if you run a DB2 Call Level Interface (CLI) catalog function (such as SQLTables(), SQLColumns(), or SQLStatistics()). The following is an example of the error in a log:

```
(430F82BD.0000-3C4:khdxodbc.cpp,319,"initializeDatabase") Connection with
Datasource "ITM Warehouse" successful
(430F82BD.0001-3C4:khdxbase.cpp,250,"setError") Error 20/3/-443(FFFFFE45)/0
executing SQLTables
(430F82BD.0002-3C4:khdxbase.cpp,266,"setError") Error "[IBM][CLI Driver][DB2/NT]
SQL0443N Routine "SYSIBM.SQLTABLES" (specific name "TABLES") has returned an
error SQLSTATE with diagnostic text "SYSIBM:CLI:-805".  SQLSTATE=38553
+430F82BD.0002 "
```

Bind the `db2schema.bnd` file against each database to resolve this error. Run the following command from a DB2 command prompt:

1. db2 connect to *dbname* (Warehouse Database)

   where:

   dbname
   Specifies the name of a database to which you want to bind the utilities, or the Warehouse Database name.

2. DB2 bind *path_name*

   where:

   path_name
   Specifies the full path name of the directory where the bind files are located, usually sqllib/bnd.

The following examples shows the rebinding commands from the c:\SQLLIB\bnd>DB2 directory:

```
c:\SQLLIB\bnd>DB2 connect to dbname (Warehouse Database)
c:\SQLLIB\bnd>DB2 bind @db2ubind.lst blocking all grant public
c:\SQLLIB\bnd>DB2 bind @db2cli.lst blocking all grant public
c:\SQLLIB\bnd>DB2 bind db2schema.bnd blocking all grant public
```

Some rows do not display in an upgraded table

You might not see all rows after upgrading the Warehouse Proxy agent to IBM Tivoli Monitoring V6.1 because some tables might be corrupted. Do the following to find the errors that occurred during the upgrade:

1. Edit the KHDRAS1_Mig_Detail.log file.
2. Search for the word EXCEPTION.

The KHD_MAX_ROWS_SKIPPED_PER_TABLE environment variable in the KHDENV_MIG file allows you to skip bad data. Use KHD_MAX_ROWS_SKIPPED_PER_TABLE to specify the number of rows per table to skip to migrate if the data that needs to be inserted is incorrect. When this number is reached, migration of the table is aborted.

Using DB2 v8.1, Warehouse Proxy Agent crashes

DB2 8.1 FP16 or higher is required.

Using DB2 V9.1 for z/OS, Warehouse Proxy agent encounters a large number of disconnections

When using DB2 for z/OS 9.1 for the warehouse database, the Warehouse Proxy agent can encounter repeated disconnections from the database. The default idle thread timeout value (DSN6FAC IDTHTOIN in DSNZPxxx) is 120 seconds. The Warehouse Proxy agent uses a pool of database connections to process export requests from monitoring agents. The warehousing interval used by agents can be set to values ranging from 15 minutes up to 24 hours. The database connections are idle between export requests, and if the idle thread timeout value is less than the warehousing interval, the database connections may timeout. This results in numerous error messages written to the Warehouse Proxy agent log. The Warehouse Proxy agent "Statistics" workspace will also show a large number of Disconnections in the "Failure / Disconnections" view.

To avoid repeated disconnections, consider increasing the DB2 idle thread timeout value to a value higher than the warehousing interval. Specifying a value of 0

disables time-out processing. If time-out processing is disabled, idle server threads remain in the system and continue to hold their resources, if any.

For more information on the DB2 IDLE THREAD TIMEOUT field (IDTHTOIN subsystem parameter), refer to the DB2 Version 9.1 for z/OS Installation Guide.

Historical data is not warehoused

Check the following Warehouse Proxy agent logs for errors that indicate why historical data is not warehoused:

- Windows Event Log (all critical errors)
- WHProxy Agent RAS1 Log.
- Operations Log

The Warehouse Proxy agent contains an audit trail for each export written to the warehouse database. You can also check the database table called WAREHOUSELOG as it contains the same information as the logs.

Historical data for logs is incorrect

If there are duplicate or missing rows in a table, incorrect historical data is collected for logs, such as managed system or situation status. Correct the incorrect rows to ensure reliable logs.

Warehouse Proxy Agent or Summarization and Pruning Agent fails due to DB2 transaction log full

If the DB2 transaction log is not large enough and fills, operations performed by the Warehouse Proxy Agent or Summarization and Pruning Agent will fail. If this happens you will see a message like the following in the Warehouse Proxy Agent log file (*hostname*_hd_java_nnnnnnnnnn.log) or the Summarization and Pruning Agent log file (*hostname*_sy_java_nnnnnnnnnn.log):

```
com.ibm.db2.jcc.a.SqlException: DB2 SQL error: SQLCODE: -964, SQLSTATE: 57011,
SQLERRMC: null
```

Increase the DB2 transaction log size. See the DB2 manuals for altering the LOGFILSIZ, LOGPRIMARY, and LOGSECOND parameters within DB2.

Incorrect data is collected in the warehouse for filtering if using a wildcard

This behavior could be caused by either of these cases:

- There are multiple historical collections distributed to your agent for the tablespace attribute group. All of the collections will write to the same short term history files and to the same database tables.
- You already had data in the short term history file for the tablespace attribute group before you created and distributed the new historical collection that has the filter. The older data would have been exported to the warehouse proxy and shown up in the Tivoli Data Warehouse database.

Wild card matching is not supported. The only way to mimic that functionality would be to use the substring or scan for string functions instead of the default value and equals. The equals operator only works with full matches.

Too much historical data is collected

The Summarization and Pruning agent is responsible for generating and storing summarized data, and pruning the data based on information that is stored in the Tivoli data warehouse. The data in the Tivoli data warehouse is a historical record of activity and conditions in your enterprise. The size of summarization data that is collected depends on the following criteria:

- The number of agents collecting data
- The number of table collected per agent
- The size of the table (number and size of columns)
- The collection interval (for example 5, 10, 15 or minutes)

Pruning data is deleting old data automatically, rather than manually. To reduce the data that is collected, limit the size of your database tables by regularly pruning old data from the Tivoli data warehouse. If you installed the Summarization and Pruning agent, your configuration settings are set to default values. You can view the current values in the History Collection Configuration window. Refer to "Changing configuration settings using the History Collection Configuration window in the Tivoli Enterprise Portal" in the *IBM Tivoli Monitoring Administrator's Guide* for instructions.

If you need to install the Summarization and Pruning agent, see the *IBM Tivoli Monitoring Installation and Setup Guide*. There you can find information for environment-wide capacity planning. You can find agent-specific capacity planning information in the user guide for the specific monitoring agent.

Warehouse Proxy agent failed to export data

The ODBC connection enables the Warehouse Proxy agent to export data to the warehouse database. The WAREHOUSELOG table lets you know how many exports succeeded and how many failed because of an ODBC error or a TIMEOUT issue. See the *IBM Tivoli Monitoring Installation and Setup Guide* for more information about the WAREHOUSELOG table and configuring the Warehouse Proxy agent.

There are ORACLE or DB2 errors in the khdras1.log file

The following errors can occur in the `khdras1.log` if the globalization system environment variable is not set correctly:

ORACLE error: [Oracle][ODBC][Ora]ORA-01461: can bind a LONG value only for insert into a LONG column

1. Set the environment variable NLS_LANG=AMERICAN_AMERICA.AL32UTF8 as a system environment on the Windows computer on which the Warehouse Proxy is installed.
2. Restart the Windows computer so that the Warehouse Proxy windows service recognizes the change.

DB2 error: SQL0302N The value of a host variable in the EXECUTE or OPEN statement is too large for its corresponding use. SQLSTATE=22003 sqlstate = 22003

1. Set the environment variable DB2CODEPAGE=1208 as a system environment on the Windows computer where the Warehouse Proxy is installed.

2. Restart the Windows computer so that the Warehouse Proxy windows service recognizes the change.

SQL0552N "ITMUSER" does not have the privilege to perform operation "CREATE BUFFERPOOL" SQLSTATE=42502

If the Warehouse database user does not have the correct permission, the following error can occur:

```
(42ED71FA.0000-E4C:khdxbase.cpp,250,"setError")
Error 20/3/-552(FFFFFDD8)/0 executing SQLExecute
(42ED71FA.0001-E4C:khdxbase.cpp,266,"setError")
Error "[IBM][CLI Driver][DB2/NT] SQL0552N "ITMUSER" does not have
the privilege to perform operation "CREATE BUFFERPOOL" SQLSTATE=42502
```

When you configure a DB2 Warehouse Proxy connection from the Manage Tivoli Enterprise Monitoring Services utility using the **Configure DB2 Datasource for Warehouse** window, the user ID the Warehouse Proxy uses to connect to the warehouse database must have SYSADM permission. SYSADM permission is required to create an 8K Tablespace and Bufferpool.

Windows

If the database is on Windows, the user must be a member of the local Administrators group.

UNIX-based system

If the database is on Linux or UNIX user must belong to the SYSADM group.

1. Log in as the DB2 instance owner (usually "su - db2inst1"),
2. Run the following command to determine the group that the UNIX-based system user must belong.

   ```
   db2 get dbm cfg | grep SYSADM
   ```

Chapter 15. Event synchronization troubleshooting

This section provides descriptions of and resolutions for problems you might experience with event synchronization for Netcool/OMNIbus or Tivoli Enterprise Console, including the forwarding situations and the Tivoli Enterprise Console Rules Check Utility.

Event synchronization installation and configuration troubleshooting

This section contains general troubleshooting information that applies to event synchronization installation and configuration.

Errors occur during installation of IBM Tivoli Monitoring event synchronization

When installation of the IBM Tivoli Monitoring Event Synchronization component is complete, the results are written to the `itm_tec_event_sync_install.log` file located in the following directories:

- Windows:

  The `itm_tec_event_sync_install.log` file is created in the directory defined by the `%TEMP%` environment variable. To determine where this directory is defined for the current command line window, run the following command:

  ```
  echo %TEMP%
  ```

- UNIX-based systems:

  The `itm_tec_event_sync_install.log` file is always created in the `/tmp` directory.

The following error is harmless and there is currently no resolution:

```
One or more errors occured during the replacement of files (tecSyncAllFile1)
with files (tecSyncAllFile1).
Refer to install log for more details.
One or more errors occured during the replacement of files (tecSyncAllFile2)
with files (tecSyncAllFile)1.
Refer to install log for more details.
One or more errors occured during the replacement of files (tecSyncAllFile3)
with files (tecSyncAllFile1).
Refer to install log for more details.
.
.
.
```

If the installation fails without any error messages, check the `itm_tec_event_sync_install.log` file.

If you are installing event synchronization on Linux and see the message below in the log file, you must install the `libXp` shared library and then run the event synchronization installation program again:

```
java.lang.UnsatisfiedLinkError: /tmp/isjSlpnGj/jre/bin/libawt.so: libXp.so.6:
cannot open shared object file: No such file or directory
```

Netcool/OMNIbus Probe for Tivoli EIF does not start after configuring the probe to use monitoring rules

If the Netcool/OMNIbus Probe for Tivoli EIF does not start after you have configured the probe's `tivol_eif.rules` file to include `itm_event.rules`, check the

probe's log file for error messages. See “Log files for Netcool/OMNIbus Event Synchronization” for the location of the log file.

You must update the Netcool/OMNIbus ObjectServer database schema with the IBM Tivoli Monitoring automations before you update the probe's `tivoli_eif.rules` file to include the itm_event.rules file or the probe won't start. See the topic "Updating the OMNIbus database schema" in the *IBM Tivoli Monitoring Installation and Setup Guide* for details on this procedure.

If you have updated the OMNIbus database schema with the IBM Tivoli Monitoring automations but the probe will not start because the BSM_Identity attribute is not defined, check if the `itm_event.rules` file has been modified to include the `tbsm_eif_event.rules` file or if `tivoli_eif.rules` is including other rules files that set the BSM_Identity attribute. If you are not integrating IBM Tivoli Monitoring, Netcool/OMNIbus, and Tivoli Business Service Manager, comment out any rules files (like `tbsm_eif_event.rules`) that are intended for Tivoli Business Service Manager integration and are setting BSM_Identity. However, if you are using Tivoli Business Service Manager, ensure you have installed the OMNIbus automations provided with that product because those automations ensure that BSM_Identity is added to the ObjectServer database schema.

Netcool/OMNIbus integration troubleshooting

This section contains general troubleshooting information that applies to Netcool/OMNIbus integration.

Log files for Netcool/OMNIbus Event Synchronization

The following logs contain trace information associated with Netcool/OMNIbus event synchronization.

IBM Tivoli Monitoring Situation Update Forwarder log file
Default location: `/tmp/itmsynch/logs/sync_trace.log`

To enable more verbose tracing, edit the `$EVENT_SYNC_INSTALLDIR/etc/situpdate.conf` file where $EVENT_SYNC_INSTALLDIR is the directory where the IBM Tivoli Monitoring Event Synchronization component is installed. Set `logLevel=verbose` and save the file. Stop and restart the Situation Update Forwarder using the **stopSUF.sh/stopSUF.cmd** and **startSUF.sh/startSUF.cmd** commands. These commands are located in the `$EVENT_SYNC_INSTALLDIR/bin` directory.

Netcool/OMNIbus Probe for Tivoli EIF log file
Default location: `$OMNIHOME/log/tivoli_eif.log` where $OMNIHOME is the directory where Netcool/OMNIbus is installed.

To enable probe tracing, run the probe with the `messagelevel` configuration parameter (for example, `nco_p_tivoli_eif –messagelevel debug`). Alternatively, set `MessageLevel: 'debug'` in the probe's properties file (`$OMNIHOME/probes/$ARCH/tivoli_eif.props`) and restart the probe.

IBM Tivoli Monitoring Netcool/OMNIbus trigger log file
Default location: `$OMNIHOME/log/eventsync_debug.log1` where $OMNIHOME is the directory where Netcool/OMNIbus is installed.

Contains trace of IBM Tivoli Monitoring triggers and procedures. Tracing is enabled by editing the `get_debug_itmsync` procedure in the Netcool/OMNIbus ObjectServer and changing the `debug_itmsync` flag to 1. The procedure can be edited using Netcool/OMNIbus Administrator.

Netcool/OMNIbus ObjectServer log file

Default location: `$OMNIHOME/log/NCOMS.log` where $OMNIHOME is the directory where Netcool/OMNIbus is installed and *NCOMS* is the name of the ObjectServer.

To enable ObjectServer tracing, run the ObjectServer with the `messagelevel` configuration parameter (for example, `nco_objserv –messagelevel debug`). Alternatively, set `MessageLevel: 'debug'` in the ObjectServer properties file, which is `$OMNIHOME/etc/NCOMS.props` and restart the ObjectServer.

Netcool/OMNIbus Process Agent log file

Default location: `$OMNIHOME/log/NCO_PA.log` where $OMNIHOME is the directory where Netcool/OMNIbus is installed.

The Process Agent is used to run the IBM Tivoli Monitoring Situation Update Forwarder. To enable Process Agent tracing, run the Process Agent with the `debug` configuration parameter (for example, `nco_pad –debug 1`).

Unable to send situation events from the hub monitoring server to Netcool/OMNIbus

If situation events are not forwarded from the hub monitoring server to Netcool/OMNIbus, consider the following possible causes and resolutions.

Table 45. Resolving problems sending events to Netcool/OMNIbus

Cause	Resolution
IBM Tivoli Monitoring is not configured to send events to OMNIbus.	Configure the hub Tivoli Enterprise Management Server to forward events to the Netcool/OMNIbus Probe for Tivoli EIF. For instructions on how to configure the hub monitoring server, see the "Configuring your monitoring server to forward events" topic of the *IBM Tivoli Monitoring Installation and Setup Guide*.
The IBM Tivoli Monitoring situation is not configured to send events to an EIF destination.	Go to the Tivoli Enterprise Portal, open the Situation editor, select the EIF tab, and make sure it is configured to forward events to your EIF destination.

