IBM Tivoli Monitoring
Version 6.3 Fix Pack 2

Troubleshooting Guide

IBM

IBM Tivoli Monitoring

Version 6.3 Fix Pack 2

Troubleshooting Guide

IBM

Note

Before using this information and the product it supports, read the information in "Notices" on page 343.

This edition applies to version 6, release 3, fix pack 2 of IBM Tivoli Monitoring (product number 5724-C04) and to all subsequent releases and modifications until otherwise indicated in new editions.

Contents

Chapter 14. Command troubleshooting 251

Chapter 15. Performance Analyzer troubleshooting 269

Chapter 16. Database troubleshooting 277

Figures

Tables

About this information

This guide provides problem determination and resolution information for the issues most commonly encountered with IBM® Tivoli® Monitoring components and related products.

You can use this guide in conjunction with the other books for your product.

Chapter 1. Introduction to troubleshooting

To troubleshoot a problem, you typically start with a symptom or set of symptoms and trace back to the cause.

Troubleshooting is not the same as problem solving, although during the process of troubleshooting, you can obtain enough information to solve a problem, such as with end-user errors, application programming errors, and system programming errors.

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, "Logs and data collection for troubleshooting," on page 5 for information on the 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 "Trace logging" on page 37 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 Authorization Policy Server

- Tivoli Enterprise Monitoring Automation Server
- Tivoli Enterprise Monitoring Agent deployment
- Tivoli Data Warehouse
- Databases
- Command-Line Interface
- Event synchronization
- Infrastructure Management Dashboards for Servers
- Performance Analyzer
- Auditing facility
- Tivoli Common Reporting

Viewing the IBM Support Portal

The IBM Support Portal is a unified, customizable view of all technical support tools and information for your IBM systems, software, and services. It brings all the support resources available for IBM hardware and software offerings together in one place.

About this task

Perform the following actions to access technotes for this product:

Procedure

1. Open the http://ibm.com website and select **Support & downloads** > **Technical support**. You can also launch an IBM support website, such as http://www.ibm.com/support/us.
2. Enter your IBM user ID when prompted or, in the Quick start page or Support home, click **Sign in** to sign in with your IBM user ID or to register if you have not yet registered.
3. Enter a keyword or keywords for the information you want to find in the **Quick Find** or **Search support** fields. You can also browse through the other **Support** tabs.

Subscribing to IBM support notifications

You can subscribe to e-mail notification about product tips and newly published fixes through the Support portal.

In the Support portal, you can specify the products for which you want to receive notifications; choose from flashes, downloads, and technotes; and set up to receive email updates.

About this task

Perform the following actions to subscribe to Support emails.

Procedure

1. Open the http://ibm.com website and select **Support & downloads** > **Technical support**. You can also launch an IBM support website, such as http://www.ibm.com/support/us.
2. In the Quick start page or Support home, click **Sign in** to sign in or to register if you have not yet registered.

3. In the Notifications area of Support home, click **Manage all my subscriptions**.
4. In the **Subscribe** and **My defaults** tabs, select a product family and continue setting your preferences to specify the information you want in your emails.
5. If you have not yet added an email address to your profile, click **My IBM** > **Profile** > **Edit** and add it to your personal information.

Results

You begin receiving "IBM My notifications" emails about the products you have selected and at the interval you specified.

Starting Manage Tivoli Enterprise Monitoring Services

Manage Tivoli Enterprise Monitoring Services is a Tivoli Monitoring utility with a graphical user interface for starting, stopping, and configuring monitoring components on a Windows, Linux or UNIX computer. Many diagnostic and problem-solving tasks are done in Manage Tivoli Enterprise Monitoring Services.

About this task

Start Manage Tivoli Enterprise Monitoring Services using one of the following methods:

Procedure

- Windows Click **Start** > **Programs** > **IBM Tivoli Monitoring** > **Manage Tivoli Enterprise Monitoring Services**
- Linux UNIX Change to the `*install_dir*/bin` directory and run `./itmcmd manage [-h *install_dir*]` where -h *install_dir* is optional and used to specify the installation directory if it is not the one in which the script is located.

Results

Manage Tivoli Enterprise Monitoring Services is started and a list of the components that are installed on the computer is displayed.

Chapter 2. Logs and data collection for troubleshooting

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

Appropriate IBM Tivoli Monitoring RAS1 trace output

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 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.

The following links to sections in this document supply more information on these files:

- For information on where they are stored, see “Log file locations” on page 37
- For information on setting the trace option for an IBM Tivoli Monitoring component, see “Setting traces” on page 46.
- For information on dynamically setting the trace settings, see “Dynamically modify trace settings for a Tivoli Monitoring component” on page 61.
- For information on reading RAS1 logs, see “Reading RAS1 logs” on page 45.
- For information on the ras1log tool, see “ras1log tool” on page 69.

Running snapcore to collect information

Use the **snapcore** command for collecting information for use in identifying and resolving problems with an application.

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.

About this task

Take the following steps to run the **snapcore** command and collect information you might need to debug and analyze the problem:

Procedure

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 the/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, run the **uncompress** 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.
```

Locating the core file

You can read the core file for information related to system stops on UNIX-based systems. Use the **errpt -a** command to get a summary of the most recent system stoppages and the location of the core file.

If the system stops on UNIX-based systems, collect the core file from the directory that stores the binary file, to which the process belongs. For example, if the failing process is the Tivoli Enterprise Portal Server server process, KfwServices, the core is created in the /opt/IBM/ITM/archtype/cq/bin/ directory.

Procedure

To retrieve information on where the core file is created, enter the **errpt -a** command.

Results

A summary of information is displayed 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/aix533/cq/bin/core
PROGRAM NAME
KfwServices
STACK EXECUTION DISABLED
---------------
```

Getting Dr. Watson dumps and logs

Use the Dr. Watson debugger to get the information needed by IBM Support to diagnose problems on Windows systems.

If you encounter errors or failures on your Windows system, collect the `drwtsn32.log` and `user.dmp` files if they are available. The `drwtsn32.log` and `user.dmp` files are located in: `\Documents and Settings\All Users\Documents\DrWatson`.

About this task

Take the following steps to enable Dr. Watson and configure it to create a detailed dump file:

Procedure

1. To enable Dr. Watson as the default debugger, at the command prompt, enter the following command: **`drwtsn32 –i.`**
2. To open the Dr. Watson configuration dialog, at the command prompt, enter the following command: **`drwtsn32`**
3. Set the following fields:
   a. Set the *Crash dump Type* to FULL.
   b. Clear the **Dump Symbol Table** check box.
   c. Enable the **Dump all Thread Contexts** check box.
   d. Enable the **Create Crash Dump File** check box.

K*pc*CMA.RAS files

IBM Tivoli Monitoring on Windows systems has (where *pc* is the two-character product or component code) `K`*`pc`*`CMA.RAS` files in the `c:\windows\system32` directory to collect information about monitoring process failures.

For example, `KNTCMA.RAS` is the Monitoring Agent for Windows OS the reliability, availability, and serviceability file. These files contain system dump information similar to the `drWatson.log`, but are generated by the IBM Tivoli Monitoring infrastructure.

Monitoring agent LG0 log

Review and agent's LG0 file in the logs directory for log entries relating to connection to the Tivoli Enterprise Monitoring Server, the situations that are started and stopped, and other events while the agent is running.

Log file location

Windows *install_dir*\TMAITM6\logs

Linux UNIX *install_dir*/logs

LG1 backup

A new version of LG0 file is generated every time the agent is restarted, and one backup copy of the file is kept with extension LG1. View the LG1 file to learn the following details regarding the previous monitoring session:

- Status of connectivity with the monitoring server
- Situations that were running
- The success or failure status of Take Action commands

Note:

1. If *instance_name:host_name.domain_name* is greater than 32 characters, the characters beyond that number are truncated from the domain name.
2. Messages related to the self-describing agent show the status code with no description if the message was from a later version of IBM Tivoli Monitoring than the agent version. For example, you run the **tacmd addsdainstalloptions** command on your V6.2.3 monitoring agent but it does not succeed and you review the LG0 file for that agent. The log file has an entry with SDA status code 1024, which was introduced in V6.3.0. What shows as the message description, `0x400`, should be `SDA Install Blocked`.

```
Self-Describing Agent Register/Install failed with STATUS (1024/0x400)
for PRODUCT "NT", with TEMS "TVT6048:CMS", VERSION_INFO "product_vrmf=06230100;
tms_package_vrmf=06230100;tps_package_vrmf=06230100;tpw_package_vrmf=06230100;".
```

Sources of other important information

You can collect important information from log files, such as trace or message logs that report system failures. Also, application information provides details on the application that is being monitored, and you can obtain information from messages or information on screen.

The following sources provide additional information to aid in troubleshooting:

- 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 screen captures or a description of what you observed, if applicable.
- Log files collected 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.

- Information about the application that you are monitoring, such as DB2 or SAP. This information includes the version number, 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 and the patch level, if available.
  - Monitoring Agent version number .
  - Tivoli Enterprise Portal (Select **Help** > **About Tivoli Enterprise Portal)**

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

Chapter 3. Common problem solving

Customers using IBM Tivoli Monitoring products or the components of Tivoli Management Services can encounter problems such as missing workspaces or historical data, or a reflex automation script that does not run when it should. In many cases you can recover from these problems by following a few steps.

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

You can access several troubleshooting tools, such as the Log analyzer or pdcollect tool to help you troubleshoot your IBM Tivoli Monitoring product or the components of Tivoli Management Services.

ITMSuper Tools

The ITMSUPER Tools give you information about the health of your managed systems, situations, and environment configuration. You can find the tools by searching for "ITMSUPER" in the IBM Integrated Service Management Library (http://www.ibm.com/software/brandcatalog/ismlibrary).

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 68.

IBM Support Assistant

The IBM Support Assistant is a free, stand-alone application that you can install on any workstation. Then, you can enhance the application by installing product-specific plug-in modules for the IBM products you use. For more information see "Support information" on page 339.

I am trying to find out what software is supported

Use resources in the *IBM Tivoli Monitoring Installation and Setup Guide* and the IBM website to determine the software that is supported. This enables you to find platform or database information for specific products.

The following resources are available to determine the software that is supported:

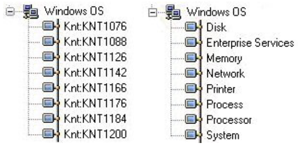
- For specific information about the supported software for IBM Tivoli Monitoring, see "Hardware and software requirements" in the *IBM Tivoli Monitoring Installation and Setup Guide*
- For platform and database support information for most Tivoli products, consult the matrix at Tivoli Supported Platforms (http://www-306.ibm.com/software/sysmgmt/products/support/Tivoli_Supported_Platforms.html)

Workspaces are missing or views are empty

You can encounter a problem that Tivoli Enterprise Portal workspaces are missing or views are empty. For example, you may have workspaces that return no data.

Symptoms of the problem:

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



- You receive message `KFWITM217E: Request error: SQL1_CreateRequest failed, rc=209`. See "Resolving application support problems" on page 13.
- You receive message `KFWITM220E: Request failed during execution.`See "Resolving monitoring agent problems" on page 16.

For more information on workspaces that relate to historical data, see "Historical data is missing or incorrect" on page 21.

To diagnose the problem that workspaces are missing or empty, see "Diagnosing that workspaces are missing or empty."

Diagnosing that workspaces are missing or empty

You can diagnose that workspaces are missing or empty by verifying that the monitoring agent has been started and that the configuration is correct.

You can also check that application support has been added.

About this task

To diagnose that workspaces are missing or empty, perform the following steps:

Procedure

Preliminary diagnostics

1. Refresh the Navigator by clicking **View** > **Refresh**.
2. Verify that the monitoring agent has been started. Restart if necessary. In the Tivoli Enterprise Portal, right-click the Navigator item of the monitoring agent and click Start or Restart
3. Verify that the monitoring agent configuration is correct.
4. If your data is missing in an Oracle Agent workspace, see "Resolving Oracle DB Agent problems - diagnostic actions" on page 34. Similar problems might exist for other monitoring agents.
5. Check that application support has been added. See "Resolving application support problems" on page 13.

What to do next

For more information on actions that relate to these diagnostics, see the problem resolution tasks.

Resolving application support problems

Application support problems are caused by a lack of application support or an application support level mismatch among the components: monitoring server, portal server, desktop and clients, and monitoring agents. Check the installed level of application support or run the ITMSUPER Tivoli Enterprise Monitoring Server analysis tool (or both) to get more information.

Before you begin

Complete one or both of the following tasks to ensure that this is an application support problem:

- "Diagnosing that workspaces are missing or empty" on page 12
- "Diagnosing that a situation does not raise when expected" on page 27

About this task

To resolve application support problems, you perform diagnostic and corrective actions. These actions include checking application support on the servers and client and running the Tivoli Enterprise Monitoring Server tool to ensure that application support is installed consistently in your environment.

Procedure

Diagnostic and corrective actions

1. Check application support on the monitoring server, portal server, and portal client:
   - Windows Run the **`kincinfo.exe -i`** command in the `%CANDLE_HOME\InstallITM` directory to show what is installed.
   - UNIX Run the **`./cinfo –i`** command in the `$CANDLEHOME/bin` directory to show what is installed.
   - z/OS (monitoring server) 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 `KppCAT`and `KppATR` where `pp` is the two-character product or component code.
2. You can also run the Tivoli Enterprise Monitoring Server 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.
4. If the desktop client or client is being used, ensure application support is installed on the portal client.

What to do next

For more information and instructions on installing application support see "Configuring application support for nonbase monitoring agents" in the *IBM Tivoli Monitoring Installation and Setup Guide*. For instructions on installing application support on a z/OS monitoring server, see "Adding application support to a monitoring server on z/OS" in *Configuring the Tivoli Enterprise Monitoring Server on z/OS*.

Resolving monitoring server problems

Monitoring server problems are caused by a monitoring server that is not started or connectivity that is lost either between servers or between servers and agents. You can restart the Tivoli Enterprise Monitoring Server, and you can also run the ITMSUPER Topology tool to get more information.

About this task

To resolve monitoring server problems, you perform diagnostic and corrective actions. These actions include running tools, such as the Topology or Connectivity tool and correcting communication failures in logs.

Procedure

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
   - Tivoli Enterprise Monitoring Server analysis tool
   - Tivoli Enterprise Portal Server
3. Check the portal server logs for messages indicating communication failures to the monitoring server.
4. Check the monitoring server logs for messages indicating communication failures to the remote monitoring servers or to monitoring agents.
5. Correct the communication failures indicated in the logs.