Table 45. Resolving problems sending events to Netcool/OMNIbus (continued)

Cause	Resolution

Configuration of the EIF destination is incorrect.	Review the configuration of the OMNIbus EIF destination on the IBM Tivoli Monitoring side. Verify that the server and port information are correct. You can use the IBM Tivoli Monitoring CLI command **listeventdest** to list all the event destinations and use IBM Tivoli Monitoring CLI command **vieweventdest** to see detail of the event destination. If you have defined more than one event destination, make sure you are looking at the correct one. For example:
	`tacmd listeventdest`
	`Server Id Server Name Server Type`
	`0 Default EIF Receiver TEC`
	`1 nswin01-OM Micromuse/Omnibus`
	
	`tacmd vieweventdest -i 0`
	`Server Id : 0`
	`Server Name: Default EIF Receiver`
	`Server Type: TEC`
	`Description: default EIF event listener`
	`Default : Y`
	`Host1 : nswin02:5527`
	
	`tacmd vieweventdest -i 1`
	
	`Server Id : 1`
	`Server Name: nswin01-OM`
	`Server Type: Micromuse/Omnibus`
	`Description: Windows OMNIbus Server`
	`Default : N`
	`Host1 : nswin01:9998`

Table 45. Resolving problems sending events to Netcool/OMNIbus (continued)

Cause	Resolution
Events are cached at the Tivoli Enterprise Monitoring Server.	The EIF cache file lists events. On Windows, you can find the EIF cache file in `%ITM_HOME%\CMS\TECLIB` directory of the hub monitoring server. On UNIX or Linux, you can find the EIF cache file in `$ITMHOME/tables/tems_name/TECLIB` directory of the hub monitoring server. • Check to see if the OMNIbus/Netcool Probe for Tivoli EIF is running. On Windows, if it is running as a service, determine whether the service is running. If it is not running as a service, look for the `nco_p_nonnative.exe` process. If the process is not running, start the process using **%OMNIHOME%\probes\win32\nco_p_tivoli_eif.bat** command. On UNIX or Linux, use **- grep** for the `nco_p_tivoli_eif` process. If the process is not running, start the process using **$OMNIHOME/probes/nco_p_tivoli_eif** command. • Check to see if the port number used to send events from the IBM Tivoli Monitoring side matches the port number used by the EIF Probe. To check the port number information on the IBM Tivoli Monitoring side, you can use the IBM Tivoli Monitoring CLI commands **listeventdest** and **vieweventdest** to find the server and port information. See the example above. On the OMNIbus side, you can look at the PortNumber property in the `$OMNIHOME/probes/$ARCH/tivoli_eif.props` file. If you are using Netcool/OMNIbus Probe for Tivoli EIF Version 8 or later, the default port number is 9998. If Tivoli Business Service Manager Version 4.2.1 was used to install the probe, the default probe port number is 5530.

Note: You can also check the Netcool/OMNIbus Probe for Tivoli EIF log file and the Netcool/OMNIbus ObjectServer log file to determine if those components are unable to process the events. See "Log files for Netcool/OMNIbus Event Synchronization" on page 236 to determine the location of the log files.

Event status updates in Netcool/OMNIbus are not forwarded to Tivoli Monitoring

If status updates for acknowledgements, deacknowledgements, and clearing of events are not forwarded from Netcool/OMNIbus to Tivoli Monitoring, consider the following possible causes and resolutions:

Table 46. Event status updates in Netcool/OMNIbus are not forwarded to Tivoli Monitoring

Possible cause	Resolution	Log files to check
Verify the bi-directional architecture is configured.	Verify that the `$EVENT_SYNC_INSTALLDIR/omnibus/itm_sync.sql` file was loaded into the Netcool/OMNIbus ObjectServer, where $EVENT_SYNC_INSTALLDIR is the directory where the ITM event synchronization component was installed. Use Netcool/OMNIbus Administrator to verify that triggers from this file are defined in the ObjectServer. For example, the itm_event_send and synchronizeitm triggers should exist. If the triggers from `itm_sync.sql` are not defined in the ObjectServer, see the topic "Updating the OMNIbus database schema" in the *IBM Tivoli Monitoring Installation and Setup Guide* for the procedure to follow to add the triggers to the Object Server.	Not applicable.
The IBM Tivoli Monitoring Situation Update Forwarder is not running on the computer system where Netcool/OMNIbus ObjectServer is installed.	Run **$EVENT_SYNC_INSTALLDIR/bin/query_state.sh** (UNIX) or **query_state.cmd**(Windows) to verify the Situation Update Forwarder is running. If it is not running, start it with **$EVENT_SYNC_INSTALLDIR/bin/startSUF.sh** (UNIX) or **startSUF.cmd** (Windows) $EVENT_SYNC_INSTALLDIR is the directory where the IBM Tivoli Monitoring event synchronization component was installed.	Look for Situation Update Forwarder startup errors in `/tmp/itmsynch/logs/synch_trace.log`.

Table 46. Event status updates in Netcool/OMNIbus are not forwarded to Tivoli Monitoring (continued)

Possible cause	Resolution	Log files to check
The IBM Tivoli Monitoring Situation Update Forwarder is not configured to send status updates to a hub monitoring server or the wrong information is configured for a monitoring server.	Review the monitoring servers that are configured in the Situation Update Forwarder `$EVENT_SYNC_INSTALLDIR/etc/situser.conf` file, where $EVENT_SYNC_INSTALLDIR is the directory where the Event Synchronization component is installed on the Netcool/OMNIbus ObjectServer system. Updates to the list of monitoring servers and their user name and password can be made using **$EVENT_SYNC_INSTALLDIR/bin/sitconfuser.sh** (UNIX) or **sitconfuser.cmd** (Windows). The Situation Update Forwarder must be restarted using **$EVENT_SYNC_INSTALLDIR/bin/stopSUF.sh** (UNIX) or **stopSUF.cmd** (Windows) and then **startSUF.sh** (UNIX) or **startSUF.cmd** (Windows) after any changes are made. If a monitoring server is not listed in the `situser.conf` file, use the **sitconfuser** command to add the monitoring server. If a monitoring server is listed in the `situser.conf` file, it may have the wrong form of the host name. If just the host name is listed (for example, `server1`), use the **sitconfuser** command to add the fully qualified host name (for example, `server1.ibm.com`) and vice versa. If the monitoring server user name or password have changed recently, use the **sitconfuser** command to update the monitoring server's information. See the *IBM Tivoli Monitoring Command Reference* for details on the syntax of the **sitconfuser** command.	Look for "Invalid Tivoli Enterprise Monitoring Server" lines in the Situation Update Forwarder log file.

Table 46. Event status updates in Netcool/OMNIbus are not forwarded to Tivoli Monitoring (continued)

Possible cause	Resolution	Log files to check

The Netcool/OMNIbus ObjectServer cannot connect to the Process Agent.	Ensure the PA.Username and PA.Password properties in the ObjectServer properties file (`$OMNIHOME/etc/NCOMS.props`) is set correctly and restart the ObjectServer if you change the property values. For more information on what user to specify, see the topic "Configuring the OMNIbus server for program execution from scripts" in the *IBM Tivoli Monitoring Installation and Setup Guide*.
	
	If the user specified by the PA.Username property is a member of a group that can connect to process control and the ObjectServer is installed on UNIX, verify that the group was specified when the process agent was started. By default, Netcool/OMNIbus creates the ncoadmin group for this purpose. This command example shows how to start the process agent and specify the ncoadmin group:
	`nco_pad –name $NCO_PA –admingroup ncoadmin`
	
	where $NCO_PA is the name of the process agent.
	
	Verify the user configured for the PA.Username property can connect to the process agent by using the **$OMNIHOME/bin/nco_pa_status** command. For example:
	`nco_pa_status -server $NCO_PA -name nco -password nco_password`
	
	where $NCO_PA is the name of the process agent.
		1. Check the ObjectServer log file for error messages
		2. Check the Process Agent log file for error messages.
		
		See "Log files for Netcool/OMNIbus Event Synchronization" on page 236 to determine the names and locations of the log files and how to enable additional debugging.

Table 46. Event status updates in Netcool/OMNIbus are not forwarded to Tivoli Monitoring (continued)

Possible cause	Resolution	Log files to check
The Netcool/OMNIbus Process Agent fails to execute the Situation Update Forwarder command (**eventcmd**)	This error can occur if the Situation Update Forwarder command (**eventcmd**) cannot be found. The `eventcmd.sh` (UNIX) or `eventcmd.bat` script is located in the `$EVENT_SYNC_INSTALLDIR/omnibus` directory, where $EVENT_SYNC_INSTALLDIR is the directory where the IBM Tivoli Monitoring event synchronization component was installed on the Netcool/OMNIbus ObjectServer system. Use Netcool/OMNIbus Administrator to view and edit the **eventcmd** procedure and: 1. Verify the executable path is correct. The executable path should not have any spaces. If the Situation Update Forwarder was installed in a directory with spaces, change the executable path to a path without space, for example, on Windows: `C:\Progra~1\IBM\SitForwarder\omnibus\eventcmd.bat`. 2. Verify that the host parameter specifies the hostname of the Netcool/OMNIbus ObjectServer and the user ID and group ID values are correct especially if the `eventcmd` script will not be run as root by the Netcool/OMNIbus Process Agent.	Look for errors related to failing to execute 'eventcmd' in the Process Agent log file

Monitoring events in Netcool/OMNIbus do not have expected values for the Summary attribute or other attributes set by the IBM Tivoli Monitoring probe rules

"*Default mapping of situation events to OMNIbus events*" in the *IBM Tivoli Monitoring Installation and Setup Guide* describes how OMNIbus attributes should be set for monitoring events. If your events do not have the expected values described in that topic, consider the following possible causes and resolutions.

Table 47. Monitoring events in Netcool/OMNIbus do not have expected values

Cause	Resolution
The Netcool/OMNIbus Probe for Tivoli EIF has not been configured to use the IBM Tivoli Monitoring probe rules file (`itm_event.rules`)	1. Verify that the `itm_event.rules` file has been copied to the `$OMNIHOME/probes/arch` directory of the EIF probe, where `$OMNIHOME` is the directory where Netcool/OMNIbus is installed and `arch` represents the operating system directory on which the probe is installed; for example, solaris2 when running on a Solaris system, and win32 for a Windows system.. 2. Verify that the include statement for `itm_event.rules` has been uncommented in the probe's master rules file (`tivoli_eif.rules`). **Note:** If you make any changes to the probe rules files, you must restart the EIF probe.

Table 47. Monitoring events in Netcool/OMNIbus do not have expected values (continued)

Cause	Resolution
Other EIF probe rules files are modifying OMNIbus attributes for monitoring events	1. Check if the `itm_event.rules` file is including the `itm_custom_override.rules` file and if the customizations in that file are causing OMNIbus attributes to be set inappropriately. 2. Check the other rules files included by the EIF probe's master rules file (`tivoli_eif.rules`). If the `tivoli_eif_virtualization_pt2.rules` or `predictive_event.rules` files are uncommented in `tivoli_eif.rules`: • verify that you are using a version of `tivoli_eif.rules` that includes these two files after the `itm_event.rules` file • verify that you are using the versions of `tivoli_eif_virtualization_pt2.rules` or `predictive_event.rules` from Netcool/OMNIbus 7.3.1 Fixpack 2 or later fixpack or Netcool/OMNIbus 7.3.0 Fixpack 6 or later fixpack. **Note:** If you change the probe rules files, you must restart the EIF probe.
EIF slot customizations are changing the values of EIF slots that are mapped to OMNIbus attributes	Use the Tivoli Enterprise Portal Situation Editor to check if EIF slot customization has been configured for a situation and is setting slots to invalid values. For information on which EIF slots should not be customized, see the topic "Default mapping of situation events to OMNIbus events" in the *IBM Tivoli Monitoring Installation and Setup Guide*.
The Netcool/OMNIbus ObjectServer default duplication trigger is processing monitoring events and setting the Summary attribute to the situation name when events are acknowledged or deacknowledged.	Verify that the default duplication trigger has been configured to ignore events from IBM Tivoli Monitoring. See the topic "Changing the default deduplication trigger" in the *IBM Tivoli Monitoring Installation and Setup Guide* for more details.

Table 47. Monitoring events in Netcool/OMNIbus do not have expected values (continued)

Cause	Resolution
An acknowledgement expiration status update event from the hub monitoring server has re-opened a sampled event in the Netcool/OMNIbus ObjectServer after the operator cleared or deleted the event in Netcool/OMNIbus and has set the Summary attribute to the situation name. (Other OMNIbus attributes may not be set as expected too.)	If a sampled event is cleared or deleted in Netcool/OMNIbus, the behavior of the bidirectional event synchronization architecture is to send a request to the hub Tivoli Enterprise Monitoring Server to acknowledge the situation with a specified timeout. The reason for this behavior is that you cannot close sampled situation events unless the monitoring agent determines the situation condition is no longer true. If the acknowledgment timeout of the situation expires and the situation is still true, then a new situation event is opened in the Netcool/OMNIbus ObjectServer so that the Netcool/OMNIbus operator is notified that the event condition has not been resolved. By default, Netcool/OMNIbus removes cleared events from the alerts.status table after 2 minutes. If the event has already been removed from the alerts.status table when the acknowledgment expiration times out, a new event is opened in the ObjectServer. However, the event data is not fully populated, because the acknowledgment expiration status update event contains a subset of the base IBM Tivoli Monitoring EIF slots and not any of the agent-specific data. In addition, the OMNIbus Summary attribute is set to the situation name and not the descriptive text that is used when the IBM Tivoli Monitoring sends an open event to Netcool/OMNIbus. To ensure that the event data is fully populated when the acknowledgement expires, set the default acknowledgment expire time to be less than the time cleared events remain in the alerts.status table. If the event is still in the alerts.status table when the acknowledgment expiration status update event is received, the event will be deduplicated by the IBM Tivoli Monitoring triggers and the event attribute settings from the original event will be maintained. To increase the time that cleared events remain in the alerts.status table, edit the Netcool/OMNIbus delete_clears automation trigger. Then set the acknowledgement expire time to be less than time used by the delete_clears trigger logic. See the topic "Changing the default acknowledgment timeout used when sampled events are deleted or cleared in Netcool/OMNIbus" in the *IBM Tivoli Monitoring Installation and Setup Guide* for more information.

After an event is cleared in Netcool/OMNIbus, the event's severity is changed back to its original severity

If you clear a monitoring event in Netcool/OMNIbus and you are using the bi-directional architecture, the hub monitoring server sends a loopback event to OMNIbus after it processes the event status change from OMNIbus. If the default deduplication trigger is processing monitoring events and the event had been cleared, the deduplication trigger changes the event's severity to the original severity value that is included in the loopback event.

Verify that the default deduplication trigger has been configured to ignore events from IBM Tivoli Monitoring. See the topic "Changing the default deduplication trigger" in the *IBM Tivoli Monitoring Installation and Setup Guide* for more details.

Tivoli Enterprise Console Integration troubleshooting

This section contains general troubleshooting information that applies to Tivoli Enterprise Console integration.

Preliminary IBM Tivoli Enterprise Console event synchronization troubleshooting

Review the following list of fundamental IBM Tivoli Enterprise Console event synchronization troubleshooting tasks:

- Before you install the IBM Tivoli Enterprise Console event synchronization on Windows and import event forwarding functionality into an existing rule base with an absolute path, you must copy `setupwin32.exe` to the local drive on which the rule base resides to import the IBM Tivoli Enterprise Console event synchronization functionality into that rule base. Launch the copied `setupwin32.exe` to start IBM Tivoli Enterprise Console event synchronization installation.
- Use the IBM Tivoli Enterprise Console Java Console to make any configuration changes to consoles and associated operator and event groups.
- Connect to a different IBM Tivoli Enterprise Console server using the embedded viewer:
  - From the desktop client:
    1. Log off the Tivoli Enterprise Portal.
    2. Log on the Tivoli Enterprise Portal.
    3. Log into a different IBM Tivoli Enterprise Console server.
  - From the browser client:

    Recycle the browser.
- For a listing of product messages, refer to the document *IBM Tivoli Monitoring Messages*.