Resolving monitoring agent problems

If the monitoring agent is running but data is not being returned or if you receive an error message from an agent log, such as `Endpoint unresponsive`, verify that the agent is connected and online. You can also verify that application support has been installed correctly.

About this task

To resolve monitoring agent problems, you perform diagnostic and corrective actions. These actions include verifying that the agent is running and that application support has been installed correctly. For information on monitoring agents on see each product's *Problem Determination Guide*.

Procedure

Diagnostic and corrective actions

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 that `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 that `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

You can encounter a problem that the status of a monitoring agent is mismatched between the Tivoli Enterprise Portal client and **`tacmd`** command. For example, a monitoring agent shows as online in the portal client and offline in the results of a **`tacmd`** command.

Diagnosing that the status of a monitoring agent is mismatched between the portal client and tacmd command

You can diagnose that the status of a monitoring agent is mismatched between the Tivoli Enterprise Portal and tacmd command by setting a trace to determine whether the problem is in the Tivoli Enterprise Portal Server or the Tivoli Enterprise Monitoring Server.

About this task

To diagnose that the status of a monitoring agent is mismatched between the portal client and tacmd command, perform the following steps:

Procedure

Preliminary diagnostics

1. Verify the state of the monitoring agent in .
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 "Resolving monitoring agent problems" on page 16.
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)./`
4. 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
   - 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 Software Support.

What to do next

For more information on actions that relate to these diagnostics, see the problem resolution tasks.

Resolving monitoring agent problems

Monitoring agent problems, such as a monitoring agent that has not started can be resolved by refreshing the Navigator status in the .

About this task

To resolve monitoring agent problems, you perform diagnostic and corrective actions. These actions include checking the status of the monitoring agent and the monitoring server.

Procedure

Diagnostic and corrective actions

1. Open the Managed System Status workspace and click **View** > **Refresh**.
2. Make sure the monitoring agent is connected to the correct monitoring server.
3. Check the status of the monitoring server that the monitoring agent is connected to. For more information, see the monitoring server problem resolution task.

Resolving monitoring server problems

Tivoli Enterprise Monitoring Server problems, such as loss of connectivity between a monitoring agent and a remote monitoring server can be resolved by checking, for example, that the remote monitoring server is connected to the hub monitoring server.

Some causes of monitoring server problems:

- A 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 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.
  ```

About this task

To resolve monitoring server problems, you perform diagnostic and corrective actions. These actions include running tools, such as the ITMSUPER tools and correcting connectivity failures.

Procedure

Diagnostic and corrective actions

1. Check the 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
   - Tivoli Enterprise Monitoring Server analysis tool
5. Correct the connectivity failures identified.

The portal server does not start or stops responding

You can encounter a problem that the does not start or stops responding. For example, you may receive a message that communication with the portal server could not be established or the portal server is not ready.

Symptoms of the problem

- Portal client logon fails. "Diagnosing that portal server 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 Portal Server could not be established`.
- You find a similar text string to `KFWDBVER, version not found when trying to start the portal server`. See "Resolving database problems - missing table or portal server database" on page 18.

Diagnosing that the portal server does not start or stops responding

You can diagnose that the does not start or stops responding by running the Analysis ITMSUPER tool.

About this task

To diagnose that the portal server does not start or stops responding, perform the following steps:

Procedure

Preliminary diagnostics

1. For more information about any messages received, see the *IBM Tivoli Monitoring Messages* (http://pic.dhe.ibm.com/infocenter/tivihelp/v61r1/topic/com.ibm.itm.doc_6.3fp2/ic/landing_messages.htm) reference guide. 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 running?
   - Yes: See step 4.
   - No: See "Resolving database problems - instance not started" on page 19.
4. Collect the portal server log or the operations log and look for the following text strings:

- KFWDBVER, version not found
- TEPS database not found
- user ID or password invalid
- DB2 instance not started

5. Run the Analysis ITMSUPER tool.

What to do next

For more information on actions that relate to these diagnostics, see the problem resolution tasks.

Resolving database problems - missing table or portal server database

Database problems caused by a missing table or Tivoli Enterprise Portal Server database, or by a mismatch between the portal server version and the version record in the database, can be resolved by reconfiguring the portal server.

About this task

To resolve database problems, you perform diagnostic and corrective actions. These actions include reconfiguring the portal server.

Procedure

Diagnostic and corrective actions

1. Windows To reconfigure the portal server, open , right-click the portal server, and select **Reconfigure**. If the problem persists, run one of the following commands and set the correct password in the window that is displayed:
   - For an SQL database, **cnpsdatasource.exe**
   - For a database, **db2datasource.exe**
2. Linux UNIX To reconfigure the portal server, take one of the following steps:
   - On the GUI interface, open right-click the portal server, and select **Reconfigure**.
   - On the command-line interface, run the **./itmcmd config -A cq** command.
3. Run the **buildpresentation** script.

Resolving database problems - user ID and password

Database problems caused by a password that does not match the operating system password or an incorrect password in the registry can be resolved by reconfiguring the Tivoli Enterprise Portal Server and verifying the user ID and password.

The causes of database problems include:

- Portal server database user password is out of sync.
- User ID does not match the operating system logon user ID.
- Password does not match the operating system password.
- Registry does not have the correct password.

About this task

To resolve database problems, you perform diagnostic and corrective actions. These actions include reconfiguring the portal server and ensuring that your portal client user ID is the same as the logon user ID of your system.

Procedure

Diagnostic and corrective actions

- Windows To reconfigure the portal server, run the `tacmd configureportalserver` command. If the problem persists, take one or more of the following steps:
  - Ensure that your portal client user ID is identical to the logon user ID of your system and use the correct capitalization for your user ID and password. If you need to change your password, take the following steps:
    1. Right-click **My Computer** and select **Manage**.
    2. Select **Local Users and Groups**.
    3. Select **Users**.
    4. Right-click your user ID and select **Properties**.
    5. For , set the password to never expire.
  - Check the UDB database and ensure that the user ID and password match those of the local account:
    1. Click **Control Panel** > **Administrative Tools** > **Services**.
    2. Right-click **DB2 - DB2** and select **Properties**.
    3. Select the **Log On** tab and ensure that the db2admin user ID and password match the db2admin UDB account.
  - Check the user ID and password for the database and data source:
    1. Click **Control Panel** > **Administrative Tools** > **Data Sources (ODBC)**.
    2. On the **System DSN** tab, select **TEPS2** and click **Configure**.
    3. Enter your user ID and password. For example: `db2admin` for database and `CNPS` for data source.
    4. To test the connection to the UDB database, click **Connect**.
  - On the **Advanced Settings** tab, verify that the DATABASE name is correct.
- Linux UNIX To reconfigure the portal server, take one of the following steps:
  - On the GUI interface, open right-click the portal server, and select **Reconfigure**.
  - On the command-line interface, run the **`./itmcmd config -A cq`** command.

Resolving database problems - instance not started

Database problems such as a instance that is not started can be resolved by recycling the Tivoli Enterprise Portal Server to resolve problems and ensuring that the user ID and password are correct.

About this task

To resolve database problems, you perform diagnostic and corrective actions. These actions include ensuring that the user ID and password are correct.

Procedure

1. Check the status of the instance in the Control Panel.
2. Recycle the portal server and resolve any issues reported.

3. Ensure that the user ID and password are correct.

Diagnosing that portal server logon fails

Logging on to the Tivoli Enterprise Portal Server fails when a user ID is locked, disabled, or an internal error occurs during logon. Examine the portal server or portal client logs for more information.

The logon failure might cause one or more of the following messages to display:

- `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.`

About this task

To diagnose that the portal server logon fails, perform the following steps:

Procedure

Preliminary diagnostics

1. For a guide to the messages and operator responses, refer to *IBM Tivoli Monitoring Messages* (http://pic.dhe.ibm.com/infocenter/tivihelp/v61r1/topic/com.ibm.itm.doc_6.3fp2/ic/landing_messages.htm).
2. Look in the portal server or portal client logs for more information concerning the message.

The portal client does not respond

You can encounter a problem that the Tivoli Enterprise Portal does not respond or stops running.

Diagnosing that the portal client does not respond

You can diagnose that the does not respond by verifying that a Tivoli Enterprise Monitoring Server is started or the selected workspace is returning data.

About this task

To diagnose that the does not respond, perform the following steps:

Procedure

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 , check the Task Manager and in the `%CANDLE_HOME\InstallITM` directory, run the following **`kincinfo.exe`** commands:
   - **`kincinfo.exe -r`** to show running processes.

- **kincinfo.exe -i** to show what is installed.

4. On or , in the `$CANDLEHOME/bin` directory, run the following **cinfo** commands:
   - **./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 "High CPU usage on a distributed system" on page 31. 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

What to do next

For more information on actions that relate to these diagnostics, see the problem resolution tasks.

Resolving storage or memory problems

Storage or memory problems are caused by a problem that leads to a lack of storage or memory. To resolve storage or memory problems, you perform diagnostic and corrective actions. These actions include reconfiguring the Control Panel.

Procedure

Reconfigure the Control Panel. See "Performance tuning > Tivoli Enterprise Portal client" in the *IBM Tivoli Monitoring Installation and Setup Guide* for more information.

Resolving client configuration problems

To resolve Tivoli Enterprise Portal configuration problems, disable the DirectDraw to reduce high CPU usage due to the Java process attempting to write to the screen.

Procedure

Disable DirectDraw by setting the `sun.java2d.noddraw` client variable to `false`. See the "Tivoli Enterprise Portal client configuration settings" topics in the *IBM Tivoli Monitoring Administrator's Guide*.

Historical data is missing or incorrect

You can encounter a problem that historical data is missing or incorrect. For example, you can have a workspace that is missing historical data.

Symptoms of the problem:

- 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.

Diagnosing that historical data is missing or incorrect

You can diagnose that historical data is missing or incorrect by using workspaces such as the Self-Monitoring Topology workspace to verify component activity. Also, you can use the **tacmd** commands to verify the configuration of historical data.

About this task

To diagnose that historical data is missing or incorrect, perform the following steps:

Procedure

Preliminary diagnostics

1. To verify component connectivity through the Self-Monitoring Topology workspace, perform the following steps:
   a. In the Navigator Physical view, click the **Enterprise** item.
   b. Select **Workspace** > **Self-Monitoring Topology**.

   Alternatively, review the Tivoli Data Warehouse workspaces for the Warehouse Proxy agent and Summarization and Pruning agent.
2. Verify the historical data collection configuration in 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**

What to do next

For more information on actions that relate to these diagnostics, see the problem resolution tasks. See also the troubleshooting topics in the *IBM Tivoli Warehouse Proxy Agent Installation and Configuration Guide* (http://pic.dhe.ibm.com/infocenter/tivihelp/v61r1/topic/com.ibm.itm.doc_6.3fp2/wpa/wpagent_user.htm) and *IBM Tivoli Warehouse Summarization and Pruning Agent Installation and Configuration Guide* (http://pic.dhe.ibm.com/infocenter/tivihelp/v61r1/topic/com.ibm.itm.doc_6.3fp2/spa/spagent_user.htm).

Resolving warehouse proxy connection problems

Tivoli Data Warehouse proxy agent connection problems can be resolved by verifying that the correct socket connection is being used.

The causes of problems might be because the short-term historical data is being stored at the monitoring agent or the Tivoli Enterprise Monitoring Server and should be switched, or because the cannot connect to the data warehouse or to the monitoring server.

About this task

To resolve warehouse proxy connection problems, you perform diagnostic and corrective actions. These actions include verifying that the monitoring agent is connected to the Tivoli Data Warehouse and that the connection from the agent to the Tivoli Enterprise Monitoring Server is not being prevented by a firewall.

Procedure

Diagnostic and corrective actions

1. Ensure that the is running.
2. Look for export failures to the in either the monitoring agent RAS1 log or the monitoring server RAS1 log. Depending on where the error is found, see the monitoring agent steps or monitoring server steps below.
   - Monitoring agent:
     a. Verify that the correct socket connection is being used.
     b. Verify that the monitoring agent is connected to the Tivoli Data Warehouse.
   - Monitoring server:
     a. Verify that the connection between the monitoring server and is not being stopped by a firewall.
     b. Verify that the correct port is being used for each component.
3. For corrective actions, perform the following steps:
   - Monitoring agent:
     – Store the collected data at the location of the monitoring server to ensure a stable connection.
   - Monitoring server:
     – Consider using a high port number for connecting to the monitoring server. See the “Controlling port number assignments” topics in the *IBM Tivoli Monitoring Installation and Setup Guide* for more information on the COUNT and SKIP options for port number allocation.

Resolving warehouse proxy agent problems - configuration

If the is connected to the Tivoli Data Warehouse and Tivoli Enterprise Monitoring Server but cannot transmit data, change the environment variable settings in the `Warehouse` configuration file.

About this task

To resolve problems, you perform diagnostic and corrective actions. These actions include modifying the environment variable settings in the `Warehouse` configuration file.

Procedure

Diagnostic and corrective actions

1. To perform a diagnostic action, review the current **`CTIRA_NCSLISTEN`** and **`KHD_QUEUE_LENGTH`** settings in the `Warehouse` configuration file.
2. To perform a corrective action, set **`CTIRA_NCSLISTEN`** equal to at least 20 times the value of **`KHD_EXPORT_THREADS`** and increase **`KHD_QUEUE_LENGTH`** equal to a value greater than the number of agents being handled by that .

Resolving warehouse proxy agent problems - connectivity

problems, such as the inability to send data to the , can be resolved by ensuring that agent can export data and that it is not too busy.

About this task

To resolve warehouse proxy agent problems, you perform diagnostic and corrective actions. These actions include verifying that the warehouse database password and user ID are correct. Also, you can update the configuration parameters.

Procedure

Diagnostic and corrective actions

1. To perform diagnostic actions:
   a. 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**.
   b. Verify that the warehouse database password and user ID are correct and have not expired.
   c. Look at the RAS1 logs for export resource availability timeout. The might be unable to export because it is too busy.
2. To perform a corrective action:
   - Update the configuration parameters. See “Environment variables” in the *IBM Tivoli Monitoring Installation and Setup Guide*.

Resolving summarization and pruning agent problems

Summarization and pruning agent problems, such as unexpected values for attributes can be resolved by reviewing the documentation for the monitoring agents that are producing the unexpected values.

The causes of monitoring server problems include: Summarization and Pruning agent yield unexpected values; unanticipated attribute behavior leads to unexpected data.

About this task

To resolve summarization and pruning agent problems, you perform diagnostic and corrective actions. These actions include comparing real-time data from a workspace view with the unexpected data.

Procedure

1. To perform a diagnostic action:
   - Open a workspace view that shows real-time data and compare it with the unexpected data.
   - To understand how data is aggregated for various data types, see *Tivoli Management Services Warehouse and Reporting* (http://www.redbooks.ibm.com/abstracts/sg247290.html). This IBM Redbooks publication describes aggregation methods used by the Summarization and Pruning Agent.
2. To perform a corrective action:

- Review the documentation for the monitoring agents that are generating the unexpected values. This clarifies the expected types of values for the attributes in question.

Resolving persistent data store for z/OS problems

If you encounter a problem with the configuration of the persistent data store on the Tivoli Enterprise Monitoring Server, you can check the RKPDLOG output to verify the configuration.

About this task

To resolve persistent data store for problems, you perform diagnostic and corrective actions. These actions include verifying that the data store is configured properly.

Procedure

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 historical data is configured to be collected at the monitoring server, see step 2 below.
   - If historical data is configured to be collected at the agent, see step 3 below.
2. To verify that the persistent data store is configured correctly, on the monitoring server, check the RKPDLOG output, 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.
     ```
3. To verify that the persistent data store is configured correctly at the agent, check the RKPDLOG of the agent, for example:
   - If KM5AGENT (this agent runs on 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 (time stamp not shown):
     ```
     Response: &philev.RMQSGRP3    1700      83   14  5000 Active   Write
     Response: &philev.RMQSGRP2    1700      25    0  5000 Empty    Read Access
     Response: &philev.RMQSGRP1    1700      25    0  5000 Empty    Read Access
     Response: &philev.RKMQPDS3   23327      31    0  4000 Empty    Read Access
     Response: &philev.RKMQPDS2   23327    6598  143  4000 Partial  Read Access
     Response: &philev.RKMQPDS1   23327    3523  105  4000 Active   Write
     ```
4. Verify that the files are not being used by another task.
5. Verify that the files are initialized correctly and that the K*pp*PDICT is inserted into the persistent data store files.

6. Verify that the maintenance procedure is correctly processing the persistent data store files.

Example

Examples of the error codes 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 a 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 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 : 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.

What to do next

For more information about the persistent data store, see the *IBM Tivoli OMEGAMON XE and Tivoli Management Services on z/OS: Common Planning and Configuration Guide* (http://pic.dhe.ibm.com/infocenter/tivihelp/v61r1/topic/com.ibm.omegamon_share.doc_6.3.0.1/zcommonconfig/zcommonconfig.htm).

Historical data does not get collected at the z/OS-based agent

When you configure Historical Data Collection for a z/OS-based monitoring agent, the short-term history for the agent framework attribute groups cannot be stored at the agent. This includes such attribute groups as the Agent Operations Log and ITM Audit.

Symptom

The following error message is visible in the z/OS agent RAS1 log (RKLVLOG) when this problem occurs (time stamp not shown):

```
(0034-D8CDE7B3:kraahbin.cpp,977,"ConnectToPDS") Unable to locate table
 KRAAUDIT
(0034-D8CDE7B3:kraahbin.cpp,977,"ConnectToPDS") Unable to locate table OPLOG
```

Solution

When historical collection data is required from any z/OS monitoring agent for the agent framework attribute groups (CCC Logs - Agent Operations Log, CCC Logs - ITM Audit, for example), configure Historical Data Collection for short-term data storage at the Tivoli Enterprise Monitoring Server rather than at the agent.

A situation does not raise when expected

You can encounter a problem that a situation does not raise. For example, certain conditions may not raise a situation as expected.

Symptoms of the problem:

- In the portal client or , certain conditions exist that should have raised a situation but the situation has not been raised.

Diagnosing that a situation does not raise when expected

You can diagnose that a situation does not open an event when expected by verifying that the monitoring agent has started.

About this task

To diagnose that a situation does not raise when expected, perform the following steps:

Procedure

Preliminary diagnostics

1. Verify that the monitoring agent has started.
2. Verify that the situation is associated with a Navigator item in the Tivoli Enterprise Portal.
3. In the situation event console, confirm that the situation is true and an event has opened.
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 any workspace that should contain the data to verify that data is arriving.
6. To provide more information, run the following ITMSUPER tools:
   - Situation Test tool
   - Exceptions Analysis tool
   - Distributions Analysis tool

What to do next

For more information on actions that relate to these diagnostics, see the following tasks:

Related tasks:

"Resolving situation-specific problems"

Resolving situation-specific problems

To resolve situation-specific problems, check the log files (such as the agent operations log) to verify that the situation was started; check that the agent returned data and that the SITMON received the data; and check that the situation opened an event.

About this task

To resolve situation-specific problems, you perform diagnostic and corrective actions. These actions include checking if the agent is online and if the agent returned data. Then, you check that the SITMON received the data.

Procedure

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: `1061110125731000KRAIRA000 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.`
2. Did the situation start?
   - No: See step 3.
   - Yes: See step 5.
3. Is the situation distributed to the agent and is the agent online?
   - Look for a text string similar to the following text string in the monitoring server log:

   ```
   KO41047 Situation CheckIfSituationCreated distribution Primary:KATE:NT
   added
   ```
   - Yes: See step 5.
   - No: Use (**UNIT**:kpxreqds all) to trace the distribution at the monitoring server for a situation.

   ```
   (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
```

4. 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
     ```
   - If Yes: See step 6.
   - If No: Is the situation authored correctly? At the agent, trace (**UNIT**:kdsfilt all).

   a. 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 monitoring agent.

   b. No: See step 5.
5. 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

   a. Attribute file is incorrect (wrong version) or missing and the RULE could not be created.

   b. A value of *1133* or *1203* leads to a value of *1131*.

   c. 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
   ```
6. Did SITMON receive the data?
   - Monitoring server trace (**UNIT**:ko4async *ERROR STATE FLOW*) (**UNIT**:ko4tobje ALL) (**UNIT**:ko4sitma ALL)
   - If Yes and SITMON receives the data: Does the situation apply to the Enterprise? For example:

   ```
   11/08/06 16:18:49 KO46256 Situation definition CheckIfSituationCreated
   created by *ENTERPRISE
   ```
   - This displays *ENTERPRISE in the MSG2 message of the monitoring server message log when the situation was created. 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 shown in the following monitoring server log examples:
  a. Enterprise situation `KO41046 Monitoring for enterprise situation MS_Offline started.`
  b. Non-Enterprise situation `KO41036 Monitoring for situation Weekday started.`
- If Yes and it is a Non-Enterprise situation: See step 7.
- If No and it is not an Enterprise situation: Reconfigure the situation to include the Enterprise flag setting.
- If No and SITMON does not receive the data: 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.

7. Is there a MSG2 message indicating the situation raised?
   - Yes: Contact Software Support. See Chapter 2, “Logs and data collection for troubleshooting,” on page 5 for information on what types of data to collect before contacting Support. Also consult the IBM Support Portal (http://www.ibm.com/support/entry/portal/software).

A reflex automation script does not run when it should

You can encounter a problem that a reflex automation script does not run when it should. For example, after a situation raised, a particular action might not occur.

Diagnosing that a reflex automation script does not run when it should

You can diagnose that a reflex automation script does not run when it should by checking if the situation raised.

Procedure

Preliminary diagnostics

If the situation does not raise, see “Diagnosing that a situation does not raise when expected” on page 27.

What to do next

For more information on actions that relate to these diagnostics, see the problem resolution task.

Resolving format and variable problems

To resolve format and variable problems, you verify that the system command is correct and that it can be executed on a specific platform. You can check the monitoring agent operations log to see if reflex automation occurred.

Procedure

Diagnostic and corrective actions

1. Does the system command run correctly from a command line?
   - Yes: Go to the next step.

- No: Verify that the command you typed in is correct.

2. Is the length of the command within the limit for your operating system?
   - Yes: Go 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 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 which error occurred.
5. Correct the identified problem.

High CPU usage on a distributed system

You can encounter a problem that CPU usage is high on a distributed system.

Symptoms of the problem:

- 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 “Resolving Oracle DB Agent problems - corrective actions” on page 34.
- Situations alert you frequently about a managed system cycling between online and offline. See “Resolving firewall problems - corrective actions” on page 33.

Diagnosing high CPU usage on a distributed system

You can diagnose that CPU usage is high on a distributed system by determining whether a monitoring component, application, or process running on the system might be the cause of the problem. Also, you can use the ITMSUPER tools, such as the Connectivity tool to provide more information.

About this task

To diagnose that CPU usage is high on a distributed system, perform the following steps:

Procedure

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.
2. Windows Use the tools and data provided by 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 OS agent.
3. Linux UNIX Use the **`top`** command to display processes using high CPU. For , you can also use the **`ps auxww`** command.
4. Verify the following:

- Is historical data collection enabled?
- Is the database undergoing a backup?

5. Windows Is the situation writing a lot of event logs?
   - Yes: Disable all event log monitoring situations.
6. Select each of the workspaces in turn, to see which one is consuming high CPU.
7. Running the following ITMSUPER tools might also provide more information:
   - Stressed Resources tool
   - Connectivity tool
   - Situations tool
8. 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. The agent might not be able to establish connectivity with the monitoring server. High CPU usage can result from the agent's frequent attempts to connect.
   a. 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.
   b. Make the changes in the associated agent `*ENV` configuration file for , or the `*.ini` configuration file for or .

What to do next

For more information on actions that relate to these diagnostics, see the problem resolution tasks.

Resolving situation problems - diagnostic actions

You can resolve situation problems by running the ITMSUPER tool. Also, you can examine the situation definition and formula in the agent-specific `.lg0` file.

Procedure

Diagnostic actions

1. Run the Situation Test ITMSUPER tool.
2. Find out which situations have been deployed to the monitoring agent.
3. Open the agent-specific`.lg0` file to view a list of situations started for that agent.
   - Windows `*install_dir*\TMAITM6\logs`
   - Linux UNIX `*install_dir*/logs`
4. Examine the situation definition and formula.
5. Does the situation contain any wildcard `*` characters against UTF8 columns?
   - Yes: See "Resolving situation problems - corrective actions."
6. Switch between situations to see which one is causing the high CPU.

Resolving situation problems - corrective actions

You can resolve situation problems by either changing the formulation of situations or rewriting the situation using the `SCAN strcscan` function. You can also use non-UTF8 columns to rewrite the situation or combine predicates with an OR.

Procedure

Corrective actions

1. Change the formulation of any situations that are causing excessive processing.
2. For situations with wildcard * characters, perform one of the following steps:
   - 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"`.
   - 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.
   - 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' ) )`.

Resolving firewall problems - diagnostic actions

A problem with firewall interference or a problem with communication between the Tivoli Enterprise Monitoring Server and monitoring agents can be resolved by using the **ping** command to verify the communication between the server and agents.

Procedure

Diagnostic actions

1. Check connectivity between the monitoring agent and the monitoring server.
2. 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.
3. 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 46 for more information.

Resolving firewall problems - corrective actions

You can resolve firewall problems by contacting Software Support.

Procedure

1. If you still have high CPU usage issues even after ensuring proper connectivity across firewalls, open a problem report with Software Support or refer to the IBM Support Portal (http://www.ibm.com/support/entry/portal/software).
2. For more information, see the "Firewalls" topics in the *IBM Tivoli Monitoring Installation and Setup Guide*.

Resolving Oracle DB Agent problems - diagnostic actions

Oracle DB Agent problems, such as a cursor performance problem can be resolved by setting an environment variable to disable problematic cursors.

Procedure

Diagnostic actions

1. Collect the detail traces of collector and RAS1 log. See the problem determination topics for enabling detailed tracing in the collector trace log and setting RAS trace parameters 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.
3. You can identify the SQL query that caused the high CPU usage issue from or the Oracle tools. Use the following procedure to identify the problematic cursors from :
   a. 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.`
   b. The default timeout value of ITM 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`
   c. 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*
```

4. The previous cursor (DB6) took about 2 minutes and 11 seconds to return data causing the performance problem.
5. Were you able to identify an SQL query?
   - Yes: Continue to the corrective actions task.

Resolving Oracle DB Agent problems - corrective actions

Oracle DB agent problems, such as problematic cursors can be resolved by setting environment variables and overriding variable settings.

Procedure

Corrective actions

1. Disable the problematic cursors by setting an environment variable:
   - Windows **`COLL_DISABLE_CURSORS`**
     a. Launch .
     b. Right-click the row that contains the name of the monitoring agent whose environment variables you want to set.
     c. From the pop-up menu, select **Advanced** > **Edit Variables**.
     d. If the agent is running, accept the prompt to stop the agent.

e. The list dialog box is displayed. When only the default settings are in effect, variables are not displayed. The variables are listed after you override them. Override the variable settings:
   1) Click **Add**.
   2) From the **Variable** menu, select **`COLL_DISABLE_CURSORS`**. If the variable is not there, you can add it.
   3) In the **Value** field, type a value and click **OK** twice.
   4) Restart the agent.

- Linux UNIX **`db_extparms`**

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

  b. 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`.

  c. 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 to recognize these changes to the **Extended Parameters** value.
3. 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:
   - Windows *`install_dir`*`\TMAITM6`
   - Linux UNIX `$CANDLEHOME/misc`

   When these cursors are enabled, the displays default attribute values of these cursors in the Tivoli Enterprise Portal, meaning, the no longer monitors the attributes of the enabled cursors.
4. 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
```

5. For more information on the cursors, see 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 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. IBM Software Support uses the information captured by trace logs to trace a problem to its source or to determine why an error occurred.

Trace logs are commonly referred to as *RAS1* logs because RAS1 is the name of the IBM Tivoli Monitoring component that manages trace logging. Furthermore, the two tracing-related environment variables are **KBB_RAS1**, which sets a product's tracing level, and **KBB_RAS1_LOG**, which assigns the name, size, count, and directory location of RAS1 log files.

By default, RAS1 logs on distributed systems are stored in the /logs directory under the installation path for IBM Tivoli Monitoring. On z/OS, the RAS1 log is stored as a SYSOUT file associated with the RKLVLOG DDNAME.

When an IBM Tivoli Monitoring product is installed and configured, RAS1 tracing for the product is configured by default to specify ERROR-level logging, which means only the most important run-time messages are traced. There are different methods for customizing the logging level, along with the size, count, and location of log files.

Log file locations

Log files are saved in log and component directories in your IBM Tivoli Monitoring installation.

The mechanism for managing log files is the KBB_RAS1_LOG environment variable.

KBB_RAS1_LOG environment variable

The KBB_RAS1_LOG environment variable specifies the full path name of a product's log file, the full path name of the inventory control file, and several options for controlling logging behavior.