Situation events are not forwarded from Tivoli Enterprise Monitoring Server to the Tivoli Enterprise Console server

Table 48 on page 246 provides troubleshooting information for when Tivoli Enterprise Monitoring Server does not forward situations to the Tivoli Enterprise Console server:

Table 48. Troubleshooting when situations are not forwarded

Problem	Resolution
The IBM Tivoli Enterprise Console Event Integration Facility is not enabled or configured correctly.	See "Configuring IBM Tivoli Enterprise Console integration" in the *IBM Tivoli Monitoring Administrator's Guide*

Table 48. Troubleshooting when situations are not forwarded (continued)

Problem	Resolution
The correct values are not specified for connection to the Tivoli Enterprise Console server in the `om_tec.config` file.	Edit the following parameters in the `om_tec.config` to specify the correct information for connection to the Tivoli Enterprise Console server: **ServerLocation** Specifies the host name or IP address of IBM Tivoli Enterprise Console server. **ServerPort** Specifies the IBM Tivoli Enterprise Console server listening port. Specify 0 if the IBM Tivoli Enterprise Console server uses port mapper. • On a Windows system: 1. Click **Start** > **Programs** > **IBM Tivoli Monitoring** > **Manage Tivoli Enterprise Monitoring Services**. 2. Right-click Tivoli Enterprise Monitoring Server and select **Advanced** from the popup menu. 3. Select **Edit EIF configuration** to open the `om_tec.config` file in Notepad. 4. Specify the correct parameters and save the file. • On a UNIX-based systems system: 1. `cd /opt/IBM/ITM/tables/`*hubname*`/TECLIB`, where *hubname* specifies the name of the hub monitoring server. 2. Open the `om_tec.config` file in a text editor. 3. Specify the correct parameters and save the file.

Table 48. Troubleshooting when situations are not forwarded (continued)

Problem	Resolution
Events are filtered out based on the parameter values in the `om_tec.config` file.	Edit the `om_tec.config` file in the following locations: • On a windows system: `c:\ibm\itm\cms\TECLIB`. • On UNIX-based systems: `/opt/IBM/ITM/tableshostname/TECLIB`. where: `/opt/IBM/ITM` is the default location where the Tivoli Enterprise Monitoring Server is installed and the host name is the value supplied during the Tivoli Enterprise Monitoring Server configuration. • On a Windows system: 1. Click **Start** > **Programs** > **IBM Tivoli Monitoring** > **Manage Tivoli Enterprise Monitoring Services**. 2. Right-click Tivoli Enterprise Monitoring Server and select **Advanced** from the popup menu. 3. Select **Edit EIF configuration** to open the `om_tec.config` file in Notepad. 4. Examine the `FilterMode:` and `Filter:` statements. 5. Specify the appropriate filter statements. – See the *IBM Tivoli Monitoring Administrator's Guide* for the supported EIF configuration parameters – Also see the *Tivoli Event Integration Facility, Version 3.9* reference manual SC32-1241 for more details. • On a UNIX-based systems system: 1. `cd /opt/IBM/ITM/tables/`*`hubname`*`/TECLIB` where: *hubname* Specifies the name of the hub monitoring server. 2. Open the `om_tec.config` file in a text editor. 3. Examine the `FilterMode:` and `Filter:` statements. 4. Specify the appropriate filter statements. – See the *IBM Tivoli Monitoring Administrator's Guide* for the supported EIF configuration parameters – Also see the *Tivoli Event Integration Facility, Version 3.9* reference manual SC32-1241 for more details. **Note:** On z/OS and 64-bit native platforms a physical event cache is not available from the TECLIB directory. The event cache is in a memory cache.

Table 48. Troubleshooting when situations are not forwarded (continued)

Problem	Resolution
Events are cached because the target IBM Tivoli Enterprise Console server is not currently running.	1. Check the cache files to determine if events are cached on the Tivoli Enterprise Monitoring Server. The cache files are located in the `TECLIB` directory on Tivoli Enterprise Monitoring Server: • Windows: `/IBM/ITM/cms/TECLIB` • UNIX-based systems: `/opt/IBM/ITM/tables/`*hubname*`/TECLIB`, where *hubname* specifies the name of the hub monitoring server. 2. Run the **wstartesvr** command to restart the IBM Tivoli Enterprise Console server from a Tivoli sourced environment. 3. Run the **wstatesvr [-S** *server***]** command on the IBM Tivoli Enterprise Console server to check the status of an event server. where: **-S** *server* Specifies the name of an event server in name registry format. The default server is the local event server. To indicate a remote server, specify `@EventServer#`*tmr*, where *tmr* is the name of a Tivoli region. Refer to the IBM Tivoli Enterprise Console documentation for more information about checking the status of the IBM Tivoli Enterprise Console server. **Note:** On z/OS and 64-bit native platforms a physical event cache is not available from the `TECLIB` directory. The event cache is in a memory cache.

See "Trace logging" on page 35 for more information about tracing for IBM Tivoli Enterprise Console forwarding.

Verifying that events are being received by Tivoli Enterprise Console

On the Tivoli Enterprise Monitoring Server, set this UNIT trace level:

```
ERROR (UNIT:kfaot ALL)
```

This setting will trace the communication between the Tivoli Enterprise Monitoring Server and Tivoli Enterprise Console. The `*_ms_*` logs from the Tivoli Enterprise Monitoring Server show this traffic. You can then verify that events are being received by Tivoli Enterprise Console by looking at the wtdumprl output. If there are no "PARSING_FAILED" messages and the Tivoli Enterprise Console is working correctly, the events should be processed and show in the Tivoli Enterprise Console.

Forwarded IBM Tivoli Enterprise Console events display with the PARSING_FAILED status in the IBM Tivoli Enterprise Console reception log

The following table lists possible causes and resolutions for the PARSING_FAILED status:

Table 49. Forwarded events display with the PARSING_FAILED status

Problem	Resolution
The IBM ITM event synchronization was not installed or was not installed correctly.	Reinstall the IBM ITM event synchronization functionality. See the *IBM Tivoli Monitoring Installation and Setup Guide* for instructions.
The expected rule base was not loaded.	Actively load the expected rule base. You can run the following command from the IBM Tivoli Enterprise Console event server to load a rule base: `wrb -loadrb rule_base` where: *rule_base* The name of the rule base to load. This makes *rule_base* the currently active rule base on the event server. The rule base must already be defined at the server, and any event class specification files and rule files in the directory must be valid. The loaded rule base replaces all event class specifications and rules currently defined at the server. Only one rule base can be active at a time. Loading another rule base overwrites the currently active rule base. **Notes:** 1. If you do not compile the rule base before attempting to load it, you get an error message. 2. You must stop and restart the Tivoli Enterprise Console server for changes to the rule base to be active. Use the following commands: • **wstopesvr [-S** *server***]** • **wstartesvr [-S** *server***]** See the IBM Tivoli Enterprise Console documentation for more information about loading rule bases, including the *IBM Tivoli Enterprise Console Command and Task Reference*.

Table 49. Forwarded events display with the PARSING_FAILED status (continued)

Problem	Resolution

There are missing BAROC files that must be imported to support the IBM Tivoli Monitoring V6.1 events.	The BAROC files are located in the `TECLIB` directories on Tivoli Enterprise Monitoring Server:
	• Windows:
	`/IBM/ITM/cms/TECLIB`
	• UNIX-based systems:
	`/opt/IBM/ITM/tables/`*`hubname`*`/TECLIB`
	where
	hubname
	Specifies the name of the hub server.
	
	You can run the following command from the IBM Tivoli Enterprise Console event server to import a BAROC file (a file of event class specifications into a rule base), appending it to the end of the class specifications unless otherwise specified with arguments:
	`wrb -imprbclass` *`class_file`* `[-encoding encoding ]`
	`[-before` *`class_file`* `| -after` *`class_file`*`]`
	`[-force]` *`rule_base`*
	
	where:
	class_file
	Specifies the name of the class file to import. This must be a path to the BAROC file.
	rule_base
	The name of the rule base to receive the imported class set.
	-after *class_file*
	Specifies the name of the class file after which the imported class file is to be placed.
	-before *class_file*
	Specifies the name of the class file before which the imported class file is to be placed.
	-encoding encoding
	Specifies the character encoding of the class file. If this option is not specified, a class file being imported into a rule base is opened in UTF-8 character encoding.
	-force Imports the class file even if it can cause rule base inconsistency.
	An error message is displayed if the class set file contains syntax errors, references to nonexistent event classes or enumerations, or if duplicate event classes or enumeration are defined. If the classes in a class file are derived from classes in another file, import the class files into the rule base in an order that preserves the inheritance structure. For example, if class file `B.baroc` contains classes that are derived from class file `A.baroc`, you must import class file `A.baroc` first.
	
	For any changes you make to the rule base to take affect you must complete the following steps:
	• Recompile the rule base
	• Load the rule base
	• Stop the Tivoli Enterprise Console server
	• Restart the Tivoli Enterprise Console server

Table 49. Forwarded events display with the PARSING_FAILED status (continued)

Problem	Resolution
There are missing BAROC files that must be imported to support the IBM Tivoli Monitoring V6.1 events. (Continued)	Refer to the *IBM Tivoli Monitoring Administrator's Guide* for information about changing the `omegamon.rls` file. See the *IBM Tivoli Enterprise Console Command and Task Reference, V3.9.0* for more information about importing class files into rule bases.
Parsing errors reported in Tivoli Enterprise Console server for ITM_ManagedSystem events.	The ITM_ManagedSystem event class is defined in the `kib.baroc` file. The `kib.baroc` file is not included in the active rule base. Copy the `kib.baroc` file from the Tivoli Enterprise Monitoring Server from `&ITMHOME/cms/TECLIB` and compile it into the current rule base.

Incomplete event data from a situation is forwarded to IBM Tivoli Enterprise Console

The typical situation for monitoring agents in IBM Tivoli Monitoring targets a specific resource and generates a limited amount of monitoring data. In some cases, a Tivoli OMEGAMON XE for Storage on z/OS situation can monitor multiple sub-objects on a managed system. For example, one situation might monitor multiple channels. As a result, relatively large amounts of monitoring data might be generated every time that the thresholds of the situation are triggered.

WhenIBM Tivoli Enterprise Console integration is enabled, the Tivoli Enterprise Console receives a buffer of monitoring data that cannot exceed 4K bytes in size. In most cases, this buffer size is sufficient. However, some situations that monitor multiple sub-objects in Tivoli OMEGAMON XE for Storage on z/OS can generate more than 4K bytes of data. When the data generated for the situation exceeds this limit, the excess data is truncated and is not presented at the Tivoli Enterprise Console.

For situations that monitor multiple sub-objects, be aware that Tivoli Enterprise Console is retrieving only the first 4K bytes of data.

TEC_ITM_OM_Situation_Sync_Error events occur

TEC_ITM_OM_Situation_Sync_Error events occur if there is a Tivoli Enterprise Console server communication problem or if you need to increase the rules cache.

Table 50. Reasons for the TEC_ITM_OM_Situation_Sync_Error event

Problem	Resolution
IOException is generated. There is no connectivity with SOAP. Logon Validation Failure is returned by the SOAP server. Fatal Error is returned by the SOAP server. The connection to the SOAP server repeatedly times out because of broken communication, network outage or the SOAP server is down.	Verify that the network connections are up and running, the SOAP server is running and receiving requests, and the ports 3661 and 1920 on the Tivoli Enterprise Monitoring Server system are open. Use the following steps to determine why the error occurred: 1. Ensure that the user ID and password configured for the Tivoli Enterprise Monitoring Server Server ID on the event server during installation is correct. Run the **sitconfsvruser.sh** script to update the configuration for the Tivoli Enterprise Monitoring Server. Refer to the *IBM Tivoli Monitoring Administrator's Guide* for more information. 2. Run the **test.sh** command on UNIX based systems or the **test.cmd** on Windows to determine if there is a communication problem between IBM Tivoli Enterprise Console server and Tivoli Enterprise Monitoring Server. 3. If the SOAP Server is running and receiving requests, initiate a CT_GET request for the SOAP server from the Web client. See the "Tivoli Enterprise Monitoring Web services" section in the *IBM Tivoli Monitoring Administrator's Guide* for more information.
The event message indicates reset, resurface, or acknowledge action failed. The original event was not in the Tivoli Enterprise Console rules cache.	Increase the size of the rules cache using the Tivoli desktop or the **wsetesvrcfg** command. Refer to the *IBM Tivoli Enterprise Console Command and Task Reference* for more information and the "Configuring Tivoli Enterprise Console integration" section in the *IBM Tivoli Monitoring Administrator's Guide* for more information.

Enabling tracing of events from the Tivoli Enterprise Console to the Tivoli Enterprise Monitoring Server

Complete the following steps to enable tracing of events:

1. Rule tracing can be set up for the `omegamon.rls`. In the OMEGAMON rule trace file, verify that the exec_program predicate is called in the rules trace to indicate that the rule set invoked `situpdate.sh`. A line like this will be seen in the log:

```
[357]                          call    exec_program(0x209372e8,
'OM_TEC/bin/situpdate.sh','-size %s
-num %s -path %s %s',['50000','10','"/space/Tivoli_
4141/var/TME/TEC/OM_TEC/persistence"',
       '/tmp/SUF0.tmp'],NO)
```

2. Tracing can be set up within the `situpdate.sh` running by editing the script (the `situpdate.sh` script is located at `$BINDIR/TME/TEC/OM_TEC/bin`). Change the `debugVerbose=`expr 0`` to `debugVerbose=`expr 1`` .

   The files are then `/tmp/situpdate.log` and `/tmp/situpdate.trace`.

3. The tracing can be increased on the Situation Update Forwarder, by editing the `sitconfig.sh script` to change the `logLevel` in the configuration file to `low`, `med`, or `verbose`. The log files will be `/tmp/itmsynch/logs/synch_trace.log` and `synch_msg.log`.

4. Verify that the `situpdate.log` log file for the short-running script indicates events are being written to the cache file, such as:

```
Sat Sep  2 15:36:03 GMT 2006 : 51600 : 1 events from /tmp/SUF1.tmp written
to cache file /space/Tivoli_4141/var/TME/TEC/OM_TEC/persistence
/situpdate_1157135641
```

5. Verify that the Situation Update Forwarder is running.

6. Verify from the Situation Update Forwarder log file synch_trace.log that it is reading from the cache files, such as:

   ```
   2006.09.02 17:36:05.876+02:00 com.tivoli.candlenet.SituationUpdateForwarder
   readCacheLine IBM Tivoli Monitoring  TEC Synchronization
   ```

7. Verify that the Situation Update Forwarder log file synch_trace.log contains successful send event messages:

   ```
   2006.09.02 17:36:06.311+02:00 com.tivoli.candlenet.SituationUpdateForwarder
    pollCacheFile IBM Tivoli Monitoring  TEC Synchronization
   Machine_Name IP Successfully sent event:
   ```

8. If there are no successful event sent messages, check the synch_trace.log for exceptions.
9. If there is no indication that the Situation Update Forwarder attempted to send the event, ensure the Situation Update Forwarder is running and verify that the Tivoli Enterprise Monitoring Server of the event (indicated by sv=*TEMS_server*:*port* in the cache file or the cms_hostname attribute of the Tivoli Enterprise Console event) matches any of the Tivoli Enterprise Monitoring Servers defined in the situser.conf configuration file.

The IBM Tivoli Enterprise Console does not indicate that a situation event was acknowledged or closed

Table 51. Situation event was not acknowledged or closed

Problem	Resolution
The `omegamon.rls` rule set was not imported in the currently loaded rule base.	Run the following commands from the IBM Tivoli Enterprise Console event server to import a rule set into a rule base: 1. `wrb -imprbrule` *`rule_file`* `[-encoding encoding ] [-force]` *`rule_base`* where: *rule_base* The name of the rule base in which the rule pack lives. *rule_file* The file name of the rule set to import to the rule base. This must be a path to a rule set file (with a file extension of .rls). **-encoding encoding** Specifies the character encoding of the class file. If this option is not specified, a class file being imported into a rule base is opened in UTF-8 character encoding. **-force** Adds the rule set to the rule base even if a rule references a nonexistent event class 2. `wrb -imptgtrule {`*`rule_set`* `|` *`rule_pack`*`} [{-before	-after} {`*`rule_set`* `|` *`rule_pack`*`}] target` *`rule_base`* where: *rule_base* The name of the rule base that contains the rule base target. *rule_pack* The name of the rule pack to import. The rule pack must have been imported into the rule base first. *rule_set* The name of the rule set to import. The rule set must have been imported into the rule base first. *target* The name of the rule base target to receive the imported rule set or rule pack. You must have first created the target with the -crttarget command option. **-after** *rule_set* `|` *rule_pack* Specifies the name of the rule set or rule pack after which the imported rule set or rule pack should be located. **-before** *rule_set* `|` *rule_pack* Specifies the name of the rule set or rule pack before which the imported rule set or rule pack should be located. For any changes you make to the rule base to take affect you must complete the following steps: • Recompile the rule base • Load the rule base • Stop the Tivoli Enterprise Console server • Restart the Tivoli Enterprise Console server Refer to the *IBM Tivoli Monitoring Administrator's Guide* for information about changing the `omegamon.rls` file.

Table 51. Situation event was not acknowledged or closed (continued)

Problem	Resolution
The events are not cached in the expected location.	The location of the cache file is specified during installation. The default locations are as follows: • On Windows: `C:\tmp\TME\TEC\OM_TEC\persistence` • On UNIX-based systems: `/var/TME/TEC/OM_TEC/persistence` The value of *fileLocation* is defined in the active configuration file as indicated by the `situpdate.properties` file in the following locations: • On Windows: `C:\Program Files\TME\TEC\OM_TEC\etc` • On UNIX-based systems: `/etc/TME/TEC/OM_TEC` You can edit the location of the cache file by running the `sitconfig.sh` script. Refer to the *IBM Tivoli Monitoring Administrator's Guide* for `sitconfig.sh` script usage.

The IBM ITM Situation Update Forwarder is not currently running.	To use event forwarding, you must start the Situation Update Forwarder. This process is started automatically when the event server starts. To start the process manually, change to the `$BINDIR/TME/TEC/OM_TEC/bin directory` and run the following command:
	On Windows:
	`startSUF.cmd`
	On UNIX-based systems:
	`startSUF.sh`
	To stop the process, run the **stopSUF.sh** command (**stopSUF.cmd** on Windows) in the same directory.
	Note: If the Situation Update Forwarder process stops abnormally, run the **stopSUF.sh** (**stopSUF.cmd** on Windows) command before restarting the process.

The IBM Tivoli Monitoring Situation Update Forwarder is not configured to send status updates to a hub monitoring server or the wrong information is configured for a monitoring server.	Review the monitoring servers that are configured in the Situation Update Forwarder `$EVENT_SYNC_INSTALLDIR/etc/situser.conf` file where $EVENT_SYNC_INSTALLDIR is the directory where the event synchronization component is installed on the Tivoli Enterprise Console system. Updates to the list of monitoring servers and their username and password can be made using **$EVENT_SYNC_INSTALLDIR/bin/sitconfuser.sh** (UNIX) or **sitconfuser.cmd** (Windows). The Situation Update Forwarder must be restarted using **$EVENT_SYNC_INSTALLDIR/bin/stopSUF.sh** (UNIX) or **stopSUF.cmd** (Windows) and then **startSUF.sh** (UNIX) or **startSUF.cmd** (Windows) after any changes are made. If a monitoring server is not listed in the `situser.conf` file, use the **sitconfuser** command to add the monitoring server. If a monitoring server is listed in the `situser.conf` file, it may have the wrong form of the host name. If just the host name is listed (for example, `server1`), use the **sitconfuser** command to add the fully qualified host name (for example, `server1.ibm.com`) and vice versa. If the monitoring server user name or password have changed recently, use the **sitconfuser** command to update the monitoring server's information. See the *IBM Tivoli Monitoring Command Reference* for details on the syntax of the **sitconfuser** command.

Table 51. Situation event was not acknowledged or closed (continued)

Problem	Resolution
There is a communication problem between IBM Tivoli Enterprise Console server and Tivoli Enterprise Monitoring Server.	Run the **test.sh** command on UNIX based systems or the **test.cmd** on Windows to determine if there is a communication problem between IBM Tivoli Enterprise Console server and Tivoli Enterprise Monitoring Server. Refer to Chapter 6, "Connectivity troubleshooting," on page 115 for additional information about solving connectivity problems.
The expected server ports 3661 and 1920 are not currently open on the Tivoli Enterprise Monitoring Server.	Ports 3661 and 1920 must be available. Run the **test.sh** command on UNIX based systems or the **test.cmd** on Windows to determine if there is a communication problem between IBM Tivoli Enterprise Console server and Tivoli Enterprise Monitoring Server. Refer to Chapter 6, "Connectivity troubleshooting," on page 115 for additional information about solving connectivity problems.
There a firewall between Tivoli Enterprise Monitoring Server and Tivoli Enterprise Console that is blocking communication over certain ports.	You might need to include the IP addresses of other IBM Tivoli Monitoring components in the access control for the firewall. Refer to Chapter 6, "Connectivity troubleshooting," on page 115 for additional information about solving connectivity problems.

Situations return to acknowledged

The default action of the `omegamon.rls` rule set is to reject acknowledgement expirations that are received from the Tivoli Enterprise Monitoring Server, and to then acknowledge the situation again on the Tivoli Enterprise Monitoring Server. This action of the `omegamon.rls` rule set might be changed to accept acknowledgement expirations from the Tivoli Enterprise Monitoring Server, and therefore leave the situation open in the Tivoli Enterprise Monitoring Server. Refer to the *IBM Tivoli Monitoring Administrator's Guide* for information on changing parameters of the `omegamon.rls` rule set.

Receiving error message when running the Rule Check Utility with the -cd and -rd options

Ensure the class definitions in the TEC_CLASSES directory that you specified with the -cd option include the supporting classes for all rule sets defined in the rule base directory specified by the by -rd option.

Table 52. Rule Base directory and BAROC event class definition directory

Option	Description
-rd	Used to specify a directory containing the rulesets (*.rls) to be checked. If not provided, the TEC_RULES subdirectory for the actively loaded rule base is used by default.
-cd	Used to specify a directory containing the BAROC event class definitions files (*.baroc) to be used as input. If not provided the TEC_CLASSES subdirectory for the actively loaded rule base is used by default.

This is the syntax for the Rule Check Utility:

```
wrules_check {[-h] | [-v] | [-rd rules_directory] [-cd baroc_classes_directory]
{class[,attribute,attribute...] [:classN,attributeN,attributeN] | [-f class_file]}
[-of output_file]}
```

For more information about the Rules Check Utility, refer to the *IBM Tivoli Monitoring Administrator's Guide*.

Expected impacted rules are not displayed when entering multiple event classes with class attributes

Ensure you input ran the **Rules Check Utility** command with the correct options:

```
wrules_check {[-h] | [-v] | [-rd rules_directory] [-cd baroc_classes_directory]
{class[,attribute,attribute...] [:classN,attributeN,attributeN] | [-f class_file]}
[-of output_file]}
```

For more information about the Rules Check Utility, refer to the *IBM Tivoli Monitoring Administrator's Guide*.

The wrules_check command fails

When you run the **wrules_check** command without specifying the –cd and –rd options, you must have permission to run the **wrb** subcommands. Run the **wrules_check** command with the –cd and –rd options or refer to the IBM Tivoli Enterprise Console documentation for more information about running the **wrb** subcommands.

This is the syntax for the Rule Check Utility:

```
wrules_check {[-h] | [-v] | [-rd rules_directory] [-cd baroc_classes_directory]
{class[,attribute,attribute...] [:classN,attributeN,attributeN] | [-f class_file]}
[-of output_file]}
```

Table 53. Rule Base directory and BAROC event class definition directory

Option	Description
-rd	Used to specify a directory containing the rulesets (*.rls) to be checked. If not provided, the TEC_RULES subdirectory for the actively loaded rule base is used by default.
-cd	Used to specify a directory containing the BAROC event class definitions files (*.baroc) to be used as input. If not provided the TEC_CLASSES subdirectory for the actively loaded rule base is used by default.

For more information about the Rules Check Utility, refer to the *IBM Tivoli Monitoring Administrator's Guide*.

Unexpected exception occurred when importing kqr.baroc, kqt.baroc, and kqv.baroc

First import both the `Sentry.baroc` and `om_tec.baroc` files to the rulebase on the Tivoli Enterprise Console server. Then import the `kqr.baroc`, `kqv.baroc`, or `kvm.baroc` files.

The NetView menus are unavailable

Ensure the NetView® console or Web console are installed on the Tivoli Enterprise Portal system and that the NVWC_HOME or NV_DRIVE variables are set correctly.

The IBM Tivoli Enterprise Console is disabled

The Tivoli Enterprise Console relies on the Tivoli Management Framework for common services, including communications. If the console loses contact with Tivoli Management Framework, no new events are added to the view. Do the following to enable event reporting:

1. Reestablish contact between Tivoli Enterprise Console and IBM Tivoli Monitoring.
2. Log off the Tivoli Enterprise Portal.

   Note: If you use Tivoli Enterprise Portal browser client, you must also close and restart the Web browser.
3. Log in to the Tivoli Enterprise Portal again to enable the Tivoli Enterprise Console view to resume event reporting.

When using a Tivoli Enterprise Console view in a workspace, receive an error message instead of event information

When you use a Tivoli Enterprise Console view in a Tivoli Enterprise Portal workspace, you can right-click an event and select **Information** in the context menu to see details regarding an event. However, you might see the following message instead of event information:

```
#C02032E: Failed to receive event information from...
```

Install and configure the optional Sample Event Information component of Tivoli Enterprise Console. This feature enables you to create a help file to record information about an event. Use of the Sample Event Information feature is optional. However, if you do not provide event information for an event, you experience the limitation that is described here.

The IBM Tivoli Enterprise Console does not display in a workspace after logging off and logging on the Tivoli Enterprise Portal

Recycle the Tivoli Enterprise Portal browser so the Tivoli Enterprise Portal can display the IBM Tivoli Enterprise Console in a workspace.

The Tivoli Enterprise Portal stops when attempting to launch the IBM Tivoli Enterprise Console behind a router

After a two-minute timeout, the following message might display when you try to add an IBM Tivoli Enterprise Console view to a Tivoli Enterprise Portal client that is behind a router:

```
The RDBMS cannot be reached.
```

During the timeout period, the Tivoli Enterprise Portal client seems hung. To avoid this problem, the Tivoli Management Framework Administrator must enable communications based on the host name rather than the IP address. Use the following steps to prevent this problem:

1. On the IBM Tivoli Enterprise Console Server on which you are logged in, set the `single_port_bdt` and `set_iom_by_name` Tivoli Management Framework settings to `TRUE` by running the following commands on the IBM Tivoli Enterprise Console Server:

   ```
   odadmin single_port_bdt TRUE all
   odadmin set_iom_by_name TRUE all
   ```

2. Run the following command to recycle the object dispatchers:

```
odadmin reexec all
```

Refer to the *Tivoli Management Framework Reference Manual* for more information about the **odadmin** command.

The error 'ECO2029E: Failed to connect to http://*servername:port_number*/cgi-bin/tec_help.pl.' occurs after clicking the Information button on the IBM Tivoli Enterprise Console

Error ECO2029E occurs because the spider Web Server provided with the IBM Tivoli Enterprise Console Server does not automatically start. To start the spider Web Server, run the **wstarthttpd** command on the Tivoli Management Region server of the IBM Tivoli Enterprise Console that you are logged in to. After the **wstarthttpd** command completes, the information button works. Refer to the *IBM Tivoli Enterprise Console 3.9 Installation Guide* for more information about the **wstarthttpd** command.

T/EC ITM Synchronization Tasks

By default, all situation events that originate from a recycled Tivoli Enterprise Monitoring Server are CLOSED. As a result, you do not need to run any of the three tasks that reside in the T/EC ITM Synchronization Task Library.

IBM Tivoli Enterprise Console task timeout expires while in process

Some tasks like "Close_All_Reset_Events" can require up to an hour to complete, depending on the number of events processed. The task continues processing in the background if the timeout expires, however the task output does not display. You do not need to run the task again. You can increase the task timeout value on task panel to prevent the task from timing out.

General event synchronization troubleshooting

This section contains general troubleshooting information that applies regardless of whether you are using Netcool/OMNIbus or Tivoli Enterprise Console.

Editing the default destination server information from the command line does not work

If the command **tacmd editEventdest** is run specifying a default destination server, these changes are not persistent in the `om_tec.config` file after running the **tacmd refreshTECinfo** command. Here is an example of this command:

```
tacmd editEventdest -i 0 -p host2=nuke.tivlab.austin.ibm.com
```

The new information also does not appear in the output of the command **tacmd viewEventDest**. This occurs because the default destination server information cannot be edited from the command line, but only manually in the `om_tec.config` file.

Manually edit the `om_tec.config` file to specify a default destination server.

tacmd refreshTECinfo -t all shows no results on console

The Tivoli Enterprise Monitoring Server facility used (**DS START** command) to trigger the refresh of the EIF info does not give a return code. So, it is not possible to give feedback as to the success or failure of the operation back to the command line interface. For a result of the refresh, look in the Tivoli Enterprise Monitoring Server log or the Universal Message Console on the Tivoli Enterprise Portal.

Changing the TCP/IP timeout setting on your event server

If the Situation Update Forwarder cannot reach a monitoring server to send an update, it could be up to 15 minutes before the Situation Update Forwarder tries to connect to the monitoring server again, depending on the TCP/IP settings for the computer where your event server is running. This situation might occur if your event server is running on an AIX, Solaris, or HP-UX computer.

Use the following steps to change the TCP/IP timeout for your computer.

On AIX, run the following command:

```
no -o tcp_keepinit=<timeout_value>
```

where *timeout_value* is the length of the timeout period, in half seconds. To configure a timeout of 30 seconds, set the *timeout_value* value to 60.

On Solaris and HP-UX, run the following command:

```
ndd -set /dev/tcp tcp_ip_abort_cinterval <timeout_value>
```

where *timeout_value* is the length of the timeout period, in milliseconds. To configure a timeout of 30 seconds, set the *timeout_value*value to 30000.

Chapter 16. Tivoli Common Reporting troubleshooting

If you cannot display reports, consider the issues and use the messages discussed in this section.

Notes:

1. When a report fails to generate or generates incorrectly, click **View the report with errors** to make diagnosis of the underlying problem easier.
2. When you troubleshoot problems with Tivoli Common Reporting, you should enable detailed logging, using the instructions found in the "Logging and tracing" section of the *IBM Tivoli Common Reporting: User's Guide*.

Locations of log files

There are several logs that might contain information to help you debug problems with Tivoli Common Reporting and reports:

- By default, only errors are logged in the WebSphere® Application Server `SystemOut.log` file.
- If you enable logging and tracing (using the information in "Logging and tracing" section of the *IBM Tivoli Common Reporting: User's Guide*), the Log and trace files are located in the `\profiles\TIPProfile\logs\serverName` subdirectory of the Tivoli Common Reporting installation directory. Standard informational log messages are written to the `SystemOut.log` file; detailed trace messages are written to the `trace.log` file.
- If the connection to Tivoli Data Warehouse cannot be established, look in the WebSphere Application Server `SystemOut.log` file or `SystemErr.log` file for more information. To address this error, ensure the drivers are placed in the correct directory.