Unless instructed to do so by IBM Software Support, you should not normally modify the KBB_RAS1_LOG default values because of the risk that critical logging information could be lost.

The KBB_RAS1_LOG has the following format:

KBB_RAS1_LOG=filename [setting=value]

[COUNT=*count*]
Maximum number of log files to create in one invocation of the product. The default count is 5. Each log file created in a product invocation gets assigned a

count, starting at 01, that is stored in the log file name. Whenever a log file fills and a new log is created, the count gets incremented by 1, up to the limit defined in the count parameter. The new log sequence number is stored as an *nn* value in the log file name, for example, the `03` in `systema_ms_4f2b12eb-03.log`.

[INVENTORY=*inventory_filename***]**
A file, with a `.inv` extension on distributed platforms, which automatically records the history of log files across the most recent invocations of the product. By default, the inventory control file is located in the *install_dir*/logs directory. The name of the file includes the local system name and the two-character product code, for example, WINSYS1_cq.inv or AIXPROD_ux.inv. If you cannot find RAS1 logs that you are searching for, you should examine the product's inventory control file and review the names and locations of the log files listed there.

[LIMIT=*limit***]**
Maximum size per log file. The default size is 8 megabytes.

[MAXFILES=*maxfiles***]**
The total number of log files in a product's inventory that will be saved. Note that saved log files can span across multiple product invocations, provided that the maxfiles limit has not yet been reached. Extra log files beyond the maxfiles value are automatically deleted. There must be a valid inventory control file in order for the maxfiles value to be enforced.

[PRESERVE=*preserve***]**
The number of log files to preserve when log files exceed the count. The default is 1. This means that if, for example, the log file count is 5 and all 5 logs are filled while the product is running, the 6th log will overwrite the -02.log, the 7th log will overwrite the -03 log, and so forth. But the -01 log will be preserved, which is important because it contains a product's startup messages and valuable configuration information. Unless instructed to do so by IBM Software Support, you should not normally modify the KBB_RAS1_LOG default values because of the risk that critical logging information could be lost.

Log file naming

RAS1 log files are maintained with the following naming, as determined by the KBB_RAS1_LOG environment variable in the product's configuration file:

- Windows RAS1 logs are stored in the `\logs` directory under the installation path for IBM Tivoli Monitoring. The following is an example of a log file name that includes the local system name, the two-character product code of the Tivoli Enterprise Portal Server, the time stamp in hexadecimal format when the process started, and the log sequence number:

  ```
  ibm-kpmn803v01_cq_472649ef-02.log
  ```

- Linux UNIX On UNIX-based systems, RAS1 logs are stored in the `/logs` directory under the installation path for IBM Tivoli Monitoring. The following example of a log file name includes the local system name, the two-character product code of the UNIX OS Monitoring Agent, the agent's “stat_daemon” child process name, the time stamp in hexadecimal format when the process started, and the log sequence number:

  ```
  f50pa2b_ux_stat_daemon_49ac1eee-01.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.

Log file path

Here are the location of the trace log files that are associated with the use of the following components. The default paths for *install_dir* are `C:\Program Files\IBM` on Windows and `/opt/ibm/` on Linux of UNIX.

Tivoli Enterprise Portal Server

Windows *`install_dir`*`\logs`

Linux UNIX *`install_dir`*`/logs/` *`hostname_CQ_timestamp`*`.log`

where:

`install_dir` specifies the directory where the portal server was installed.

`hostname` specifies the name of the system hosting the product.

`CQ` is the component code for the portal server.

`timestamp` is a decimal representation of the time when the process was started.

Tivoli Enterprise Portal browser client and Java™ Web Start

Location of trace log files that are associated with the use of the Tivoli Enterprise Portal when the client is deployed within a browser or as a Java Web Start application:

Windows The log location depends somewhat on the version of Windows being used. Here are the two most common locations:
`%USERPROFILE%``\AppData\LocalLow\IBM\Java\Deployment\log`
`%USERPROFILE%``\Application Data\IBM\Java\Deployment\log`

Linux `$`*`{user.home}`*`/.java/deployment/log`

For the browser client, the file name is `plugin`*`nnnnn`*`.trace`. For Java Web Start, the file name is `javaws`*`nnnnn`*`.trace`.

where *nnnnn* is a unique, randomly generated numeric suffix to support generational logs.

Tivoli Enterprise Portal desktop client

Windows *`install_dir`*`\cnp\logs\kcjerror`*`_n`*`.log`
`install_dir``\cnp\logs\kcjras1.log`
`install_dir``\cnp\kcj.log`

Linux *`install_dir`*`/logs/`*`hostname_CJ_timestamp`*`.log`

where:

`install_dir` specifies the directory where the portal client was installed.

`_n` represents the circular sequence in which logs are rotated. The logs range from no *_n* for the current log file, to 1 through 9 for the previous logs. A new `kcjerror.log` file is generated each time the desktop client is started, at which time the previous log is renamed `kcjerror_1.log`. If there was a `kcjerror_1.log`, that one gets renamed to `kcjerror_2.log`, and so on until 9 is reached and the logs start over with `kcjerror_1.log`.

`hostname` specifies the name of the system hosting the product.

`CJ` is the component code for the portal client.

`timestamp` is a decimal representation of the time when the process was started.

You can configure for multiple named instances of the desktop client. This is typically done, for example, when you want to have multiple desktop client instances connecting to different portal server environments. When you use the “Create instance” action from either the Windows Manage Tivoli Enterprise Monitoring Services utility or the Linux CandleManage panel associated with the desktop client, you are prompted to provide a name for the new instance. The default instance has no name. All the log file names for the desktop client include the instance name, so the file naming conventions for the 3 logs are as follows: kcj*instance_name*.log, kcjerror*instance_name*.log, and kcjras1*instance_name*.log. For Linux, the kcj*instance_name*.log file actually uses the standard Linux log filename convention of *hostname_CJ_timestamp*.log.

Tivoli Enterprise Monitoring Server

Windows *install_dir*\logs\*hostnameMS_ HEXtimestamp-nn*.log

Linux UNIX *install_dir*/logs/*hostname_MS_timestamp*.log

where:

install_dir specifies the directory where the monitoring server was installed.

hostname specifies the name of the system hosting the monitoring server.

MS is the component code for the monitoring server.

HEXtimestamp is a hexadecimal representation of the time when the process was started.

nn represents the circular sequence in which logs are rotated. The logs range from 1 to 5, by default, although the first is always retained because it includes configuration parameters.

Dashboard Application Services Hub

Windows C:\Program Files\IBM\JazzSM\profile\logs\server1\SystemOut.log

Linux UNIX /opt/ibm/JazzSM/profile/logs/server1/SystemOut.log

tivcmd Command-Line Interface for Authorization Policy

Windows C:\IBM\TivoliMonitoring\logs\kdqras1_51229cb8-01.log

Linux UNIX /opt/IBM/TivoliMonitoring/logs/kdqras1_51229cb8-01.log

Audit logs for the Authorization Policy Server

Windows C:\Program Files\IBM\JazzSM\AuthPolicyServer\PolicyServer\audit\hostname_2013.02.18_16.04.38.458.w7_audit.log

Linux UNIX /opt/IBM/JazzSM/AuthPolicyServer/PolicyServer/audit/*hostname_2013.02.18_16.04.38.458.w7*_audit.log

where:

hostname is the name of the computer where the Authorization Policy Server is installed.

2013.02.18_16.04.38.458.w7 is the log time stamp.

Automation Server

Windows *install_dir*\logs\kasmain.msg

Linux UNIX *install_dir*/logs/*hostname*_AS_*HEXtimestamp*.log

where:

hostname is the name of the computer where the automation server is installed.

AS is the component code for the Automation Server.

HEXtimestamp is the log time stamp in hexadecimal.

Monitoring agents

Windows *install_dir*\tmaitm6\logs\ *hostname_PC_HEXtimestamp-nn*.log

Linux UNIX *install_dir*/logs/*hostname_PC_timestamp*.log

where:

install_dir specifies the directory where the monitoring agent was installed.

hostname specifies the name of the system hosting the monitoring agent.

PC specifies the product code, for example, NT for Windows OS.

HEXtimestamp is a hexadecimal representation of the time when the process was started.

nn represents the circular sequence in which logs are rotated. The logs range from 1 to 5, by default, although the first is always retained because it includes configuration parameters.

IBM Tivoli Warehouse Proxy agent

Windows *install_dir*\logs*hostname_HD_ timestamp*.log

Linux UNIX *install_dir*/logs/*hostname_PC_ timestamp*.log

where:

install_dir specifies the directory where the monitoring agent was installed.

hostname specifies the name of the system hosting the Warehouse Proxy agent.

HD is the product code for the IBM Tivoli Warehouse Proxy agent.

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.

Windows *install_dir*\logs*hostname_SY_ HEXtimestamp-nn*.log
install_dir\logs\hos tname_SY_ ras1java_HEXtimestamp-nn.log
install_dir\logs\hostname_PC_ java_HEXtimestamp-nn.log

Linux UNIX *install_dir*/logs/*hostname_SY_ HEXtimestamp-nn*.log
install_dir/logs/*hostname_SY_ras1java_ HEXtimestamp-nn*.log
install_dir/logs/*hostname_SY_java_ HEXtimestamp-nn*.log

where:

install_dir specifies the directory where the monitoring agent was installed.

hostname specifies the name of the system hosting the monitoring agent.

SY specifies the product code for the Summarization and Pruning agent.

HEXtimestamp is a hexadecimal representation of the time when the process was started.

nn represents the circular sequence in which logs are rotated. The logs range from 1 to 5, by default, although the first is always retained because it includes configuration parameters.

Installation log files

Use the log files that are created during installation to help diagnose any errors or operational issues.

The following table lists and describes the log files created when installing when installing a Tivoli Enterprise Monitoring Server, Tivoli Enterprise Portal Server, Tivoli Enterprise Portal client, and Tivoli Enterprise Monitoring Agent:

Table 1. 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 installation 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

Obtain details about the installation (or upgrade) process in the logging and tracing information. You can set the trace levels.

You can set the degree of logging and tracing to one of three 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

Obtain details about the installation (or upgrade) process in the logging and tracing information. You can set the trace levels.

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. See "pdcollect tool" on page 68.

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

upgrade 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.

Table 2. Upgrading from Tivoli log file

Windows	UNIX-based systems
$DBDIR/AMX/logs/log_tool_ timestamp.log	$DBDIR/AMX/logs/log_tool_ timestamp.log

where:

$DBDIR
The 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 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

RAS1 logs are primarily a diagnostic tool for IBM Software Support. However, the logs can also be read by administrators to gain an understanding of the major events in the life of an IBM Tivoli Monitoring process.

Even with default ERROR-level logging, you can find information in RAS1 logs about product configuration, security settings, network interfaces, listening ports, key milestones during startup and shutdown, run-time errors, user logins, commands issued, etc.

At the top of a product's first RAS1 log, with -01 in the log file name, there is a banner section containing details about the general operating environment. Here is a sample banner section from a Windows OS agent log:

```
!4F68BA8C.0000!=================>  IBM Tivoli RAS1 Service Log  <===================
+4F68BA8C.0000      System Name: ITMSYSZ                   Process ID: 7132
+4F68BA8C.0000     Program Name: kntcma                     User Name: SYSTEM
+4F68BA8C.0000        Task Name: kntcma                   System Type: WinXP;5.1-SP3
+4F68BA8C.0000   MAC1_ENV Macro: 0xC112                    Start Date: 2012/03/20
+4F68BA8C.0000       Start Time: 10:12:44                   CPU Count: 1
+4F68BA8C.0000        Page Size: 4K                       Phys Memory: 2039M
+4F68BA8C.0000      Virt Memory: 2048M                     Page Space: 3935M
+4F68BA8C.0000    Service Point: system.itmsysz_nt     UTC Start Time: 4f68ba8c
+4F68BA8C.0000         ITM Home: C:\IBM\ITM               ITM Process: itmsysz_nt
+4F68BA8C.0000  Executable Name: C:\IBM\ITM\TMAITM6\kntcma.exe
+4F68BA8C.0000         KBB_RAS1: ERROR
+4F68BA8C.0000     KBB_RAS1_LOG: C:\IBM\ITM\TMAITM6\logs\ITMSYSZ_NT_4f68ba8c-.log
                    INVENTORY=C:\IBM\ITM\TMAITM6\logs\ITMSYSZ_nt_kntcma.inv
                      COUNT=05 LIMIT=8 PRESERVE=1 MAXFILES=10
+4F68BA8C.0000      KBB_ENVPATH: C:\IBM\ITM\TMAITM6\KNTENV
+4F68BA8C.0000 =====================================================================
```

As you can see, the values of the two RAS1 environment variables, KBB_RAS1 and KBB_RAS1_LOG, are echoed in the banner section. You can find the Process ID of this invocation of the product, as well as statistics about available memory and CPUs. On UNIX-based systems, you also see Stack Limit, Core Limit, and the maximum number of file descriptors in the `NoFile Limit` field. The UTC Start Time is the hexadecimal representation of the product's start time, which gets included in the log file name.

After the banner section in the first RAS1 log, are messages concerning major events during product startup. Although RAS1 logs are often analyzed for evidence of problems and errors, the logs also contain key messages indicating the health of a product, such as its initialization status. For example, here is an excerpt from a Tivoli Enterprise Portal Server's first RAS1 log:

```
("CTServer::startServerDll") KFW1002I Starting Service: 'CEV v1.0'
("JVMProxyServer::start") id of object to deploy is 'CTCEV'.
("BSS1_GetEnv") KFW_CEV_TEST_CONFIG="N"
("CTServer::startServerDll") KFW1003I Started Service: 'CEV v1.0'
("CTServer::startServerDll") KFW1002I Starting Service: 'MCSAttribute v1.0'
("JVMProxyServer::start") id of object to deploy is 'CTMCSAttribute'.
("BSS1_GetEnv") KFW_MCS_XML_FILES="c:\ibm\itm\cnps\teclib"
("CTServer::startServerDll") KFW1003I Started Service: 'MCSAttribute v1.0'
("CTServer::startServerDll") KFW1002I Starting Service: 'Startup  Complete v2.0'
("CTServer::startServerDll") KFW1003I Started Service: 'Startup Complete v2.0'
("CTServer::runORB") KFW1020I ****** Waiting for requests. Startup complete ******
("BSS1_GetEnv") TEPS_SDA="Y"
```

The “Waiting for requests...”" trace message signifies that the portal server is ready to accept users logging in, which is an important milestone in the portal server startup. RAS1 logs also echo the value of each product environment variable. As shown in the excerpt, the Self-Describing Agent (SDA) feature is enabled in the portal server.

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 RAS1 log for the product encountering the error.

The RAS1 log is an essential part of the trace diagnostic tools in Tivoli Monitoring.

By default, the RAS1 tool is set to only log errors and other critical messages. However, you can configure RAS1 to log more detailed product information, as instructed by IBM Software Support. If you are modifying a product's configuration file to change RAS1 logging levels, be sure to first back up the configuration file.

RAS1 syntax

Follow the RAS1 syntax for setting traces in your environment file.