For more information about implementing logging in the reports that you create, see http://www.ibm.com/developerworks/tivoli/library/t-tcr/ibm_tiv_tcr_report_logging.pdf

Tivoli Common Reporter uses logger scripts to log during report generation.

If you see Javascript errors in the reports that you create, look for "Caused by"" in the stack trace. This phrase points out the line number of the script in the report design at which the error occurred. To see the SQL query that was generated by this error, look at the log file.

Running OS Cognos Reports with Tivoli Common Reporting 2.1.1 on 64-bit AIX 6.1 results in error DPR-ERR-2056

When running OS Cognos Reports against a DB2 Tivoli Data Warehouse, you might encounter error message DPR-ERR-2056, as depicted in the following example:

```
The Report Server is not responding.

Handler trace back: [the_dispatcher] com.cognos.pogo.handlers.
performance.PerformanceIndicationHandler
[the_dispatcher] com.cognos.pogo.handlers.logic.ChainHandler
[service_lookup] com.cognos.pogo.handlers.engine.ServiceLookupHandler
```

```
[load_balancer] com.cognos.pogo.handlers.logic.ChainHandler
[lb_forwarder] com.cognos.p2plb.clerver.LoadBalanceHandler
[reportservicechain] com.cognos.pogo.handlers.logic.ChainHandler
[ifElseBirthandler] com.ibm.cognos.birtservice.logic.IfElseBirtHandler
[reportservicemain] com.cognos.pogo.handlers.logic.ChainHandler
[warp_with_authenticate] com.cognos.pogo.handlers.logic.ChainHandler
[do_warp] com.cognos.pogo.handlers.logic.ChainHandler
[warpmta] com.cognos.pogo.reportservice.ReportServerHandler
```

To remedy this issue, manually delete the *.rtm files located in the `cognos/data/cqe/RTModels` directory.

Displaying data for Situations History report results in error

If you encounter an error displaying data for the Situations History report, ensure that at least 10 GB of disk space is available after installing Tivoli Common Reporting. This available disk space accomodates temporary data to generate reports on the Tivoli Common Reporting server when you use Tivoli Monitoring provided reports.

Date and time format in IBM Tivoli Monitoring OS Agents reports not localized

When you display IBM Tivoli Monitoring OS Agents reports within Internet Explorer 7 (IE7), you might see date and time formats that are not localized, but display as *MMM dd, yyyy* and *hh:mm* 12h format, instead.

Prompted to select report type when installing reports with CLI

When you install IBM Tivoli Monitoring OS Agents reports within the CLI, you might be prompted to "Choose the report type" after you have already specified the reports you want to install. Simply specify option **2** when prompted. This is a known limitation.

Cognos Query Studio displays Japanese text within the Thai web browser

When working in the Cognos Query Studio, you might see strings of Japanese text within the Thai web browser. This is a limitation of the current product.

The prompt page of a Cognos report within the Tivoli Common Reporting tool displays strings that are not translated

When selecting options from a list box or a combination box in the prompt page of a Cognos report within the Tivoli Common Reporting tool, you might see strings that are not translated at the beginning of the list. The strings do not represent an error. The strings are the internal names of the parameters that are not part of the translatable strings.

The generated report displays an incorrect date and time format

The Utilization Comparison for Single Resource report displays an incorrect date and time format when you select either Excel 2000 or Excel 2002 as the output format and either English or French as the output language. To avoid this situation, select Excel 2007 as the output format.

The generated report does not display report legend

The Top Resources Utilization Summary Heat Chart report does not include the report legend when you select either Excel 2000 or Excel 2002 as the output format and either English or French as the output language. To avoid this situation, select Excel 2007 as the output format.

Receive a 'statement is too long' error message when running a report

When running a report, you receive the following message:

```
SQL0101N the statement is too long or too complex. SQLSTATE=54001.
```

The statement could not be processed because it exceeds a system limit for either length or complexity. Change the DB2 configuration by increasing the db2 statement heap size STMTHEAP to run the report.

Running COGNOS reports against a DB2 database is slow

Check the values of the stmtheap and APPLHEAPSZ database parameters if you have slow performances when running these reports. You might need to increase the db2 statement heap size for these parameters.

Cognos reports are displayed as a blank page

The Cognos server and client are not configured with the same locale and you included decimal numbers. To be able to enter decimal numbers, ensure that the Cognos server and client are configured with the same locale.

You are missing drivers after the Tivoli Common Reporting installation

In this scenario, you have installed Tivoli Common Reporting and imported a report package, but when you try to run a report, you see this message from Tivoli Common Reporting:

```
CTGTRV014E The report can not be successfully formatted because it completed
with errors, reference ID [REPORTID_3_OBJECTID_7ec67ec6].
Click on the following link to view the report with the errors.

CTGTRV011E See the Tivoli Common Reporting log files for more information.
https://localhost:30343/TCR/Reports/view
```

This problem is occurring because you are missing drivers required by Tivoli Common Reporting. You did not copy the required driver files or copied incorrect driver files. Refer to the "Configuring a JDBC data source" topic in the *IBM Tivoli Common Reporting: User's Guide* for additional information about this requirement. For example, if your Tivoli Data Warehouse is running on DB2 and you selected **View the report with errors**, you would see error message:

```
No Data Returned
Warning: No data is available for this parameter set.
```

And this information is displayed:

```
The following items have errors:

ReportDesign (id = 1):
+ Cannot open the connection for the driver: org.eclipse.birt.report.data.oda.jdbc
Cannot load JDBC Driver class: com.ibm.db2.jcc.DB2Driver
```

To address this problem for a DB2 database, you would need to copy the following files:

- db2jcc.jar
- db2jcc_license_cu.jar

Typically found in this default DB2 installation path or in the java directory of whatever alternate path you specified for DB2 installation, into this directory.

Make these corrections and then try running the report again.

You receive message CTGTRW1000E

This error message is often displayed when first entering the Integrated Services Console (ISC) and clicking on Tivoli Common Reporting on the left side of the page. Ignore this error message. Click **OK** on the error message to remove it, and the ISC and Tivoli Common Reporting reports will remain operational.

The report fails to generate because the SQL query was not valid

If you have made changes to the reports or to the workspace against which the query is being run, you could see SQL query errors. Typically this error looks similar to this:

```
The following items have errors:

ReportDesign (id = 1):
+ Cannot get the result set metadata.

SQL statement does not return a ResultSet object.
SQL error #1: DB2 SQL error: SQLCODE: -206 SQLSTATE: 42703, SQLERRMC: ASDF
SQL error #2: DB2 SQL error: SQLCODE: -727,SQLSTATE: 54098, SQLERRMC:
2:-200:42703:ASDF
SQL error #3: DB2 SQL error: SQLCODE: -727,SQLSTATE: 50098, SQLERRMC:
2:-200:42703:ASDF
```

Additional information about the error might be found in the SQLERRMC file.

If you experience SQL errors, try generating the report with a different set of parameters. If all executions of the report generate SQL errors, it is likely that, for some reason, the running report is not compatible with your database.

Message "SQL Statement does not return a ResultSet object" displayed

In this scenario, the report generation process fails to produce a report and this error message will be displayed:

```
SQL Statement does not return a ResultSet object
```

This message is followed by some SQL codes and the name of the table or view that is absent.

This message is displayed when the tables and views from which data is to be extracted do not exist in the database. To view the SQL query that generated this problem and determine what historical data is not being collected, review the log files. See “Locations of log files” on page 263 for the locations of log files.

Your report fails to generate with unexpected error messages displayed

In this scenario, you have defined report parameters for an OMEGAMON XE or NetView for z/OS report and clicked **Run**. After a long wait, these messages are displayed:

```
Processing has ended because of an unexpected error.
See the Tivoli Common Reporting log files for more information
```

These error messages are generated by Tivoli Common Reporting and might indicate that you need to increase the default heap size for the JVM on the java command to start the Tivoli Common Reporting server. To confirm that this is the problem, do the following:

1. Open the `SystemOut.log` file, found in this location:

   On Windows Systems: <*tcr_install_dir*>`/tcr/eWas61/profiles/tcrProfile/logs/tcrServer/`
2. Confirm that this line can be found:

   ```
   An OutOfMemory error happened while running the report.
   ```

If you find this line, do the following to correct this problem:

1. Stop Tivoli Common Reporting.
2. Edit the `startServer.bat` file, usually found in this location:

   On Windows Systems: `C:\Program Files\IBM\tivoli\tip\bin`
3. Locate this instruction about half way through the bat file:

   ```
   "%JAVA_HOME%\bin\java" -Dcmd.properties.file=%TMPJAVAPROPFILE% %WAS_TRACE%
   %WAS_DEBUG% %CONSOLE_ENCODING% "%CLIENTSAS%" "%CLIENTSSL%"
   %USER_INSTALL_PROP% "-Dwas.install.root=%WAS_HOME%" com.ibm.ws.bootstrap
   .WSLauncher com.ibm.ws.management.tools.WsServerLauncher "%CONFIG_ROOT%"
   "%WAS_CELL%" "%WAS_NODE%" %* %WORKSPACE_ROOT_PROP%
   ```
4. Increase the JVM heap size by adding the `-xms` and `-xmx` options, as in the example shown below:

   ```
   "%JAVA_HOME%\bin\java" -Xms128m -Xmx512m -Dcmd.properties
   .file=%TMPJAVAPROPFILE% %WAS_TRACE% %WAS_DEBUG% %CONSOLE_ENCODING% "%CLIENTSAS%"
   "%CLIENTSSL%" %USER_INSTALL_PROP% "-Dwas.install.root=%WAS_HOME%" com.ibm.ws
   .bootstrap.WSLauncher com.ibm.ws.management.tools.WsServerLauncher
   "%CONFIG_ROOT%" "%WAS_CELL%" "%WAS_NODE%" %* %WORKSPACE_ROOT_PROP%
   ```
5. Re-start the Tivoli Common Reporting server and try generating the report again.

The generated report displays the message "SQL Error"

In this scenario, you complete the report parameters window to generate a report and click **Submit**. After clicking **Submit**, you see a new report page that shows the error message `SQL error` displayed at the bottom of the report.

Here are some possible reasons for this error:

- The Tivoli Data Warehouse does not contain all of the attributes requested by the report. This happens when you are running the report against an unsupported product version such as a version 3.1 OMEGAMON XE monitoring agent or a version of NetView for z/OS prior to 5.3.
- You did not allocate and configure historical data sets when you configured the monitoring agent using the Configuration Tool, or did not enable historical collection from Tivoli Enterprise Portal, or not enough time has passed for Tivoli

Data Warehouse to collect the data for your requested report time period before you tried to generate an historical report with Tivoli Common Reporting.

- You might have incorrect or missing agent .atr files installed at the Warehouse Proxy Agent.
- You might have attempted to use reports with a non-supported database manager. All reports work with DB2 UDB, and some reports work with other database managers supported by Tivoli Data Warehouse DW. You could circumvent this problem by collecting Tivoli Data Warehouse data in DB2 and then switching the TCR Data Source for the affected report package to that DB2 database.

Verify at the Tivoli Enterprise Portal console that you see the Historical Collection icon for the subject workspace and can draw a report for the subject time period. If you cannot, you do not have historical collection enabled. Start it and try the task again.

The report fails with a SQLSTATE:22003 arithmetic overflow error

In this scenario, you have defined report parameters for an OMEGAMON XE or NetView report and clicked **Run**. Report processing ends rather quickly and you see an error messages similar to these:

```
CTGTRV014E The report can not be successfully formatted because it completed with
errors, reference ID [REPORTID_59_OBJECTID_6bee6bee]. Click on the following link to
view the report with the errors.
```

Or:

```
CTGTRV011E See the Tivoli Common Reporting log files for more information.
https://localhost:30343/TCR/Reports/view
```

After seeing this message, if you click to the link **View the report with the errors**, you see this message displayed at the bottom:

```
 ReportDesign (id = 1):
+ Cannot execute the statement.
SQL statement does not return a ResultSet object.
SQL error #1: DB2 SQL error: SQLCODE: -802, SQLSTATE: 22003, SQLERRMC: null
```

Finding the statement `SQLSTATE 22003` indicates that you are experiencing a SQL arithmetic overflow at the Tivoli Data Warehouse database.

To remedy the problem, choose a smaller time period (the recommended action) or possibly a different metric. This change causes the calculations being performed for the report to process less data, reducing the chance of overflow.

Note: All occurrences of this failure in the IBM-provided reports were eliminated by casting DB2 Integer values to `DECIMAL(column_name 31,0)`. This problem should not occur with IBM-provided reports, but could be an issue in customer-generated reports.

No data is plotted in graph, or some columns in the table are blank

In this scenario, you complete the report parameters window to generate a report. After clicking **Submit**, you see a report where some columns have data and some do not.

When you check version levels, you find that the version of database manager you are using for Tivoli Data Warehouse is correct and that it is defined as your data

source and that all the requested columns in the attribute table are available. However, even though data is displayed in the other columns of this table in Tivoli Enterprise Portal, no data is available in the column needed to draw the graph.

Historical data sets have been allocated, and historical collection has been configured and enabled Some data has been collected. Tivoli Common Reporting is configured and is drawing a partial report. If the report does not meet your needs, you may be able to obtain the needed data by one of these methods:

- By choosing a different attribute on the **Report Parameters** window.
- By ensuring that data for the selected attribute is available for this workspace configuration. For example, the OMEGAMON XE for Mainframe Networks monitoring agent cannot collect data for some attributes in OSA reports, depending on how the OSA adapter is configured.

Confirm that the values for these attributes are being displayed in Tivoli Enterprise Portal. If no data is being collected for a key attribute because of configuration issues, consult the product manual to see what configuration change would provide data for the missing attributes.

To determine the cause of this problem you need to enable detailed logging in Tivoli Common Reporting, as described in the *IBM Tivoli Common Reporting: User's Guide*, and you need to know which agent table (or attribute group) contains the attribute that is not being displayed. Go to the Tivoli Enterprise Portal console and validate that this column contains data and, if the issue is with summarized data, that summarization is enabled for this attribute.

Another reason might be that you have not configured historical collection when you installed and configured the monitoring agent or that not enough time has passed for Tivoli Data Warehouse to collect the data for your requested report time period before you tried to generate an historical report with Tivoli Common Reporting. If you do not see the historical collection icon (a clock) in the workspace in Tivoli Enterprise Portal, then data has not been collected in Tivoli Data Warehouse.

The solution might require changes to the persistent datastore, the z/OS repository for short-term historical data. Those changes should be made using the Configuration Tool.

The generated report displays the message "The requested data is not available"

In this scenario, you complete the report parameters window to generate a report and click **Submit**. After clicking **Submit**, you see a blank report page with no graphed or tabular information and the error message `The requested data is not available` is displayed in the message area.

When you check version levels, you find that Tivoli Data Warehouse is your data source, but none of the requested columns in the Tivoli Enterprise Portal attribute table contain data.

This indicates that no data is being collected in Tivoli Data Warehouse. Verify this by querying the same table in the database or by requesting data from the matching workspace, for this time period, in the Tivoli Enterprise Portal. If, for example, your installation stopped collecting historical data for this report 8 days

ago, and you query the last 7 day, no data will be returned. If the managed resource (for example, a TN3270 Server or a CICS® Region) were taken offline, then no data can be collected.

To address the time period issue, expand the time period for your query. To correct the resource availability issue, ensure that the managed resource is online and your agent is collecting data for it.

The solution might require changes to the persistent datastore, the z/OS repository for short-term historical data. Those changes should be made using the Configuration Tool.

You receive the message "serverName is unknown host"

This error message is displayed as red text at the bottom of a report. Although this error can occur for several reasons, the most common problem is incorrectly entering the Tivoli Data Warehouse database URL into the data source for the report. If some reports are working and others are not, the URL was entered incorrectly. If no reports are working, contact those within your organization who installed the product for the correct URL.

You receive the message "Empty Data Set"

The Empty Data Set message is not an error. The message is displayed to convey that no data was returned when it ran the report. The message is usually displayed for one of three reasons:

- The report parameters have excluded all the data.
- You recently started using IBM Tivoli Monitoring for Energy Management and have not put data into the Tivoli Data Warehouse.
- The computers you are monitoring do not have the correct level of firmware.

If you think you have received this message incorrectly, run the Exception Report to find if there is another reason why no data is being returned.

Chapter 17. Tivoli Audit Facility troubleshooting

An auditing facility in IBM Tivoli Monitoring includes detailed information for certain major state changes or events that occur within your monitoring environment. Audit events in the system reflect authorization and authentication failures, and major and minor changes, but do not reflect minor service messages stored in the RAS logs.

Audit Log workspace shows only 100 of the most recent audit records

By default, all Tivoli Monitoring components show only the 100 most recent audit records in the Audit Log workspace. The environment variable, AUDIT_MAX_HIST, defines the maximum number of audit records kept in short-term memory for direct queries. You can increase the setting for this environment variable and recycle the component that you want to display more audit records in the Audit Log workspace. Note that only audit events created since the component was started are displayed.

If you want to display audit records for events that occured before the most recent component startup, you must enable historical data collection for the ITM Audit attribute group and distribute the history collection settings to the components you want to have access to the historical audit data.

If data warehousing is available, it might be more efficient to collect audit records historically from critical ITM components. See the Audit Log workspace description in the *Tivoli Enterprise Portal User's Guide* for details on configuring historical data collection for the ITM Audit attribute group.

Audit Log workspace does not display records before the latest component startup

The Audit Log workspace shows audit records generated since the component was most recently started. To access audit records that were generated before the latest restart, collect audit records historically from critical ITM components. See the Audit Log workspace description in the *Tivoli Enterprise Portal User's Guide* for details on configuring historical data collection for the ITM Audit attribute group.

On distributed systems, you can also examine the component's XML-formatted audit log to access audit records that were generated prior to the latest restart. These logs are located on the component in the *<install_dir>/auditlogs* directory. Refer to *Appendix F. ITM Audit log* in the *IBM Tivoli Monitoring Version 6.2.3 Administrator's Guide*.

ITM components in a z/OS environment can enable the SMF audit facility to collect ITM Audit records. For more information, see the *Planning and Configuration Guide* for the specific component.

Appendix A. IBM Tivoli Monitoring processes

The following table lists the processes according to operating system platform and IBM Tivoli Monitoring component.

Table 54. IBM Tivoli Monitoring processes by operating system

Component	Windows	UNIX and Linux-based systems
Tivoli Enterprise Monitoring Server	cms.exe kdsmain.exe	cms kdsmain
Tivoli Enterprise Portal Server	KfwServices.exe	KfwServices
UNIX agent	N/A	kuxagent
Linux agent	N/A	klzagent
Windows agent	kntcma.exe	N/A
Universal agent	kuma610.exe	kuma610
Log Alert agent	N/A	kulagent
Warehouse proxy agent	khdxprto.exe	khdxprtj
Summarization and Pruning Agent	ksy610.exe	ksy610
Eclipse help server	kkfhelpsvr.exe	kkfstart.sh for the java process, search for /kf/ in the process name

Appendix B. Environment variables

This appendix lists IBM Tivoli Monitoring environment variables that you can customize.

Common environment variables

The following table lists the environment variables that are common to all components:

Table 55. Common environment variables

Variable	Value type	Useful for . . .
KDC_DEBUG	Y or N	Default is N. Diagnosing communications or connectivity problems between the Tivoli Enterprise Portal Server to the Tivoli Enterprise Monitoring Server.
KDH_DEBUG	Y or N	Default is N. Diagnosing connectivity problem with integrated web server.
KDH_SERVICEPOINT		Determining the service point.
KBB_RAS1	Trace specification string	See each specific environment variable section below.
KBB_RAS1LOG		Determining the count limit and the max files settings.
TACMD_JVM_MAX _MEMORY	256 through to 2048	Increase the java JVM memory size

Tivoli Enterprise Portal Server environment variables

The following table lists Tivoli Enterprise Portal Server environment variables.

Table 56. Tivoli Enterprise Portal Server environment variables

Variable	Value type	Useful for . . .
DSUSER1	Y or N	Part of a set of 9 variables DSUSER1...DSUSER9 that you can set using the **tacmd configureportalserve**r command. For more information, see the *IBM Tivoli Monitoring Administrator's Guide*.
KBB_RAS1	Trace specification string	Default tracing level: KBB_RAS1=ERROR Diagnosing client request problems: KBB_RAS1=ERROR (UNIT:ctsql IN ER) (UNIT:ctdata IN ER) Diagnosing client or Tivoli Enterprise Monitoring Server interaction problems: KBB_RAS1=ERROR (UNIT:ctsql IN ER) (UNIT:ctdata IN ER) (UNIT:ctcmw IN ER) (UNIT:kv4 IN ER) Diagnosing SQL generation problems: KBB_RAS1=ERROR (UNIT:ctsql IN ER) (UNIT:ctdata IN ER) (UNIT:ctreport ALL) Diagnosing login problems: KBB_RAS1=ERROR (UNIT:ctsql IN ER) (UNIT:ctdata IN ER) (UNIT:ctauth ALL)
KFW_CMW_SPECIAL_HUB_ ENTERPRISE=N	Y or N	Default is N. When set to Y, associates situations to the Tivoli Enterprise Portal Server.
KFW_DATABUS_INPUT_ TRACE_IGNORE_HEARTBEAT	Y or N	Default is N. Reduces trace volume by skipping client heartbeat requests when (UNIT:ctdata IN ER) request tracing is used.
KFW_DATABUS_QUERY_ VERBOSE	Y or N	Default is N. Tivoli Enterprise Portal Server client side response time and request life cycle tracing.
KFW_MIGRATE_CMS	Y or N	Default is N. When set to Y, causes initial migration of managed objects and user IDs from the monitoring server the first time the Tivoli Enterprise Portal Server starts after installation.
KFW_MIGRATE_FORCE	Y or N	Default is N. When set to Y, SQL seed files are processed even if the date, time, or size of the files have not changed since prior seeding. This occurs when running the `buildpresentation.bat` file (Windows) and when running the `InstallPresentation.sh` file or reconfiguring the Tivoli Enterprise Portal Server (UNIX/Linux). To be effective, this value must be set in `kfwalone` (Windows) or in `cq.ini` or `lnxenvnocms` (UNIX/Linux).
KFW_MIGRATE_VERBOSE	Y or N	Default is N. When set to Y, provides greater detail about operations performed in `migrate.log` when seeding the Tivoli Enterprise Portal Server database. This occurs when running the `buildpresentation.bat` file (Windows) and when running the `InstallPresentation.sh` file or reconfiguring the Tivoli Enterprise Portal Server (UNIX/Linux). To be effective, this value must be set in `kfwalone` (Windows) or in `cq.ini` or `lnxenvnocms` (UNIX/Linux).

Table 56. Tivoli Enterprise Portal Server environment variables (continued)

Variable	Value type	Useful for . . .
KFW_REPORT_FIND_ WAREHOUSE_AT_ STARTUP	Y or N	Default is Y. When set to Y, the portal server queries the data warehouse during startup. If set to N, the warehouse will be initialized at the first deliberate query instead of pre-initialized.
KFW_REPORT_TERM_ BREAK_POINT	Y or N	Default is N. When set to Y, specifies the point where a historical request selects from short-term or long-term history data.
KFW_SQL_VERBOSE	Y or N	Default is N. When set to Y, provides RAS1 trace of each SQL statement issued by the Tivoli Enterprise Portal Server to the Tivoli Enterprise Monitoring Server or to the DB2/ODBC data source. The use of this variable is deprecated because the same capability is available using the standard RAS1 trace setting "KBB_RAS1=ERROR (UNIT:ctsql IN ER)"
MSG_MODE	kms or MSG2	Specify kms if you want to use IBM Tivoli Monitoring Operations Logging. Specify MSG2 to use MSG2 logging.

Tivoli Enterprise Monitoring Server environment variables

The following table lists Tivoli Enterprise Monitoring Server environment variables.

Table 57. Tivoli Enterprise Monitoring Server environment variables

Variable	Purpose
ATTRLIB	Specifies the Tivoli Enterprise Monitoring Server attribute (ATR) files directory.
CANDLE_HOME	The directory where the product was installed.
CMS_BINPATH	Specifies the Tivoli Enterprise Monitoring Server binary files directory.
CMS_EXTERNALBROKERS	Whether there are internal brokers.
CMS_FTO	Whether to use Tivoli Enterprise Monitoring Server Hot Standby.
CMS_MSGBASE	Specifies the Tivoli Enterprise Monitoring Server message file directory.
CMS_NODEID	The Tivoli Enterprise Monitoring Server IBM Tivoli Monitoring Node ID.
CMS_NODE_VALIDATION	Enables the rejection of incorrect managed system names.
KDC_GLBSITES	Specifies the Tivoli Enterprise Monitoring Server global sites network file with Tivoli Enterprise Monitoring Server Hub host names.
KDH_SERVICEPOINT	The service point.
KDS_CATLGLIB	Specifies the catalog library.
KDS_HUB	Specifies that this Tivoli Enterprise Monitoring Server is a Hub Tivoli Enterprise Monitoring Server (*LOCAL) or Remote Tivoli Enterprise Monitoring Server (*REMOTE).
KDS_NCS	Whether to use IBM Tivoli Monitoring network lookup services.
KDS_RULELIB	Specifies the rule library.
KDS_RUN	Specifies Tivoli Enterprise Monitoring Server components or probes to run at Tivoli Enterprise Monitoring Server startup.
KDS_START	Specifies Tivoli Enterprise Monitoring Server KDS component startup.
KDS_VALIDATE	Whether to use Tivoli Enterprise Monitoring Server authentication.
KGLCB_FSYNC_ENABLED	Whether to enable UNIX or Linux fsync calls.

Table 57. Tivoli Enterprise Monitoring Server environment variables (continued)

Variable	Purpose
KGL_CBTBUFCNT	Specifies Tivoli Enterprise Monitoring Server internal table buffer count.
KGL_CBTBUFSZ	Specifies Tivoli Enterprise Monitoring Server internal table buffer size.
KGL_KEYRING_FILE	Specifies LDAP authentication SSL GSKit keyring file.
KGL_KEYRING_LABEL	Specifies LDAP authentication SSL GSKit keyring label.
KGL_KEYRING_PASSWORD	Specifies LDAP authentication SSL GSKit keyring password.
KGL_KEYRING_STASH	Specifies LDAP authentication SSL GSKit keyring password stash file.
KGL_KGLMSGBASE	Specifies the Tivoli Enterprise Monitoring Server KGL message file directory.
KGL_LDAP_BASE	LDAP authentication LDAP search base.
KGL_LDAP_BIND_ID	LDAP authentication LDAP server bind Distinguished Name (DN).
KGL_LDAP_BIND_PASSWORD	LDAP authentication LDAP server bind password.
KGL_LDAP_HOST_NAME	LDAP authentication LDAP server host name.
KGL_LDAP_PORT	LDAP authentication LDAP server port.
KGL_LDAP_SSL_ENABLED	Whether to use LDAP SSL communications.
KGL_LDAP_USER_FILTER	LDAP authentication user filter.
KGL_LDAP_VALIDATE	Whether to use LDAP authentication.
KGL_MSG2_EVENTLOG	Whether to format Event Log.
KGL_MSG2_UNIVERSAL	Whether to enable Universal Messages.
KGL_TRC1	Whether to enable the error log.
KHD_HISTRETENTION	Specifies the default retention period in hours for the short term history files (default is 24 hours). This can be used to reduce the amount of data kept on disk after a successful upload to the warehouse is performed.
KIB_MAXCOLS	Tivoli Enterprise Monitoring Server internal dictionary column maximum.
KMS_DISABLE_TEC_EMITTER	TEC Emitter to be disabled.
KMS_OMTEC_ GLOBALIZATION_LOC	TEC Integration Globalization locale.
KMS_OMTEC_INTEGRATION	TEC Integration enabled.
KPX_WAREHOUSE_LOCATION	Allows a fixed warehouse route for the agents connected to that Tivoli Enterprise Monitoring Server when the usage of the Global Location Broker default algorithm is not supported. It is a list of fully qualified, semicolon delimited network names such as: `KPX_WAREHOUSE_LOCATION= family_protocol: #network_address[port_number]; ...`
KPX_WAREHOUSE_REGCHK	Number of minutes to wait between re-checking the Global Location Broker for any warehouse proxy agent registration changes. The default value is set to 60 minutes.
KSH_DIRECTORY	Specifies the Tivoli Enterprise Monitoring Server SOAP Server HTML files directory.
KT1_TEMS_SECURE	YES is required for the tacmd commands, **putfile**, **getfile**, and **executecommand**. Also required when **executeaction** is issued with advanced options. Not required when issuing **executeaction** to agent without advanced options.
MSG_MODE	Specify kms if you want to use IBM Tivoli Monitoring Operations Logging. Specify MSG2 to use MSG2 logging.
NLS1_LOCALEDIR	The directory of the locale file.
RKDSCATL	Specifies the Tivoli Enterprise Monitoring Server catalogue (CAT) files directory.

Table 57. Tivoli Enterprise Monitoring Server environment variables (continued)

Variable	Purpose
SQLLIB	Specifies the Tivoli Enterprise Monitoring Server seeding and query (SQL) files directory.

Universal Agent environment variables

The following table lists environment variables you can set to customize tracing for the Universal Agent.

Table 58. Universal Agent environment variables

Variable	Purpose
KBB_RAS1=ERROR (UNIT:kumamain ALL)	Problems involving managed system online/offline processing.
KBB_RAS1=ERROR (UNIT:kumpdpda Error Output) (UNIT:kumpmd2a Error Detail)	Incorrect report data.
KBB_RAS1=ERROR (UNIT:kumpfile Error State Detail Flow Metrics) (UNIT:kumpdcmf ALL)	Detailed File Data Provider tracing.
KBB_RAS1=ERROR (UNIT:kumpsosr ALL) (UNIT:kumpspst ALL) (UNIT:kumpscku ALL) (UNIT:kumpstcp ALL) (UNIT:kumplpba ALL)	Detailed API or Socket Data Provider tracing.
KBB_RAS1=ERROR METRICS	Problems involving Universal Agent memory usage.
KUMA_DCH_TRAPEMIT	SNMP Emitter tracing. Use to display emitted traps in the UAGENT Action report.
KUMA_VERBOSE	Tracing a Universal Agent API client program. This variable must be set on the system where the API client program is executing, not where Universal Agent is running) Example: KUMP_API_VERBOSE=Y dpapi.log. The KUMP_API_VERBOSE option is valuable when debugging an API program that communicates with the Universal Agent API data provider.
KUMP_HTTP_DEBUG	HTTP Data Provider tracing.
KUMP_ODBC_DEBUG	ODBC Data Provider tracing.
KUMP_SCRIPT_DEBUG	Script Data Provider tracing.
KUMP_SNMP_DEBUG_TRAP KUMP_SNMP_DEBUG_DISCOVERY_ROUTE KUMP_SNMP_DEBUG_DISCOVERY_NETWORK KUMP_SNMP_DEBUG_MIB_MANAGER KUMP_SNMP_DEBUG_MIB_IO	SNMP Data Provider tracing. All of the debug environment variables listed default to No. As an example, if you use the SNMP Data Provider and have problems collecting MIB data, you set these two environment variables: KUMP_SNMP_DEBUG_MIB_MANAGER=Y KUMP_SNMP_DEBUG_MIB_IO=Y

For a complete list of the Universal Agent environment variables, see the *IBM Tivoli Universal Agent User's Guide*.