```
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 (such as KHL for OMEGAMON® z/OS® Management Console).

RAS1 supports partial matches on a compilation unit name, which can help reduce the number of UNIT parameters that you need to specify. For example, in the Tivoli Enterprise Monitoring Server, all Self-Describing Agent (SDA) functions reside in compilation units whose names begin with “kfasd”. Therefore, you can specify (`UNIT:kfasd ALL`) in the **`KBB_RAS1`** environment variable for the monitoring server, and it provides a concise way to capture detailed RAS1 tracing of all SDA functions.

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.

Usage notes

Avoid configuring RAS1 tracing with excessive **`UNIT`** parameters or a predominant use of the **`ALL`** filter. Otherwise, RAS1 tracing might be suspended or the Tivoli Monitoring process becomes unresponsive during product runtime or shutdown. Such behavior can be caused by a setting of KBB_RAS1=ALL, for example, because it results in intensive filtering. This limitation can be circumvented by using more restrictive filters (ERROR or STATE) or fewer UNIT keywords. The i5 OS monitoring agent process is particularly sensitive to overload (see the workaround in “Setting the trace option for the i5/OS agent” on page 54.)

As a rule, syntax checking of RAS1 tracing filters is lenient, for the following reasons:

- The RAS1 grammar is flexible, which makes it difficult to determine what the coder really intended and whether a coding error has occurred.
- A Tivoli Monitoring process should not fail to start because of a RAS1 syntax problem, thus every effort is made to revert to defaults to allow the process to keep running with a valid RAS1 setting in effect, even if KBB_RAS1 was specified incorrectly.

Because of the lenient syntax checking, it is not always obvious if there's a typographical error or other mistake in a RAS1 filter. This issue applies whether **`KBB_RAS1`** was configured in an environment file before process startup, or if it was dynamically modified using one of the methods, such as **`tacmd settrace`**, that are described in other Tools topics (see also "Dynamically modify trace settings for a Tivoli Monitoring component" on page 61). In the **`unit_name`** example above, if you inadvertently specified (**`UNIT:kfasdALL`**) without a blank between "kfasd" and "ALL", the RAS1 syntax checker interprets it to mean that the filter applies to compilation units whose names begin with "kfasdALL". Because no class value is present in (**`UNIT:xyzALL`**), a default class of NONE is used for those compilation units. When **`KBB_RAS1`** changes are implemented, it is important to carefully check what was specified to ensure it matches what was intended.

Setting the trace option for the portal client trace

A log file is created automatically the first time you start the Tivoli Enterprise Portal, and is named differently depending on whether you are launch the client through your browser, Java Web Start, or as a desktop application.

This log file contains all of the RAS1 tracing for the 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 the portal client again. The `kcj.log` file contains errors generated by the Java™ libraries used in the portal client.

Procedure

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 portal server trace

Set the trace options for the Tivoli Enterprise Portal Server through Manage Tivoli Enterprise Monitoring Services.

Before you set the trace options for the portal server, determine the trace string. The trace string specifies the trace setting. Set trace options for the portal server when you start it. The log file continues to grow until you either turn off the trace or recycle the portal server. Always backup the files before altering them.

Procedure

- Windows On the computer where the portal server is installed, click **Start** > **Programs** > **IBM Tivoli Monitoring** > **Manage Tivoli Enterprise Monitoring Services**.
  1. Right-click the Tivoli Enterprise Portal Server service.
  2. Select **Advanced** > **Edit Trace Parms to display the Trace Parameters window**.
  3. Select the RAS1 filters. The default setting is ERROR.
  4. Accept the defaults for the rest of the fields and click **OK**.
- Linux UNIX Set the following variable in the *install_dir*/config/cq.ini where `filter` is the component you want to trace and `trace_level` is the level of tracing you want.

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

What to do next

Recycle the Tivoli Enterprise Portal Server.

Setting the trace option for the monitoring server

Set the trace option for the Tivoli Enterprise Monitoring Server in Manage Tivoli Enterprise Monitoring Services or the environment file.

Before you begin

Back up the environment file before editing it.

Procedure

- Windows:
  1. On the computer where the Tivoli Enterprise Monitoring Server is installed, select **Start** > **Programs** > **IBM Tivoli Monitoring** > **Manage Tivoli Enterprise Monitoring Services**.
  2. Right-click the Tivoli Enterprise Monitoring Server service and select **Advanced** > **Edit Trace Parms to display the Trace Parameters window**.
  3. Select the RAS1 filters, adding a space between each UNIT trace setting, such as `ERROR (UNIT:kdy all) (UNIT:kfaprpst all)`. RAS1 is the unit trace for the monitoring server. 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.
- Linux and UNIX:
  1. Change to the *install_dir*/config directory.
  2. Open the `ms.ini` file in a text editor.
  3. Set the following variable, adding a space between each UNIT trace setting, such as `KBB_RAS1=ERROR (UNIT:KDY ALL) (UNIT:KFAPRPST ALL)`:

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

where *filter* is the component to trace and *trace_level* is the level of tracing. The following example traces everything in the Deploy component: `KBB_RAS1=ERROR (UNIT:KDY ALL)`

4. To trace the monitoring server command line interface, set the following variable in *install_dir*/bin/tacmd.
5. Regenerate the *hostname*_ms_*tems_name*.config file by running the `./itmcmd config -S [ -h` *install_dir* `] [ -a` *arch* `] -t` *tems_name* command. (For more information in the itmcmd commands, see the *IBM Tivoli Monitoring Command Reference* (http://pic.dhe.ibm.com/infocenter/tivihelp/v61r1/topic/com.ibm.itm.doc_6.3fp2/ic/landing_cmdref.htm).)
6. Recycle the monitoring server. The command syntax for starting and stopping the monitoring server is `./itmcmd server [ -h` *install_dir* `] [-l] [-n] start|stop` *tems_name*.

What to do next

For information on how to set trace levels dynamically, see "Dynamically modify trace settings for a Tivoli Monitoring component" on page 61.

Setting the trace option for the automation server

The Tivoli Enterprise Monitoring Automation Server diagnostic facility is controlled with the KAS_DEBUG and **KAS_DEBUG_MAXLOGS** environment variables. You can set specific levels of tracing in the automation server environment file.

Before you begin

The Tivoli Enterprise Monitoring Automation Server supports two types of diagnostic facilities to assist in debugging problems. The first is the standard ITM RAS1 trace facility, for tracing the C++ source modules within the automation server. The second diagnostic facility, for tracing the automation server script files, is controlled by the **KAS_DEBUG** and **KAS_DEBUG_MAXLOGS** environment variables.

Due to the performance impact of enabling diagnostic tracing, do not enable RAS1 or KAS_DEBUG tracing unless instructed to do so by IBM Support.

KAS_DEBUG

The KAS_DEBUG facility writes its trace messages directly to the existing automation server RAS1 log file. The following list shows the increasing granularity of trace message levels that are supported for KAS_DEBUG.

`I` - for Inhibit (NONE)

`N` - for Normal (default value for Error tracing)

`P` - for Performance

`Y` - for Yes (the same as S)

`S` - for State

`V` - for Verbose

`T` - for Trace (the same as internal FLOW tracing)

`D` - for Detail

`M` - for Maximum

`A` - for ALL (turn on all available levels)

Each **KAS_DEBUG** trace level that you set displays messages for the specified trace level, plus all lower trace levels. For example, setting **KAS_DEBUG=P** displays debug trace messages for **P** (Performance) and **N** (Error); and setting **KAS_DEBUG=V** displays debug trace messages for **V** (Verbose) plus **S** (State), **P** (Performance), and **N** (Error).

KAS_DEBUG_MAXLOGS

The **KAS_DEBUG_MAXLOGS** variable is used to create two log files that capture additional debug messages:

resources.txt captures a snapshot of the Registry Services entries

itmevents.log captures each table event from the following Tivoli Enterprise Monitoring Server attribute groups: Managed System Status (inodests table) and Situation Status Log (tsitstsh table).

The log files are created in the automation server runtime directory:

Windows *install_dir*\CAS

Linux UNIX *install_dir*/as

Set KAS_DEBUG_MAXLOGS=Y before starting the server. After the automation server is started, the two log files are created and continue to grow until the server is stopped or recycled. Be sure to set the variable back to KAS_DEBUG_MAXLOGS=N and delete the resources.txt and itmevents.log files after you are done using this variable. Note that KAS_DEBUG_MAXLOGS must be set in the automation server environment file; you cannot change it dynamically.

About this task

Complete these steps to set the automation server trace option in the kas environment file:

Procedure

1. Stop the automation server.
2. Edit the environment file:
   - Windows
     a. Click **Start** > **Programs** > **IBM Tivoli Monitoring** > **Manage Tivoli Enterprise Monitoring Services**.
     b. Right-click the Tivoli Enterprise Monitoring Automation Server and select **Advanced** > **Edit Variables**.
     c. Click **Add** and enter KAS_DEBUG for the variable name and one of the trace levels for the value, such as Y or D (for the list of trace levels, see KAS_DEBUG).
     d. If you also want to create two log files that capture additional debug messages, click **Add** and enter KAS_DEBUG_MAXLOGS for the variable name and Y for the value.
     e. Click **OK** to save your changes.
   - Linux UNIX
     a. Change to the *install_dir*/config directory.
     b. Open the as.ini file in a text editor, and add the following line to the end of the file: KAS_DEBUG=*N*, where *N* is the trace level you want to specify, such as S or V (for the list of trace levels, see KAS_DEBUG).
     c. If you also want to create two log files that capture additional debug messages, add the following line to the end of the file: KAS_DEBUG_MAXLOGS=Y.
     d. Save and close the environment file.
3. Restart the automation server for the changes to take effect.

Results

After you restart the automation server, the trace level is changed and you can see the following message in the log file, where *ERROR* is the trace level:

```
INFO: KAS DEBUG set to [ERROR]
```

What to do next

If you set a high trace level, repeat the procedure to return the level to the normal setting after you are done with diagnostic tracing.

If you also set **KAS_DEBUG_MAXLOGS**, the two log files are created and continue to grow until the server is stopped or recycled. Set the value back to **KAS_DEBUG_MAXLOGS=N** and delete the `resources.txt` and `itmevents.log` files after you are done using this variable.

Setting the trace option for the automation server dynamically

You can set specific levels of Tivoli Enterprise Monitoring Automation Server tracing dynamically from your web browser.

Before you begin

The Tivoli Enterprise Monitoring Automation Server diagnostic facility is controlled by the following environment variables:

KAS_DEBUG

KAS_DEBUG_MAXLOGS (cannot be changed dynamically)

KBB_RAS1

KBB_RAS1_MAXLOGS (cannot be changed dynamically)

For a description, see the prolog of "Setting the trace option for the automation server" on page 50.

Due to the performance impact of enabling diagnostic tracing, do not enable **KAS_DEBUG** tracing unless instructed to do so by IBM Support.

To set the **KBB_RAS1** trace dynamically for the automation server using the Service Console interface, see the instructions in "Dynamically modify trace settings for a Tivoli Monitoring component" on page 61. The port to reach the Service Console interface for the automation server is the HTTP or HTTPS port configured in the automation server connection information. For information about the port HTTP or HTTPS port used by the automation server, see "Installing and configuring the Tivoli Enterprise Monitoring Automation Server" in the *IBM Tivoli Monitoring Installation and Setup Guide*. In the Service Console, use the IBM Tivoli Monitoring Service Console link for setting the trace.

About this task

Complete the following steps to set the automation server trace level from your browser:

Procedure

Enter the following URL in your browser:

```
protocol://host:port/kas_srv/provider?kas_debug=level
```

where
protocol is the http or https protocol used by the automation server.
host is the name of the computer where the automation server is installed.
port is the port number used by the automation server for incoming requests (default for http is 10001).
level is the KAS_DEBUG trace level to use, such as `Detail` or `D`:

I - for Inhibit (NONE)

N - for Normal (default value for Error tracing)

P - for Performance

Y - for Yes (the same as S)

S - for State

V - for Verbose

T - for Trace (the same as internal FLOW tracing)

D - for Detail

M - for Maximum

A - for ALL (turn on all available levels)

Results

After the new trace level is accepted by the automation server, a message is displayed in the browser confirming the trace level; an equivalent message appears in the RAS log. Example web browser message:

```
INFO: KAS DEBUG set to [ERROR]
```

Example RAS log message:

```
(508AD6EF.0000-A80:kascontr.cpp,5245,"autoTEMSWriteRAS")
INFO: KAS DEBUG set to [ERROR]"
```

What to do next

If you set a high trace level, repeat the procedure to return the level to the normal setting after you are done with diagnostic tracing.

Setting the trace option for the Agent Deploy tool

About this task

On Windows systems:

1. On the computer where the Tivoli Enterprise Monitoring Server is installed, select **Start** > **Programs** > **IBM Tivoli Monitoring** > **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 i5/OS agent

The i5/OS monitoring agent can become unresponsive or tracing can be suspended if KBB_RAS1 is configured with excessive **UNIT** parameters or the **ALL** filter.

Configure RAS1 tracing on the i5/OS monitoring agent appropriately to ensure adequate performance.

About this task

Configure the KBB_RAS1 variable in the i5/OS monitoring agent environment file with one of the following settings to set RAS1 tracing:

Procedure

- **KBB_RAS1=NONE**
  1. Set **KBB_RAS1=NONE** in QAUTOTMP/KMSPARM(KBBENV) for the i5/OS agent.
  2. Recycle the agent.

  This setting produces a limited RAS1 log and the agent ends gracefully during shutdown.
- **KBB_RAS1=ERROR**
  1. Set **KBB_RAS1=ERROR** in QAUTOTMP/KMSPARM(KBBENV) for the i5/OS agent.
  2. Comment out the following two lines by adding an asterisk (*) at the beginning of each line:

     ```
     KBB_RAS1_LOG=(QAUTOTMP/KA4AGENT01 QAUTOTMP/KA4AGENT02
     QAUTOTMP/KA4AGENT03)
     INVENTORY=QAUTOTMP/KA4RAS.INV LIMIT=5 PRESERVE=1
     ```
     Commenting out the lines removes them from processing and a spool file is created under the QAUTOMON user with trace data, which can be discarded unless requested by IBM Support.
  3. Save the environment file and recycle the agent.
  4. To verify that the agent is ending normally, use **ENDOMA** or select **Option 3** on **GO OMA** and accept the default options.