Tivoli Data Warehouse environment variables

The following Tivoli Data Warehouse parameters can be changed in the KHDENV_MIG file to customize tracing for the warehouse upgrade tool.

Table 59. Tivoli Data Warehouse environment variables

Variable	Purpose
KHD_MAX_ROWS_SKIPPED_PER_TABLE	Specifies the maximum number of rows per table that can be skipped during an upgrade. Rows with incorrect data are skipped until the maximum specified number is reached. When this number of rows are skipped, the migration of the table is aborted.
KHD_MAX_ROWS_PER_TRANSACTIONS	Specifies how many rows are committed at each insert of data.
KHD_CNP_SERVER_HOST	Specifies the name of the CNP server.
KHD_CNP_SERVER_PORT	Specifies the port used by the CNP server.
KHD_SOURCE_DATABASE_SCHEMA	Specifies the owner or schema of the Candle tables in the source database.
KHD_SOURCE_JDBC_DRIVER	Specifies the JDBC driver used to connect to the source database.
KHD_SOURCE_URL	Specifies the URL to connect to the source database
KHD_SOURCE_DATABASE_USER	Specifies the user to connect to the source database.
KHD_SOURCE_DATABASE_PASSWORD	Specifies the password to connect to the source database.
KHD_TARGET_JDBC_DRIVER	Specifies the JDBC driver used to connect to the target database
KHD_TARGET _URL	Specifies the URL to connect to the target database
KHD_TARGET _DATABASE_SCHEMA	Specifies the owner or schema of the tables in the target database
KHD_TARGET _DATABASE_USER	Specifies the user to connect to the target database
KHD_TARGET _DATABASE_PASSWORD	Specifies the password to connect to the target database

The following Warehouse Proxy agent parameters can be changed in the KHDENV file on Windows systems and the hd.ini file in non-Windows systems to customize tracing for the Warehouse Proxy agent.

Table 60. Warehouse proxy environment variables

Variable	Purpose
CTIRA_NCSLISTEN	The number of RPC threads.
KHD_BATCH_USE	Reduces network flow when the Tivoli Data Warehouse database is not installed on the same system where the warehouse proxy agent resides, this variable must be set to Y. This functionality is available on both Windows and UNIX systems. This is done automatically when the Use Batch check box on the UNIX warehouse proxy configuration panel is checked.
KHD_CNX_POOL_SIZE	The total number of preinitialized ODBC connection objects available to the work queue export threads. The default value is 3.
KHD_CNX_WAIT	The time in minutes to wait before trying to reconnect. Default is 10 minutes.
KHD_CNX_WAIT_ENABLE	A time to wait before a retry. Default is Y. Changing this variable to N does not wait before retries. Setting this variable to N can generate a large log file if the tests to the database fail at each retry.
KHD_EXPORT_THREADS	The number of worker threads exporting data to the database. The default value is 10.

Table 60. Warehouse proxy environment variables (continued)

Variable	Purpose
KHD_QUEUE_LENGTH	The length of the KHD work queue. This is an integer that identifies the maximum number of export work requests that can be placed on the work queue before the queue starts rejecting requests. The default value of KHD_QUEUE_LENGTH is 1000. Setting this value to 0 means the queue length has no limit.
KHD_SRV_STATUSTIMEOUT	The time in seconds set by default to 600s = 10 minutes. Set KHD_SRV_STATUSTIMEOUT less than KHD_STATUSTIMEOUT by at least 60 seconds.
KHD_STATUSTIMEOUT	The time in seconds set by default to 900s = 15 minutes. An export request on the application agent is resent if a status is not received from the Warehouse Proxy agent before the timeout expires.
KHD_WAREHOUSE_TEMS_LIST	A space or coma delimited separated list of monitoring server. A warehouse proxy agent serves all the agents reporting to those monitoring servers listed. The same monitoring server name must not appear more than once in all the warehouse proxy Tivoli Enterprise Monitoring Server lists in the entire enterprise environment.
KHD_DB_COMPRESSION	Used to change the configuration of the Warehouse Proxy Agent to enable or disable database compression.
KHD_WHLOG_ENABLE	Used to change the configuration of the Warehouse Proxy Agent to enable or disable data warehouse log tables.
KHD_SERVER_DIST_ COMPRESSION_ENABLE	Used to send compressed data. This variable is set to Y by default.
KHD_SERVER_Z_ COMPRESSION_ ENABLE	Used to allow z/OS clients to send compressed data. This variable is set to N by default.
KHD_CLIENT_ COMPRESSION_ ENABLE	Used to specify that historical data will not be compressed if set to N. This is true even if the Warehouse Proxy Agent server has allowed the compression. This variable does not exist by default.

Table 61 lists the Summarization and Pruning agent parameters that you can edit in the `KSYENV` file on Windows systems and the `SY.ini` file on non-Windows systems to customize tracing for the Summarization and Pruning agent.

Table 61. Summarization and Pruning agent environment variables

Variable	Purpose
KSY_BLACKOUT	Specifies a comma separated list of exception times where the Summarization and Pruning agent should not start when using the flexible scheduling. The values in the list should be in the format HH:MM-HH:MM where HH must be between 00 and 23 and MM must be between 00 and 59. The starting time must be smaller than the end time of the exception period. For example, to block the Summarization and Pruning agent from starting between 1 and 2 AM and 5 and 6 PM, use the following: 01:00-01:59,17:00-17:59.
KSY_CNP_SERVER_HOST	Tivoli Enterprise Portal Server connection default host.
KSY_CNP_SERVER_PORT	Tivoli Enterprise Portal Server connection default port.
KSY_DAY_AGE_UNITS	The minimum age of data for daily data in days before aggregation is done.
KSY_EVERY_N_DAYS	How often to run the schedule in days (number).

Table 61. Summarization and Pruning agent environment variables (continued)

Variable	Purpose
KSY_EVERY_N_MINS	Indicates the frequency between Summarization and Pruning agent runs when using the flexible scheduling. Must be a multiple of 15 minutes, with a minimum of 15 and a maximum of 1440 (one day).
KSY_FIXED_SCHEDULE	Indicates whether the Summarization and Pruning agent is configured for fixed schedule if set to Y or flexible schedule when set to N.
KSY_HOUR_AGE_UNITS	The minimum age of data for hourly data in hours before aggregation is done.
KSY_HOUR_AM_PM	Whether to run in the AM or PM (AM/PM).
KSY_HOUR_TO_RUN	The hour of the day to run (number).
KSY_MAX_ROWS_PER_ TRANSACTION	Maximum rows per database transaction.
KSY_MAX_WORKER_THREADS	Maximum number of simultaneous worker threads. Default is 1. Recommended value is the number of processors on your server minus 1.
KSY_MINUTE_TO_RUN	The minute of the day to run (number).
KSY_SHIFT1_HOURS	A comma-separated list of hour numbers for the shift.
KSY_SHIFT2_HOURS	A comma-separated list of hour numbers for the shift.
KSY_SHIFTS_ENABLED	Shift periods. Only two shifts are allowed. If shifts are enabled, each hour (0-23) must be specified once.
KSY_START_OF_WEEK_DAY	Start of the week day, for example: 0 = Sunday 1 = Monday.
KSY_TIMEZONE_IND	Time zone indicator. AGENT specifies use the time zone offset of the agent. WAREHOUSE specifies use the time zone offset of the warehouse .
KSY_VACATION_DAYS	Vacation days in a comma-separated list of days in YYYYMMDD format.
KSY_VACATIONS_ENABLED	Whether or not vacation are enabled with Y or N.
KSY_WAREHOUSEAGGREGLOG_PRUNE	Use to specify the pruning for the WAREHOUSEAGGREGLOG table. The format of the value should be *number.unit*, where *number* is the number of units to retain and *unit* specifies the retention unit, which can be one of day, month or year.
KSY_WAREHOUSELOG_PRUNE	Use to specify the pruning for the WAREHOUSELOG table. The format of the value should be *number.unit*, where *number* is the number of units to retain and *unit* specifies the retention unit, which can be one of day, month or year.
KSY_WAREHOUSE_DRIVER	The Warehouse Database Connection JDBC Driver.
KSY_WAREHOUSE_PASSWORD	The Warehouse Database Connection Password (encrypted).
KSY_WAREHOUSE_SCHEMA	The Warehouse Database Connection Schema.
KSY_WAREHOUSE_URL	The Warehouse Database Connection JDBC URL.
KSY_WAREHOUSE_USER	The Warehouse Database Connection User (encrypted).
KSY_WEEKENDS_AS_VACATIONS	Whether or not weekends are vacation with Y or N.
KSZ_JAVA_ARGS	Java arguments.
KSY_WHLOG_ENABLE	Used to change the configuration of the Summarization and Pruning Agent to enable or disable data warehouse log tables.
KSY_DB_COMPRESSION	Used to change the configuration of the Summarization and Pruning Agent to enable or disable database compression.

Tivoli Enterprise Monitoring Agent deploy environment variables

The following Tivoli Enterprise Monitoring Agent parameters can be changed in the KBBENV file:

Table 62. Tivoli Enterprise Monitoring Agent deploy environment variables

Variable	Purpose
AGENTDEPOT	An OS agent parameter. Determines the location on the agent host where agent bundles will be transferred.
CMS_MSGBASE	Applies to is/5 platform Tivoli Enterprise Monitoring Agent only. Specify the MSG2 message file for Tivoli Enterprise Monitoring Agent framework messages.
CT_CMSDIRECT	OBSOLETE – Has been replaced by IBM Tivoli Monitoring v6.X firewall communications services. Specify the full NAT firewall address of the Tivoli Enterprise Monitoring Server to be connected to, including protocol:address[port#].
CT_CMSLIST	Required variable specifying the primary and/or secondary Tivoli Enterprise Monitoring Server for the agent to connect with. Takes a semicolon delimited list of Tivoli Enterprise Monitoring Server by network protocol:hostname or protocol:address.
CTIRA_CELL_NAME	OBSOLETE – Agents only. Replaced by agent configuration variable CT_CMSLIST.
CTIRA_HEARTBEAT	The interval, in minutes, of the agent to Tivoli Enterprise Monitoring Server heartbeat data sample. Default is 10 minutes. Using shorter heartbeat intervals will increase network traffic between the agent and Tivoli Enterprise Monitoring Server.
CTIRA_HIST_DIR	Required variable specifying the directory where Tivoli Enterprise Monitoring Agent based short-term history data files will be stored. Does not apply to Tivoli Enterprise Monitoring Server short-term history data files.
CTIRA_HOSTNAME	Used by many, but not all, agents to provide an alternate hostname qualifier (subsystem:hostname:nodetype) for the published agent managed system name. Used to remove a long network domain name, for example, acme.us.com, from the default Tivoli Enterprise Monitoring Agent hostname. Not honored by all agents. For some agents, might cause unpredictable Tivoli Enterprise Portal navigation tree results.
CTIRA_IP_PORT	Applies to z/OS agents only. DO NOT MODIFY. Is set to 0 so the OS can provide the agent rpc listen port. Avoids a port conflict for some z/OS configurations.
CTIRA_LOG_PATH	Required variable specifying the directory where the Tivoli Enterprise Monitoring Agent Operations Log file is stored. The file names use suffix of ".LG0" and ".LG1". Does not apply to z/OS based agents.
CTIRA_MAX_RECONNECT _TRIES	Number of consecutive times without success the agent will attempt to connect to a Tivoli Enterprise Monitoring Server before giving up and exiting. Default is 720. This environment variable is now obsolete. If you decide to use this variable, and the number of connection attempts to the monitoring server exceeds CTIRA_MAX_RECONNECT_TRIES, the agent attempts to shutdown. If the Agent Management Services Watchdog is running, it immediately restarts the agent. If you want the agent to shutdown when CTIRA_MAX_RECONNECT_TRIES is exceeded, this Watchdog process must be disabled. Use the AMS Stop Management action to disable this watchdog process.
CTIRA_NCSLISTEN	Number of RPC listen server threads to create for the agent. Default is 10.
CTIRA_NODETYPE	Supply the agent node type qualifier (subsystem:hostname:nodetype) of the agent managed system name (MSN). Provide the agent product indicator in the MSN. Value can also be set by the Tivoli Enterprise Monitoring Agent API.

Table 62. Tivoli Enterprise Monitoring Agent deploy environment variables (continued)

Variable	Purpose
CTIRA_OS_INFO	Override default value for agent entries in the Tivoli Enterprise Monitoring Server "ManagedSystem.Host_Info" column. Used to build Tivoli Enterprise Portal Server navigation tree. Value must match existing entry in the `CNPS/osnames` file. Not applicable to subnode type records in the ManagedSystem table.
CTIRA_PRODUCT_SEP	Supply alternate qualifier for the agent managed system name (MSN). Default is a colon character ':'.
CTIRA_RECONNECT_WAIT	Time interval, in seconds, for the agent to wait between attempts to register with a Tivoli Enterprise Monitoring Server. Default is 600 seconds.
CTIRA_REFLEX_ATOMIC	Default is "Y". For subnode targets only. Evaluate situation state by any existing specified display item column name when deciding which reflex situation automation command the Tivoli Enterprise Monitoring Agent should execute. Not applicable to reflex situation commands executed or evaluated by the Tivoli Enterprise Monitoring Server. Disable by setting to "N".
CTIRA_REFLEX_TARGET	Default is "Y". For subnode targets only. Evaluate situation state by subnode name value in the ORIGINNODE column when deciding which reflex situation automation command the Tivoli Enterprise Monitoring Agent should execute. Not applicable to reflex situation commands executed or evaluated by the Tivoli Enterprise Monitoring Server. Disable by setting to "N".
CTIRA_SIT_CLEAN	Number of seconds between garbage clean up of stale entries in the agent persistent situation file. Default is 900 seconds.
CTIRA_SIT_FILE	Specify an alternate name for the default Tivoli Enterprise Monitoring Agent based persistent situation file. This should only be done in exceptional conditions since the file name reflects the agent's managed system name. Unsupported for z/OS based agents.
CTIRA_SIT_MGR	Specify whether or not to use the Tivoli Enterprise Monitoring Agent persistent situation file when registering with the Tivoli Enterprise Monitoring Server. Using this file improves Tivoli Enterprise Monitoring Server performance. Set to "N" to disable usage. For z/OS Tivoli Enterprise Monitoring Agent the value must be "N" since this feature not implemented for z/OS. For all other platforms, default is "Y".
CTIRA_SIT_PATH	Required variable specifying directory where the Tivoli Enterprise Monitoring Agent based agent persistent situation file is stored. This is the Tivoli Enterprise Monitoring Agent's only file, and it contains a copy of the Tivoli Enterprise Monitoring Server monitoring situations for Tivoli Enterprise Monitoring Agent use during Tivoli Enterprise Monitoring Server registration. The file is named `psit_`*`msn`*`.str`, where *msn* is the Managed System Name of the agent process. Unsupported for z/OS based agents.
CTIRA_STANDALONE	OBSOLETE – Should never be set. If it is specified, it MUST only be set to "N" or "n". Using any other value, including an empty string "", will cause the agent to fail to connect to a Tivoli Enterprise Monitoring Server.
CTIRA_SUBSYSTEM_ID	Optional variable to override the subsystem ID qualifier (subsystem:hostname:nodetype) of the agent managed system name (MSN). Describes a monitored resource instance to help make the MSN unique. Value can also be set by the Tivoli Enterprise Monitoring Agent API.
CTIRA_SYSTEM_NAME	Set alternate system name value for the agent entries in the Tivoli Enterprise Monitoring Server "ManagedSystem.Host Address" column within the "<NM>mysystem</NM>" tags. Used to build the Tivoli Enterprise Portal Server navigation tree. Not applicable to subnode type records in the Tivoli Enterprise Monitoring Server ManagedSystem table.
CTIRA_USE_HBTIMER	This variable should never be used! It will degrade agent heartbeat performance by NOT creating a separate heartbeat data thread.