  Note that it is possible for the spool file to become full based on the agent trace configuration settings.

Setting the trace option for the Warehouse Proxy agent

Procedure

1. On Windows systems, on the computer where the Tivoli Enterprise Monitoring Server is installed, select **Start** > **Programs** > **IBM Tivoli Monitoring** > **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.

trace configuration:
You can edit the handler configuration file `*install_dir*\Config\ITMConfigRAS.properties` for UNIX systems and the `*install_dir*\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 *install_dir*\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 `*install_dir*/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.

Trace options for the Summarization and Pruning agent

Use the trace options for the Tivoli Summarization and Pruning agent to gather data for diagnosing problems.

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 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.

Note:

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 300,000 lines. To change the defaults, use the following settings in the `KSYENV` (Windows) or `sy.ini` (Linux or UNIX) file:

   ```
   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.

   To reduce the number and size of `*_sy_java_*.log` to the minimum, you can set <*A*> and <*B*> to 1, which creates a single `*_sy_java_*.log` file with a maximum file size of approximately 225 KB. (If you set <*A*> and <*B*> to 0, the Summarization and Pruning agent stops working.)

Summarization and Pruning agent user interface:

Edit the handler configuration file to set the debug tracing level and other parameters.

You can edit the handler configuration file, *install_dir*/Config/ITMConfigRAS.properties, set the handler99 as the configuration handler, and set the debug tracing to the maximum DEBUG_MAX as shown in the following settings:

```
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 in the (Linux and UNIX) *install_dir*\TMAITM6 or (Windows) *install_dir*\TMAITM6 directory, containing a link to the handler configuration file:

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

After the Summarization and Pruning agent configuration is started, tracing appears in the (Linux or UNIX) *install_dir*/logs/config.trc or (Windows) *install_dir*\logs\config.trc file, as described by the handler configuration file.

To trace the 2-way 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 options for tacmd commands

You can set specific levels of tacmd command tracing.

Procedure

- Windows Manually edit the *install_dir*\KUIENV file with the standard KBB_RAS1 statement to include the following settings:

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

  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)
  ```

- Linux UNIX Manually edit the *install_dir*/bin/tacmd shell script to add a line like the following example:

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

  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 3. Setting the trace option for the Tivoli Monitoring upgrade toolkit

Trace option	Instructions
Endpoint tracing	Run the following command to set `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 event forwarding

If your monitoring environment is configured for event forwarding, you can forward situation events to the and view events on the event server through the . If you want to forward situation events to and view updates from event server in the portal client, you can set the trace for the event forwarder on the .

Use the event forwarding trace facility to diagnose problems with event forwarding.

About this task

The event forwarding trace facility uses RAS1 tracing. 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 monitoring server for the change to take effect.

Use the following instructions to set the trace levels:

Windows :

1. In , right-click the .
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 monitoring server for the trace to take effect.

Linux UNIX

1. Edit `install_dir/config/hostname_ms_Tivoli_Enterprise_Monitoring_Server_ID.config`

   where:

   install_dir
   Specifies the installation directory of the monitoring server.

   hostname
   Specifies the host name value supplied during installation.
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 the monitoring server for the trace to take effect.
5. The 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

Edit the `K`*`pc`*`ENV` (where *pc* is the product code) environment file to set the RAS1 trace level for your OMEGAMON product.

This syntax is used to specify a RAS1 trace in the `K`*`pp`*`ENV` 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 configuration setting to the `KppENV` file, you must stop and restart the address space for the setting 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.

RAS1 trace setting syntax

The KBB_RAS1 environment variable setting follows the RAS1 trace setting syntax as described in “RAS1 syntax” on page 46.

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 systems, see your individual monitoring agent's user's guide.

Dynamically modify trace settings for a Tivoli Monitoring component

You can dynamically modify a product's trace settings using the **`tacmd settrace`** command or the RAS1 interface on the IBM Tivoli Monitoring Service Console. With both methods, the changed RAS1 trace settings take effect immediately.

The tacmd settrace command is described in the *IBM Tivoli Monitoring Command Reference* (http://pic.dhe.ibm.com/infocenter/tivihelp/v61r1/topic/com.ibm.itm.doc_6.3fp2/ic/landing_cmdref.htm). The IBM Tivoli Monitoring Service Console and its RAS1 interface are described here.You can also view the IBM Education Assistant training, Dynamically modify trace settings with the tacmd command.

Note: When a product is restarted, its trace settings are read again from the product's configuration file, either `K`*`pc`*`ENV` or *`pc`*`.ini` where *pc* is the two-character product code. Dynamically modifying trace settings does not change the **`KBB_RAS1`** environment variable in the product's configuration file. To persist tracing changes across product restarts, you must update **`KBB_RAS1`** in the product's configuration file.

IBM Tivoli Monitoring Service Console

Every IBM Tivoli Monitoring process automatically includes an integrated web server. The server provides web access to a facility known as theIBM Tivoli Monitoring Service Console. Each Tivoli Monitoring process that is active on a system has a separate service console.

The service console is available on all platforms and it offers a variety of system administrator utilities to display component status and to query and modify configuration information for an active Tivoli Monitoring process.

Service consoles are uniquely identified by their service point names. If you point a browser to the integrated web server's 1920 listening port on a system that is running any IBM Tivoli Monitoring processes, you will see a web page like the one shown here.

Table 4. IBM Tivoli Monitoring Service Index. In this representation of the IBM Tivoli Monitoring Service Console are two monitoring agents running on the AIX system, the UNIX Log File agent and the UNIX OS agent. To access the service console for the UNIX Log File agent, you would click the “IBM Tivoli Monitoring Service Console” link under the service point name, “root.tameaix5_ul”.

IBM Tivoli Monitoring Service IndexWed, 21 Mar 2013 14:31:02 GMT
• Service Point: tameaix5_ux
– UX Agent Service Interface
• Service Point: root.tameaix5_ux
– IBM Tivoli Monitoring Service Console
• Service Point: tameaix5_ul
– IBM Tivoli UL Agent Service Interface
• Service Point: root.tameaix5_ul
– IBM IBM Tivoli Monitoring Service Console

In addition to service console links, the example has links to the Agent Service Interface, which allows you to get reports for an installed agent. These reports include information about an agent's private situations, private history data, attribute descriptions, and current values. You can also make a service interface request by supplying XML elements.

A Service Index might include other types of links. For example, if you are running a hub Tivoli Enterprise Monitoring Server, the Service Index on that system includes a link to the “IBM Tivoli Monitoring Web Services”, which provides an interface to the hub monitoring server's SOAP server.

Starting the IBM Tivoli Monitoring service console

If at least one IBM Tivoli Monitoring process is running on a system, you can start a web session to the service console.

Before you begin

The service console performs user authentication using the native OS security facility:

- On UNIX-based systems, your user ID and password must be authenticated by the local security controls.
- On Windows systems, you must pass the Windows workstation user ID and password prompt.
- On z/OS systems, your user ID and password are checked by the z/OS security facility (RACF/SAF).

By default, users are permitted five unsuccessful login attempts to the service console before they are locked out. The default lockout period is 30 minutes.

A password is always required to access the service console. Blank passwords, even if defined for a particular user ID, cannot access the service console. You can only access the service console with a user ID and non-blank password.

Procedure

1. Open a browser window.

2. Enter the following URL where `hostname` is the fully qualified name or IP address of the computer where the Tivoli Monitoring process is running, and 1920 is the well-known HTTP listening port of the integrated web server:

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

   If the 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 65.
3. Click the service console link associated with the desired process (service point name).
4. After the login window opens, enter a valid user ID and password for the system that you are accessing. Upon successful login, the service console web page is displayed with three areas:
   - Header
   - Command Results
   - Command Field
5. Issue service console commands in the command input area. For a list available commands, type a question mark (?) and click **Submit**.

Service console RAS1 interface

Among the utilities offered by the IBM Tivoli Monitoring Service Console is a RAS1 interface for listing and setting RAS1 trace levels, which is invoked with the **`ras1`** command.

If you type **`ras1`** in the command input area, you can see usage information for this command. The **`ras1`** sub-commands include **`set`**, **`list`**, and **`units`**.

Turn on dynamic tracing: `ras1 set`

The **`ras1 set`** command dynamically replaces a product's current `KBB_RAS1` value with the new value that you specify. As an example, if the default `KBB_RAS1=ERROR` is in effect and you want to enable full tracing of the *xxx* compilation unit and low-level detailed tracing of the *yyy* compilation unit, you would enter this command after logging in to the service console:

```
ras1 set ERROR (UNIT:xxx ALL) (UNIT:yyy ERROR DETAIL)
```

. The two additional `UNIT` filters take effect immediately, without requiring a product recycle.

Display current tracing levels: `ras1 list`

The **`ras1 list`** command displays a product's current tracing levels.

Best practice is to issue a **`ras1 list`** before **`ras1 set`** for the following reasons:

- To not omit an important tracing parameter in the new **`ras1 set`** value. (Note that each **`ras1 set`** command is a complete replacement.)
- To record the original tracing level so that you can restore it after you finish capturing diagnostic data.

Setting trace to **`ALL`** includes every trace point defined for a particular component or compilation unit. It is the equivalent of setting "Error Detail Flow State Input Output Metrics". This might result in a large amount of trace. **`ALL`** can sometimes be necessary when you begin troubleshooting a problem but if you have been given a more specific setting, use the specific setting instead of **`ALL`**.

The ras1 list**ras1 list** command displays information in a slightly different format that requires some explanation. For example, here is the **ras1 list** ras1 list output against a Universal Agent running with **KBB_RAS1=ERROR (UNIT:kumamain Error State) (UNIT:kt1 Error Detail Flow)**.

```
00000003, Unit="kt1", Class=EVERYE+EVERYU+ER+FL+DET
00000001, Unit="kumamain", Class=EVERYE+EVERYU+ER+ST
00000005, Comp="KLX", Class=EVERYE+EVERYU+ER
00000007, Comp="KDE", Class=EVERYE+EVERYU+ER+ST+IN+OUT+ME
00000009, Comp="NCS", Class=EVERYE+EVERYU+ER
0000000B, Comp="KDH", Class=EVERYE+EVERYU+ER

Default trace class(es): EVERYE+EVERYU+ER
```

ERROR-level logging is displayed as EVERYE+EVERYU+ER where EVERYE stands for “EveryEntry”, EVERYU stands for “EveryUnit”, and ER is an abbreviation for ERROR. The first parameter after **KBB_RAS1=** is designated as the global class. Because it has been set to ERROR, we see Default trace class(es): EVERYE+EVERYU+ER. The kumamain.cpp compilation unit has its own **UNIT** parameter with the Error and State classes specified, and that results in ER+ST in the **ras1 list** output. Similarly, the “kt1” compilation unit shows ER+FL+DET to represent Error Detail Flow.

In this sample Universal Agent configuration, there is a component debug variable active, KDE_DEBUG=Y. This environment variable provides a short-hand notation for activating ERROR STATE INPUT OUTPUT METRICS tracing (listed above as ER+ST+IN+OUT+ME) in all compilation units belonging to the KDE component. The components KLX, NCS, and KDH are running with a Kxx_DEBUG value of ‘N’, which defaults to ERROR (EVERYE+EVERYU+ER).

Determine which UNITs and COMPs are active: ras1 units

The **ras1 units** command helps you determine which UNITs and COMPs are active in an IBM Tivoli Monitoring product. The first column contains the available UNIT values, and the last column shows the corresponding COMP values. Here is an excerpt of **ras1 units** command output for the Windows OS agent:

```
kbbcre1.c, 630, Mar 20 2013, 14:42:14, 1.1, *
kbbcrn1.c, 630, Mar 20 2013, 14:42:13, 1.1, *
kdhb1de.c, 630, Mar 20 2013, 14:52:47, 1.1.1.1, KDH
kdh0med.c, 630, Mar 20 2013, 14:52:28, 1.1.1.1, KDH
kdhsrej.c, 630, Mar 20 2013, 14:53:37, %I%, KDH
kdhb1fh.c, 630, Mar 20 2013, 14:52:45, 1.1, KDH
kdhb1oe.c, 630, Mar 20 2013, 14:52:53, 1.2, KDH
kdhs1ns.c, 630, Mar 20 2013, 14:53:38, 1.3.1.2, KDH
kbbacdl.c, 630, Mar 20 2013, 14:41:46, 1.2, ACF1
kbbaclc.c, 630, Mar 20 2013, 14:41:45, 1.4.1.1, ACF1
kbbacli.c, 630, Mar 20 2013, 14:41:47, 1.11.1.1, ACF1
kdhsfcn.c, 630, Mar 20 2013, 14:53:42, 1.3, KDH
kdhserq.c, 630, Mar 20 2013, 14:53:15, 1.2, KDH
kdhb1pr.c, 630, Mar 20 2013, 14:52:54, 1.1, KDH
kdhsgnh.c, 630, Mar 20 2013, 14:53:12, 1.1.1.4, KDH
kdh0uts.c, 630, Mar 20 2013, 14:52:27, 1.1, KDH
kdhsrsp.c, 630, Mar 20 2013, 14:53:46, 1.2, KDH
kdhs1rp.c, 630, Mar 20 2013, 14:53:44, 1.1, KDH
kdhscsv.c, 630, Mar 20 2013, 14:53:25, 1.14.1.1, KDH
kdebbac.c, 630, Mar 20 2013, 14:50:03, 1.11, KDE
kdebsac.c, 630, Mar 20 2013, 14:50:34, 1.2, KDE
```

The output shows that KDH, ACF1, and KDE are among the active components. Several Tivoli Monitoring components have their own

DEBUG environment variable that provides equivalent tracing functionality to the COMP option. For example, adding **KDH_DEBUG=A** to an agent's KpcENV or *pc*.ini file would have the same effect as adding **(COMP:KDH ALL)** to **KBB_RAS1**. It activates **ALL** level tracing for each source file that has KDH listed in the last column.

Suppose that you want to capture additional tracing for the first two source files in the **ras1 units** output. We know that the UNIT value matches any compilation unit that starts with the specified character string. Therefore, you can use the **ras1 set** command to add **(UNIT:kbbcr ERROR FLOW)**. ERROR tracing is already in effect because it is the global class, but the addition of FLOW tracing causes function entry and exit data to be logged for the two source files that begin with "kbbcr", namely, "kbbcre1.c" and "kbbcrn1.c".

Turn off dynamic tracing: ras1 set (UNIT:*name* ANY)
After you have used **ras1 set** to activate additional tracing and captured the required diagnostic data, you can use the ANY option to turn off the tracing. Continuing with the previous example, you would deactivate **kbbcr FLOW** tracing by entering the following command: **ras1 set (UNIT:kbbcr ANY)**. This command has the effect of removing kbbcr from the list of active UNITs, and any source files beginning with "kbbcr" now run with default ERROR-level logging.

Blocking access to the IBM Tivoli Monitoring Service Console

The IBM Tivoli Monitoring Service Console facility is automatically included in the integrated web server that is part of every Tivoli Monitoring process.

You can prevent users from accessing the service console that is available through the integral web server.

About this task

If you need to prevent users from accessing the service console, use one of the following steps. Each step is listed in order from most general to most specific:

Procedure

- Disable the entire integrated web server so that it is not initialized during process startup:
  1. Update the **KDE_TRANSPORT** environment variable that configures a product's networking options. (Note that KDC_FAMILIES is an older environment variable that serves the same purpose and follows the same syntax rules as KDE_TRANSPORT)
  2. At the end of the **KDE_TRANSPORT** string, add a space and the following parameter:

     ```
     http_server:n
     ```

  The resulting value might look like this: **KDE_TRANSPORT=IP.PIPE PORT:1918 use:y IP.SPIPE PORT:3660 use:y IP use:n SNA use:n http_server:n**. As a consequence of setting this environment variable, the service console facility and its listening ports are not started. For more information on the **KDE_TRANSPORT** parameters, see the "Tivoli Monitoring protocol usage and protocol modifiers" in the *IBM Tivoli Monitoring Installation and Setup Guide*.
- Disable only the service console and allow the integrated web server to start:

1. Update the **KDE_TRANSPORT** environment variable that configures a product's networking options.
2. At the end of the **KDE_TRANSPORT** string, add a space and the following parameter:

   ```
   http_console:n
   ```

The resulting value might look like this: **KDE_TRANSPORT=IP.PIPE PORT:1918 use:y IP.SPIPE PORT:3660 use:y IP use:n SNA use:n http_console:n**. After you update the environment variable and recycle the product, if you go to `http://`*hostname*`:1920`, you do not see “IBM Tivoli Monitoring Service Console” listed under the product’s service point.

- Disable a particular listening port so that the service console cannot be accessed:

1. By default, the integrated web server starts an http listener on port 1920 and an https listener on port 3661. Assigning a port number of 0 has the effect of disabling that listener.
2. If you want to enforce SSL-only web access, you can update the **KDE_TRANSPORT** environment variable: **KDE_TRANSPORT=IP.PIPE PORT:1918 use:y IP.SPIPE PORT:3660 use:y IP use:n SNA use:n http:0**

After setting this environment variable, you can access the service console only through the `https://`*hostname*`:3661` URL. To block both listening ports, and prevent all service console access, add a space and the follow parameter to the **KDE_TRANSPORT** value:

https:0

Displaying portal server tasks in the command prompt

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

Procedure

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

Results

The next time the portal server is started, the process tasks are shown in a command prompt window.

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 with the Tivoli Enterprise Portal browser client, IBM Support might instruct you to uninstall and to clear the Java archive (JAR) cache.

Procedure

1. If the Tivoli Enterprise Portal is running, exit by closing the browser window.
2. Start the Java Control Panel:
   - Windows Click **Start** > **Settings** > **Control Panel** and double-click the Java Control Panel icon.
   - Linux Run the following command: `*java_install_dir*/jre/bin/ControlPanel`
3. In the Java Control Panel's General panel, click the Settings button and the Delete Files button. Select all the check boxes that contain references to Applications and Applets. Click **OK** to clear the cache.
4. When a message indicates that the JAR cache is cleared, click **OK**.

What to do next

If you want to start browser mode again, restart your browser and type the URL for the 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 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, such as IBM Tivoli Composite Application Manager products. For more information about this command, see the *IBM Tivoli Monitoring Command Reference* (http://pic.dhe.ibm.com/infocenter/tivihelp/v61r1/topic/com.ibm.itm.doc_6.3fp2/ic/landing_cmdref.htm).

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.

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.

Common logging facility

The common logging facility captures events that occur with your IBM Tivoli Monitoring environment, including the self-describing agents, actions of the Warehouse Proxy Agent, EIF-SSL connections, automated Take Action commands, and the integration of Tivoli Monitoring with Tivoli Application Dependency Discovery Manager.

You can record these events in the Tivoli Data Warehouse for later retrieval and analysis.

For more information about common logging, see "Audit logging" in the *IBM Tivoli Monitoring Administrator's Guide*. For errors that occur with the facility, see Chapter 19, "Auditing facility troubleshooting," on page 315.

ITMSuper

The tool performs audits of the 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 on any platform. You can run the tool from a Windows system without having other 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. See IBM Support Assistant (http://www-01.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 problems and resolutions" on page 74
- "Windows installation problems and resolutions" on page 90
- "UNIX-based system installation problems and resolutions" on page 93
- "Troubleshooting z/OS-based installations" on page 103
- "Uninstallation problems and workarounds" on page 115

Frequently asked questions

General installation frequently asked questions

The following table lists general installation frequently asked questions.

Table 5. 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 6. 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 6. Windows installation frequently asked questions (continued)

Question	Answer
How can I diagnose problems with product browse settings?	1. Select **Start** > **Programs** > **IBM Tivoli Monitoring** > **Manage Tivoli Enterprise Monitoring Services**. 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.

Linux and UNIX-based systems installation frequently asked questions

Review the most common issues related to installation on Linux and UNIX-based computers for an explanation and possible solution.

Table 7. Frequently asked questions for Linux and UNIX-based systems installation

Problem	Solution
The product was installed as root. Without reinstalling 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 starting the 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.
The product was installed with non-root user and started by root user. Why am I having issues with permissions?	When the hub Tivoli Enterprise Monitoring Server is installed and configured with non-root user and is started by root user, there might be some files that are accessible to the root user but not the non-root user. The non-root user cannot access some files created when the monitoring server was started as root The changes in permissions due to the root user affect the monitoring server. Several attempts with root user might cause the monitoring server service to fail. To overcome the permission issue, run **`securemain`** with non-root user, and start the component with non-root user.
How can I set the trace option to capture any abends (core files)?	Add the following in the `pc.ini` file where `pc` is the two-character product code for the monitoring agent. 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 must 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)

Table 7. Frequently asked questions for Linux and UNIX-based systems installation (continued)

Problem	Solution
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 the 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.
Pressing the backspace key, characters such as "^?" and "^H" are displayed 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, the backspace key was incorrectly configured. 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 installation, 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 7. Frequently asked questions for Linux and 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 binary files have hard-coded execution paths. This coding is required by the operating system in order to start 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. 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

Review the symptoms of the most common installation and initial configuration problems for suggested causes and solutions.

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 Tivoli Enterprise Monitoring Server and Tivoli Enterprise Portal Server to IBM Tivoli Monitoring V6.2.3 or higher, 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 “Resolving application support problems” on page 13 for more information.

Review the symptoms that can occur in the for suggested causes and solutions.

Failure to create the Tivoli Data 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.

Failure to reset the sysadmin password on the hub monitoring server

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

New user is not created or a password is not reset

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

On Windows systems, a Tivoli Monitoring Warehouse DSN is not created in the

If the Tivoli Monitoring Warehouse DSN is not created by the , create the DSN manually by using the Warehouse Proxy Agent configuration instructions. See “Configure communications between the Tivoli Enterprise Portal Server and the data warehouse > Configuring a Windows portal server (ODBC connection)” 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 *`temporary_directory`*`\DSNUtil` (for example, `C:\Temp\DSNUtil`).

Failure to test DSN with database connectivity

If you have an existing 32-bit Tivoli Data Warehouse database in the 64-bit DB2 instance, the 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 *temporary_directory*\DSNUtil, for example, C:\Temp\DSNUtil.

Some system types show as "Unknown Operating System"

When you run the discovery process for available machines, the 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 operating system, the system is moved to the correct category in the list.

The 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 operating system that is not discovered correctly, you should ideally force nmap to generate a signature, so that you can submit it to Insecure.Org for integration in 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`.

Unable to discover systems within a specified IP range

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

Tivoli Enterprise Monitoring Agents

Review the monitoring agent installation and configuration symptoms for suggested causes and solutions to the problems that occur during or after installation and initial configuration.

Configuration panel is blank on 64-bit Windows systems

Problem

The configuration panel is blank on 64-bit Windows systems where the Tivoli Enterprise Monitoring Agent Framework (component GL) is version 06.23.00.00 or 06.23.01.00.

Solution

Check the GL component version by running `kincinfo -t GL` from a Windows command line. Example:

```
install_dir\kincinfo -t GL
```

If the GL component version is 06.23.00.00 or 06.23.01.00, take one of the following actions:

- The preferred action is to upgrade the Windows OS Agent to Version 6.2.3 Fix Pack 2 or later.
- The alternate action is to install the Agent Compatibility (AC) component from the IBM Tivoli Monitoring V6.2.3 Fix Pack 1 (or later) media. See “Windows: Installing a monitoring agent” > “Installing the Agent Compatibility (AC) component” in the *IBM Tivoli Monitoring Installation and Setup Guide*.

Agent reconfiguration is not saved on Windows

Problem

You reconfigure the monitoring agent but your changes do not take affect. Also, you cannot start or stop the monitoring agent, and running the **`kincinfo -i`** command fails (see “Performance tuning > Validating your installation” in the *IBM Tivoli Monitoring Installation and Setup Guide*).

Cause On Windows 7 and Windows 8 the Administrator user is disabled by default. The IBM Tivoli Monitoring installer requires Administrator rights, hence the Administrator user is enabled temporarily to install the agents. If a non-administrator user modifies the agent configuration, the changes are not saved.

Solution

Log on to Windows with a user ID that has administrator rights before installing, configuring, and working with Tivoli Monitoring components.

Monitoring server connection information is changed after upgrade

Problem

A Tivoli Enterprise Monitoring Agent that connects to a different Tivoli Enterprise Monitoring Server than the one that the OS agent connects to might have its monitoring server changed after the monitoring agent is upgraded to a new version using remote deployment.

For example, consider an environment in which the monitoring agent for DB2 and the Linux OS agent V6.2.3 are installed on the same computer. The DB2 agent connects to the RTEMS 1 monitoring server and the OS agent connects to the RTEMS 2 monitoring server. After the upgrade, the DB2 agent connection is to RTEMS 2 rather than RTEMS 1. The same problem occurs when agents at V6.2.3 or earlier are updated using group deploy or single deploy.

Solution

If you have a Tivoli Monitoring V6.2.3 (or earlier) OS agent installed on the same computer as a product monitoring agent and both agents connect to different monitoring servers, upgrade the OS agent to V6.2.3 Fix Pack 1 or later version before upgrading the other monitoring agent. Otherwise, a remote deployment upgrade of the monitoring agent causes the monitoring server connection to change to the same monitoring server that the OS agent connects to.

Receive duplicate insert errors

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.

OS Agent installation does not detect s

Any monitoring 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 s.

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.

- Windows 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
  ```

- Linux UNIX 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 monitoring agent:

  ```
  CTIRA_SYSTEM_NAME=$RUNNINGHOSTNAME$
  ```

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.

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.

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 -rKproductcode**.
- 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

About this task

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 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 a 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.

Backup failure message during a remote monitoring server upgrade

During a remote Tivoli Enterprise Monitoring Server upgrade, if you receive the 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?", exit the upgrade installation to avoid losing data.

About this task

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:

Procedure

1. Click NO and exit the upgrade installation.
2. Restart the remote monitoring server computer.
3. Stop all Tivoli Monitoring components.
4. Rerun the upgrade installation now with the remote monitoring server in the stopped state.

Results

The upgrade installation is complete.

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 shows error AMXUT7502E

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 8 to determine the exact cause of the problem.

Table 8. 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, “Logs and data collection for troubleshooting,” on page 5 for information on what types of data to collect before contacting Support. See the IBM Support Portal (http://www.ibm.com/support/entry/portal/software).

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.

The monitoring server and portal server automatically start after running Application Support Installer

After running the Application Support Installer the Tivoli Enterprise Monitoring Server and Tivoli Enterprise Portal Server automatically start, even if they were not running before the installation. 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.

Self-describing capability

Review the self-describing agent and application support problems to learn if your installation or configuration problem is related.

Receive a message after installing a self-describing agent

After installing 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.

Receive fatal errors during self-describing agent installation

Certain fatal error conditions when a self-describing monitoring agent installation is running on a Tivoli Enterprise Monitoring Serverrequire 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.

Missing agent managed system group in a hot standby environment

In certain IBM Tivoli Monitoring environments, it is possible to get no predefined managed system group for a self-describing agent in a hot standby environment.

Tivoli Monitoring environment:

- Hub Tivoli Enterprise Monitoring Server and the mirror hub monitoring server are at V6.2.3 Fix Pack 1 (or later)
- Remote monitoring server (or servers) is at V6.2.3
- A monitoring agent with an affinity that is not known to the monitoring server, such as a new agent

If only a single hub monitoring server is available during an agent's application support installation and the hub is stopped, the mirror hub is started, the application support installation to the new (mirror) hub is initiated. In such a scenario, it is possible to get no predefined managed system group for a product.

To verify that the managed system group is present, run `tacmd listsystemlist` at the command line. If the managed system group is not listed, recycle the monitoring agent.

Self-describing agent installation completes successfully but sqlStatus 79 error messages are logged

After the product is successfully installed, the self-describing agent mechanism tries to delete all prior versions of the installation record for the same product. If there is no prior version of the installation record, the deletion attempt returns a code of 79.

As an example, consider the following error messages that were logged even though the installation was successful. Such messages can be disregarded.

```
(0002-E9A166E3:kfasdwlm.c,1961,"KFASDM_RequestMgr") Self-Describing Install
 Completed Successfully for PRODUCT "CP", VER "05100173", ID "TMS", IDVER
my "05100173".
(003-E9A166E3:kfasdsrm.c,1531,"KFASDM_DeleteTapplpropLocal") Open request for
 delete local TAPPLPROPS failed.
status <79> product <CP> product version <05100173>
(0004-E9A166E3:kfasdwlm.c,1976,"KFASDM_RequestMgr") KFASDM_DeleteTapplpropLocal
 returned sqlStatus 79. product <CP> product version <05100173>
```

Self-describing agent overwrites most recent manually installed z/OS monitoring server support

An older version of a self-describing agent might overwrite the most recent version of Tivoli Enterprise Monitoring Server application support that is manually installed on a z/OS monitoring server.