Table 62. Tivoli Enterprise Monitoring Agent deploy environment variables (continued)

Variable	Purpose
DATACHUNKSIZE	Specifies the size of the data chunk that will be passed to RPC for transfer.
DEPLOYQUEUESIZE	Specifies the maximum number of requests that the request queue on the agent deployment controller.
DEPLOYTHREADPOOLSIZE	Specifies the number of threads that are available to the deployment controller.
DEPOTHOME	Specifies the root directory of the agent depot on the file system.
IRA_DUMP_DATA	Used by Tivoli Enterprise Monitoring Agent and Tivoli Enterprise Monitoring Server for debugging. Set to "Y" to do a hex dump of certain detailed data row contents into the RAS1 log. Default is "N". Can produce voluminous RAS1 message output if enabled.
IRA_EIF_ENABLE_LOG	Enables logging of EIF events sent for private situations directly from the Tivoli Enterprise Monitoring Agent to the agent's *.LG0 operational log if set to "Y".
ITM_BINARCH	Set by Tivoli Enterprise Monitoring Agent installer to supply the platform architecture code. Used by Tivoli Enterprise Monitoring Agent to read the agent installation version files and retrieve the agent version information.
KBB_NFS_TIMEOUT	Specifies the timeout value for NFS monitoring. The default is 2 seconds, and the allowed range is 1-30 seconds. The timeout occurs when a NFS file system is not reachable. The related data is shown as "Not collected" after the timeout is reached.

KBB_RAS1	• View state of main Tivoli Enterprise Monitoring Agent functions like situation and report processing:
	`ERR (UNIT:KRA ST)`
	• Detailed debug messages for Tivoli Enterprise Monitoring Agent functions:
	`ERR (UNIT:KRA ALL)`
	• View state of short-term history data uploads to Tivoli Data Warehouse:
	`ERR (UNIT:KHDX ST)`
	• Detailed debug messages of short-term history data uploads to Tivoli Data Warehouse:
	`ERR (UNIT:KHD ALL)`

KBB_SHOW_NFS=true | false	Specifies whether NFS monitoring is enabled. The default value is false on Linux and false on UNIX.
KHD_HISTRETENTION	Specifies the default retention period in hours for the short term history files (default is 24 hours). This can be used to reduce the amount of data kept on disk after a successful upload to the warehouse is performed.
TIMEOUT	Specifies the time in seconds that Agent Deployment tool has to complete a task. If the tool does not complete in the task in the time specified by the TIMEOUT value, the task is terminated. The default value is 600 seconds.

Appendix C. Support information

If you have a problem with your IBM software, you want to resolve it quickly. IBM provides the following ways for you to obtain the support you need:

Online
Go to the IBM Software Support site at http://www.ibm.com/software/support/probsub.html and follow the instructions.

IBM Support Assistant
The IBM Support Assistant (ISA) is a free local software serviceability workbench that helps you resolve questions and problems with IBM software products. The ISA provides quick access to support-related information and serviceability tools for problem determination. To install the ISA software, go to http://www.ibm.com/software/support/isa.

Searching knowledge bases

You can search the available knowledge bases to determine whether your problem was already encountered and is already documented.

Searching the information center

IBM provides extensive documentation that can be installed on your local computer or on an intranet server. You can use the search function of this information center to query conceptual information, instructions for completing tasks, and reference information.

Searching the Internet

If you cannot find an answer to your question in the information center, search the Internet for the latest, most complete information that might help you resolve your problem.

To search multiple Internet resources for your product, use the Web search topic in your information center. In the navigation frame, click Troubleshooting and support Searching knowledge bases and select Web search. From this topic, you can search a variety of resources, including the following:

- IBM technotes
- IBM downloads
- IBM Redbooks
- IBM developerWorks
- Forums and newsgroups
- Google

Obtaining fixes

A product fix might be available to resolve your problem. Obtain these fixes from the following site: http://www14.software.ibm.com/webapp/download/home.jsp.

Accessing terminology online

The IBM Terminology Web site consolidates the terminology from IBM product libraries in one convenient location. You can access the Terminology Web site at the following Web address:

http://www.ibm.com/software/globalization/terminology

Accessing publications online

IBM posts publications for this and all other Tivoli products, as they become available and whenever they are updated, to the Tivoli Documentation Central Web site at http://www.ibm.com/tivoli/documentation.

Note: If you print PDF documents on other than letter-sized paper, set the option in the **File → Print** window that allows Adobe Reader to print letter-sized pages on your local paper.

Ordering publications

You can order many Tivoli publications online at http://www.elink.ibmlink.ibm.com/publications/servlet/pbi.wss.

You can also order by telephone by calling one of these numbers:

- In the United States: 800-879-2755
- In Canada: 800-426-4968

In other countries, contact your software account representative to order Tivoli publications. To locate the telephone number of your local representative, perform the following steps:

1. Go to http://www.elink.ibmlink.ibm.com/publications/servlet/pbi.wss.
2. Select your country from the list and click **Go**.
3. Click **About this site** in the main panel to see an information page that includes the telephone number of your local representative.

Accessibility

Accessibility features help users with a physical disability, such as restricted mobility or limited vision, to use software products successfully. With this product, you can use assistive technologies to hear and navigate the interface. You can also use the keyboard instead of the mouse to operate all features of the graphical user interface.

Visit the IBM Accessibility Center at http://www.ibm.com/alphaworks/topics/accessibility/ for more information about IBM's commitment to accessibility.

Tivoli technical training

For Tivoli technical training information, refer to the following IBM Tivoli Education Web site at http://www.ibm.com/software/tivoli/education.

Tivoli user groups

Tivoli user groups are independent, user-run membership organizations that provide Tivoli users with information to assist them in the implementation of Tivoli Software solutions. Through these groups, members can share information and learn from the knowledge and experience of other Tivoli users. Tivoli user groups include the following members and groups:

- 23,000+ members
- 144+ groups

Access the link for the Tivoli Users Group at www.tivoli-ug.org.

Appendix D. Documentation library

This appendix contains information about the publications related to IBM Tivoli Monitoring and to the commonly shared components of Tivoli Management Services. These publications are listed in the following categories:

- IBM Tivoli Monitoring library
- Related publications

See *IBM Tivoli Monitoring and OMEGAMON XE Products: Documentation Guide*, SC23-8816, for information about accessing and using the publications. You can find the *Documentation Guide* in the IBM Tivoli Monitoring and OMEGAMON XE Information Center at http://publib.boulder.ibm.com/infocenter/tivihelp/v15r1/. To open the *Documentation Guide* in the information center, select **Using the publications** in the **Contents** pane.

To find a list of new and changed publications, click **What's new** on the Welcome page of the IBM Tivoli Monitoring and OMEGAMON XE Information Center. To find publications from the previous version of a product, click **Previous versions** under the name of the product in the **Contents** pane.

IBM Tivoli Monitoring library

The following publications provide information about IBM Tivoli Monitoring and about the commonly shared components of Tivoli Management Services:

- *Quick Start Guide*, GI11-8058

  Introduces the components of IBM Tivoli Monitoring.
- *Installation and Setup Guide*, GC32-9407

  Provides instructions for installing and configuring IBM Tivoli Monitoring components on Windows, Linux, and UNIX systems.
- *Program Directory for IBM Tivoli Management Services on z/OS*, GI11-4105

  Gives instructions for the SMP/E installation of the Tivoli Management Services components on z/OS.
- *Configuring the Tivoli Enterprise Monitoring Server on z/OS*, SC32-9463

  Gives detailed instructions for using the Configuration Tool to configure Tivoli Enterprise Monitoring Server on z/OS systems. Includes scenarios for using batch mode to replicate monitoring environments across the z/OS enterprise. Also provides instructions for setting up security and for adding application support to a Tivoli Enterprise Monitoring Server on z/OS.
- *Administrator's Guide*, SC32-9408

  Describes the support tasks and functions required for the Tivoli Enterprise Portal Server and clients, including Tivoli Enterprise Portal user administration.

- *High-Availability Guide for Distributed Systems*, SC23-9768

  Gives instructions for several methods of ensuring the availability of the IBM Tivoli Monitoring components.
- *Performance Analyzer User's Guide*, SC27-4004

  Explains how to use the Performance Analyzer to understand resource consumption trends, identify problems, resolve problems more quickly, and predict and avoid future problems.
- Tivoli Enterprise Portal online help

  Provides context-sensitive reference information about all features and customization options of the Tivoli Enterprise Portal. Also gives instructions for using and administering the Tivoli Enterprise Portal.
- *Tivoli Enterprise Portal User's Guide*, SC32-9409

  Complements the Tivoli Enterprise Portal online help. The guide provides hands-on lessons and detailed instructions for all Tivoli Enterprise Portal features.
- *Command Reference*, SC32-6045

  Provides detailed syntax and parameter information, as well as examples, for the commands you can use in IBM Tivoli Monitoring.
- *Troubleshooting Guide*, GC32-9458

  Provides information to help you troubleshoot problems with the software.
- *Messages*, SC23-7969

  Lists and explains messages generated by all IBM Tivoli Monitoring components and by z/OS-based Tivoli Management Services components (such as Tivoli Enterprise Monitoring Server on z/OS and TMS:Engine).
- *IBM Tivoli Universal Agent User's Guide*, SC32-9459

  Introduces you to the IBM Tivoli Universal Agent, an agent of IBM Tivoli Monitoring. The IBM Tivoli Universal Agent enables you to use the monitoring and automation capabilities of IBM Tivoli Monitoring to monitor any type of data you collect.
- *IBM Tivoli Universal Agent API and Command Programming Reference Guide*, SC32-9461

  Explains the procedures for implementing the IBM Tivoli Universal Agent APIs and provides descriptions, syntax, and return status codes for the API calls and command-line interface commands.
- *Agent Builder User's Guide*, SC32-1921

  Explains how to use the Agent Builder for creating monitoring agents and their installation packages, and for adding functions to existing agents.

Documentation for the base agents

If you purchased IBM Tivoli Monitoring as a product, you received a set of *base* monitoring agents as part of the product. If you purchased a monitoring agent product (for example, an OMEGAMON XE product) that includes the commonly shared components of Tivoli Management Services, you did not receive the base agents.

The following publications provide information about using the base agents.

- Operating system agents:
  - *Windows OS Agent User's Guide*, SC32-9445
  - *UNIX OS Agent User's Guide*, SC32-9446
  - *Linux OS Agent User's Guide*, SC32-9447
  - *i5/OS Agent User's Guide*, SC32-9448
  - *UNIX Log Agent User's Guide*, SC32-9471
- Agentless operating system monitors:
  - *Agentless Monitoring for Windows Operating Systems User's Guide*, SC23-9765
  - *Agentless Monitoring for AIX Operating Systems User's Guide*, SC23-9761
  - *Agentless Monitoring for HP-UX Operating Systems User's Guide*, SC23-9763
  - *Agentless Monitoring for Solaris Operating Systems User's Guide*, SC23-9764
  - *Agentless Monitoring for Linux Operating Systems User's Guide*, SC23-9762
- Warehouse agents:
  - *Warehouse Summarization and Pruning Agent User's Guide*, SC23-9767
  - *Warehouse Proxy Agent User's Guide*, SC23-9766
- System P agents:
  - *AIX Premium Agent User's Guide*, SA23-2237
  - *CEC Base Agent User's Guide*, SC23-5239
  - *HMC Base Agent User's Guide*, SA23-2239
  - *VIOS Premium Agent User's Guide*, SA23-2238
- Other base agents:
  - *Monitoring Agent for IBM Tivoli Monitoring 5.x Endpoint User's Guide*, SC32-9490

Related publications

You can find useful information about related products in the IBM Tivoli Monitoring and OMEGAMON XE Information Center at http://publib.boulder.ibm.com/infocenter/tivihelp/v15r1/.

Other sources of documentation

You can also obtain technical documentation about IBM Tivoli Monitoring and related products from the following sources:

- Tivoli Integrated Service Management Library

  http://www-01.ibm.com/software/brandcatalog/ismlibrary/

  The Tivoli Integrated Service Management Library is an online catalog that contains integration documentation and other downloadable product extensions.
- Redbooks

  http://www.redbooks.ibm.com/

  IBM Redbooks and Redpapers include information about products from platform and solution perspectives.

- Technotes

  Technotes provide the latest information about known product limitations and workarounds. You can find technotes through the IBM Software Support Web site at http://www.ibm.com/software/support.
- Tivoli wikis on the IBM developerWorks® Web site

  Tivoli Wiki Central at http://www.ibm.com/developerworks/wikis/display/tivoli/Home is the home for interactive wikis that offer best practices and scenarios for using Tivoli products. The wikis contain white papers contributed by IBM employees, and content created by customers and business partners.

  Two of these wikis are of particular relevance to IBM Tivoli Monitoring:

  – Tivoli Distributed Monitoring and Application Management Wiki at http://www.ibm.com/developerworks/wikis/display/tivolimonitoring/Home provides information about IBM Tivoli Monitoring and related distributed products, including IBM Tivoli Composite Application Management products.
  – Tivoli System z® Monitoring and Application Management Wiki at http://www.ibm.com/developerworks/wikis/display/tivoliomegamon/Home provides information about the OMEGAMON XE products, NetView for z/OS, Tivoli Monitoring Agent for z/TPF, and other System z monitoring and application management products.

Notices

This information was developed for products and services offered in the U.S.A. IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785 U.S.A.

For license inquiries regarding double-byte (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan, Ltd.
1623-14, Shimotsuruma, Yamato-shi
Kanagawa 242-8502 Japan

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law:

INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement might not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

IBM Corporation
2Z4A/101
11400 Burnet Road
Austin, TX 78758 U.S.A.

Such information may be available, subject to appropriate terms and conditions, including in some cases payment of a fee.

The licensed program described in this document and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement or any equivalent agreement between us.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurement may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

All statements regarding IBM's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

All IBM prices shown are IBM's suggested retail prices, are current and are subject to change without notice. Dealer prices may vary.

This information is for planning purposes only. The information herein is subject to change before the products described become available.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to

IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs. You may copy, modify, and distribute these sample programs in any form without payment to IBM for the purposes of developing, using, marketing, or distributing application programs conforming to IBM's application programming interfaces.

Each copy or any portion of these sample programs or any derivative work, must include a copyright notice as follows:

© (your company name) (year). Portions of this code are derived from IBM Corp. Sample Programs. © Copyright IBM Corp. _enter the year or years_. All rights reserved.

If you are viewing this information in softcopy form, the photographs and color illustrations might not be displayed.

Trademarks

IBM, the IBM logo, and ibm.com® 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 IBM trademarks is available on the Web at "Copyright and trademark information" at www.ibm.com/legal/copytrade.shtml.

Adobe, Acrobat, PostScript and all Adobe-based trademarks are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States, other countries, or both.

Cell Broadband Engine and Cell/B.E. are trademarks of Sony Computer Entertainment, Inc., in the United States, other countries, or both and is used under license therefrom.

Intel, Intel logo, Intel Inside, Intel Inside logo, Intel Centrino, Intel Centrino logo, Celeron, Intel Xeon, Intel SpeedStep, Itanium, and Pentium are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.

IT Infrastructure Library is a registered trademark of the Central Computer and Telecommunications Agency which is now part of the Office of Government Commerce.

ITIL is a registered trademark, and a registered community trademark of the Office of Government Commerce, and is registered in the U.S. Patent and Trademark Office.

Java and all Java-based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates.

Linux is a trademark of Linus Torvalds in the United States, other countries, or both.

Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation 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, and service names may be trademarks or service marks of others.

Index

Special characters

Numerics

A

B

C

D

E

F

G

H

I

J

K

L

M

N

O

P

Q

R

S

T

U

V

W

Z

Printed in USA

GC32-9458-04