The most recent version of the monitoring server application support is not installed through the self-describing mechanism.

To resolve this issue, disable self-describing mode on the agent that has the older application support and add the most recent version of application support to the z/OS monitoring server or use the self-describing mechanism to install the new monitoring server support across your environment. See “Adding application support to a monitoring server on z/OS” in the *Configuring the Tivoli Enterprise Monitoring Server on z/OS* guide.

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. Here is an a example of the error (timestamp removed):

```
OnMiaMoving - Processing Feature [KIWWICNS]
OnMiaMoving - Error log [C:\IBM\ITM\InstallITM\MiaError.log] created.
OnMiaMoving - Feature KIWWICNS [Tivoli Enterprise Portal Server Extensions]
 will be installed.
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.
OnMiaMoving - Install for Feature[KIWWICNS/Tivoli Enterprise Portal Server
 Extensions] successful RC=-1073741819.
OnMiaMoving - Install for Feature[KIWWICNS/Tivoli Enterprise Portal Server
 Extensions] may have failed, please check!
```

Checking the *install_dir*\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 installation 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

About this task

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 installation 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 host name 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.

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.

Deploying an agent instance gives a KUICAR020E error

You get a KUICAR020E error 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).

```
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. After 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 installation processes and reboot the system.

UNIX-based system installation problems and resolutions

Review the symptoms and possible resolutions to solve IBM Tivoli Monitoringinstallation problems on Linux or UNIX system.

Self-describing capability might be overwritten by UNIX monitoring server application support

Under the following conditions, if self-describing product installation is expected, one or more Tivoli Monitoring products might not be properly enabled for monitoring:

- The self-describing product installation for a hub or remote monitoring server might not run
- The product application support installation (seeding) step might not take place on the hub or remote monitoring server
- The self-describing product installation on the Tivoli Enterprise Portal Server might not take place

If your environment has a self-describing monitoring agent that is at a lower version of IBM Tivoli Monitoring than the Tivoli Enterprise Monitoring Server on Linux or UNIX that it connects to, it is possible that the installation of application support to the monitoring server overwrites the monitoring agent's self-describing capability.

Diagnosing that the self-describing capability is not available

Installation of a monitoring server on Linux or UNIX is different from that on Windows in that application support for all base monitoring agents and other supported agents are automatically installed on the monitoring server. The automatic installation of application support files for the agents might affect the self-describing agent capability. Check the monitoring server and portal server to ensure that self-describing agent products are installed as expected.

To determine if the monitoring server self-describing agent product installation and seeding took place, check the enterprise self-describing agent installation status with the following command:

```
tacmd listappinstallrecs -t PC
```

where *PC* is the product code for the self-describing agent in question, such as `nt` for the Windows OS agent. The following example of the output from `tacmd listappinstallrecs -t nt` shows how the results of a successful installation might look:

```
HUB/RTEMS        PRODUCT  VERSION  GRPID ID  IDVER    SEEDSTATE STATE STATUS
HUB_TEMS         NT       06230000 5655  TMS 06230000 Y         IC    0
HUB_TEMS         NT       06230000 5655  TPS 06230000           IC    0
HUB_TEMS         NT       06230000 5655  TPW 06230000           IC    0
REMOTE_TEMS_ZOS  NT       06230000 5655  TMS 06230000 Y         IC    0
```

The command output has entries for the `HUB TEMS` and any `REMOTE_TEMS` that the agent can be connected to. The entries for `PRODUCT NT` with `ID TMS` have a value of `IC` in the `STATE` column, `Y` in the `SEEDSTATE` column, and `0` in the `STATUS` column.

An unsuccessful installation and seeding might generate results like those in the following example:

```
HUB/RTEMS        PRODUCT  VERSION  GRPID ID  IDVER    SEEDSTATE STATE STATUS
HUB_TEMS         NT       06230000 5655  TMS 06230000                 0
```

The record for `PRODUCT NT` and `ID TMS` might not exist or, if it does exist, the `STATE` and `SEEDSTATE` columns are empty. In this example, the results show that the product `NT` was manually installed at the hub (`STATE` column is empty and there is an entry only for `ID TMS`).

Conditions that cause the problem

- The Self-Describing Agent feature is enabled for the enterprise
- You are installing or upgrading a Linux or UNIX monitoring server
- You intend to configure a self-describing agent to automatically install at one or more of the Tivoli Monitoring base agents
- The self-describing base agent is at a lower release level (such as Windows OS V6.2.3) than the Linux or UNIX monitoring server (such as monitoring server V6.2.3 Fix Pack 1).
- During the Linux or UNIX monitoring server installation, you do not select this base agent product (Windows OS) to seed (because you expect the self-describing agent to install and seed).
- During the portal server installation, the you do not select this base agent product (Windows OS) to install (because you expect the self-describing agent to install).
- The monitoring agent is installed and started, but the installation of the Linux or UNIX monitoring server self-describing capability does not occur. No errors are generated.

- If the higher level Linux or UNIX monitoring server is the hub, the self-describing agent does not attempt to install the product on the portal server. No errors are generated.

As a result, the Windows OS product is never seeded and the portal server might not have product support for Windows OS.

Cause of the problem

- The Linux or UNIX monitoring server installation program silently installs all available base monitoring agent product support files during any installation or upgrade, whether you want it or not.
- No option to select base monitoring agent product support was presented or visible during the Linux or UNIX monitoring server installation or upgrade. (Monitoring server installation on Windows and all portal server platform installations provide a base agent selection list of products to install or upgrade.)
- You might not expect the silent installation of product support to occur on the Linux or UNIX monitoring server.
- The silent installation of product application support files causes the monitoring server self-describing agent installer to bypass self-describing agent installation and seeding of a lower version of this base agent. The monitoring server self-describing agent installer will not overlay a higher level of application support already on a server with a lower version from the agent.
- If there is no self-describing agent enabled agent for this product running in the environment that is at the same release (or higher) of this Linux or UNIX monitoring server, the self-describing agent installation will never run.

Resolving the problem

- Run the manual product seeding step on this Linux or UNIX hub (or remote in some cases) monitoring server for the failed self-describing agent product.
- Manually install this product on the portal server and portal client if the expected self-describing agent product installation did not take place.

See “Self-describing agent installation” in the *IBM Tivoli Monitoring Installation and Setup Guide* and “Self-describing monitoring agents” in the *IBM Tivoli Monitoring Administrator's Guide*.

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

Review the cause and solution for errors encountered on RHEL6 64-bit systems during Tivoli Monitoring installation.

Problem

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
```

Cause 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.

Solution

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 included:

```
--------------------------------
# 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

See the Flash note about a newer ksh shell if you get a message about the Korn Shell after running the installer.

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.`

The Flash note includes detailed descriptions of the root cause, and also information on how to deal with this issue.

Linux OS agent fails to load shared libraries

If you get an error while loading shared libraries on Linux, install the libstdc++.so.5 library.

Problem

You get the following error when you attempt to load the shared object file for a Tivoli Monitoring component on Linux:

```
opt/IBM/TivoliMonitoring/bin/tivcmd: error while loading shared libraries:
libstdc++.so.5: cannot open shared object file: No such file or directory
```

The same error when loading the shared object file for the Linux OS agent shows a path of `/data/itm/li6263/lz/bin/klzagent/` (where `li6263` is the platform).

Cause The Linux missing C-runtime library error affects Tivoli Monitoring products or components running on Linux that make calls to C runtime functions.

Solution

Ensure that the appropriate 32-bit or 64-bit Linux `libstdc++.so.5` library is installed:

```
ls /usr/lib/libstdc++.so.5
```

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

If you get a runGSkit failure while running the **`install.sh`** command, install the libstdc++.so.5 library.

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.

Note: When specifying special characters (for example, $) within command parameters, use single quotes (') instead of double quotes (") around the characters.

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 installation 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`.

Receive KCIIN2363E error during non-root upgrade

If you get a KCIIN2363E error message regarding an incorrect password during a non-root upgrade of Tivoli Monitoring components, the remote execution service might not be running or enabled.

Symptom

During a non-root upgrade on a UNIX-based system, the Installer software might encounter root-owned files that cannot be upgraded. You are prompted for the root password to change ownership of the problematic files. Although you provide the correct root password, the `KCIIN2363E`

ERROR - the password is incorrect. Do you want to try another password [1=Yes, 2=No ; default is "1"] ? message is persisted.

Cause This can occur if the remote shell rsh and remote execution rexec services are not enabled on the system.

You can tell if rexec is enabled by entering the following command: rexec *hostname* ls (where *hostname* is the host name). If, after entering the password, you get a Connection Refused message, rexec is not running or enabled.

Solution
Consult the documentation for your operating system to enable the rsh and rexec services and start the installation again.

On HP-UX systems with a host name different from nodename, the upgrade installation fails to stop running processes

Running IBM Tivoli Monitoring processes were not shut down by the installer during the upgrade of the Tivoli Enterprise Monitoring Server or agents when the nodename does not equal the host name on HP-UX systems. On HP-UX, if the system has a host name longer than 8 characters, then the nodename should be 8 characters or fewer.

If the nodename and the host name are not in sync then you must shutdown all IBM Tivoli Monitoring processes before starting an addition product installation or upgrade.

Installation Manager is suspended during upgrade

The IBM Installation Manager can stop in the middle of an upgrade on non-Windows operating systems. If this happens, change the preferences to prevent a search of service repositories during the update.

Problem
After starting the Installation Manager to update an installed package, you select the Authorization Policy package and click **Update**. The installer starts searching for updates to install and does not finish.

Solution
Click **Cancel** to cancel the update, and edit the preferences:

1. In the Installation Manager, click **File** > **Preferences**.
2. In the Repositories panel, clear the **Search service repositories during installation and updates** check box and click **OK**.
3. Restart the update.

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.

KfwSQLClient utility fails on Linux and AIX systems

If the KfwSQLClient utility fails on Linux or AIX, set the library path in the Tivoli Enterprise Portal Server configuration file.

Set the following environment variable before running the command:

Linux **LD_LIBRARY_PATH**

AIX **LIBPATH**

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

Alternatively, this command can be invoked on Linux and AIX systems using the **itmcmd execute** command. Example:

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

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 installation in command line mode. However, you can run the installation 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 returns an encryption key setting error

Errors occur if you attempt a silent installation 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=IBMTivoliOMEGAMONEncrytionKey62
```

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

A Java VM heap dump occurs during installation, which uses the JRE.

About this task

Use the following steps to resolve the problem:

Procedure

1. In a terminal window, run the following command to display the Java version:
   ```
   java -version
   ```
2. Determine where the Java executable program is located by entering the following command:
   ```
   which java
   ```
3. Rename or uninstall the Java program. This effects any other applications which depend on Java. Be sure that it is safe to do so. If you are unsure, rename the Java executable program.
4. Run the following command again to ensure that the Java program 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 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

About this task

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.

AIX

Review the AIX errors for problem descriptions and solutions during installation and configuration on AIX systems.

The checkprereq fails on AIX 7.1

Problem
You get a failure from the prerequisite checking of the UNIX OS agent related to required memory on AIX 7.1.

Cause
The prerequisite checker is checking is the remaining available virtual memory. Although the system might have ample memory for the Tivoli Monitoring components being installed, the scanner flags an error (FAIL result), which can be caused by the slow release of available memory.

Solution
Determine the available memory on the AIX system with the following calculation where `vmstat('fre')` and `swap -s ('free')` are AIX OS commands to get system information:

```
available virtual memory(MB) = ( vmstat('fre') + swap -s ('free') ) *
pagesize(KB)/1024
```

If the calculated amount is larger than the Expected Memory delineated in the prerequisite checker report, the memory is sufficient to continue with the installation.

If this error happens with a prerequisite check that is part of the CLI tacmd command **`createNode`**, **`addSystem`**, or **`updateAgent`**, use the `IGNOREPREREQCHECK=Y` option to by pass the prerequisite check failure and proceed with the agent install.

Installation fails on AIX 7.1 TL 1

Problem
Installation of IBM Tivoli Monitoring on AIX 7.1 Technology Level (TL) 1 fails with the following message:

```
Initializing ...
Error: Port Library failed to initialize: -125
Error: Could not create the Java Virtual Machine.
```

Cause Installation of IBM Tivoli Monitoring on AIX 7.1 requires TL 1, Service Pack (SP) 2 or later.

To determine if your operating system is at this level, you can run the following command: **`oslevel -s`**

The result has the following format where the first `01` is the TL and the second `01` is the SP: `7100-01-01-1141`

Solution
Upgrade to AIX TL 1 SP 2. If you cannot upgrade to SP 2, you can download the fix for APAR IV09585 or an interim fix as described in the technote at http://www-01.ibm.com/support/docview.wss?uid=swg21575120. You must restart your system after you have upgraded to SP 2 or applied the fix for APAR IV09585.

Manage Tivoli Enterprise Monitoring Services does not start on AIX V6.1

Problem
You get a Java exception after invoking `itmcmd manage` to start Manage Tivoli Enterprise Monitoring Services on a 64-bit AIX V6.1 system,

Cause The following APARs must be installed before Manage Tivoli Enterprise Monitoring Services can be started:

- 6100-00 - AIX APAR IZ16878
- 6100-01 - AIX APAR IZ16847

Solution
Install the APARs from IBM Support:

AIX stat_daemon memory leak

Problem
The process stat_daemon has a memoryleak.

Solution
Install APAR IZ62080 for AIX 5.3 and APAR IZ58432 for AIX 6.1.

Related reference:

"Linux and UNIX-based systems installation frequently asked questions" on page 72

"Installation Manager is suspended during upgrade" on page 99

"KfwSQLClient utility fails on Linux and AIX systems" on page 100

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:

- "Tivoli Monitoring z/OS initialization checklist" on page 104
- "z/OS-based installations problems and resolutions" on page 111

Tivoli Monitoring z/OS initialization checklist

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

- "Tivoli Monitoring Services Engine initialization"
- "RAS1 service initialization"
- "TCP/IP service initialization" on page 105
- "SNA service initialization" on page 107
- "The Server list" on page 108
- "Local Location Broker service initialization" on page 109
- "Global Location Broker service initialization" on page 110
- "Tivoli Enterprise Monitoring Server hub availability" on page 111

Tivoli Monitoring Services Engine initialization

The 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 the Tivoli Monitoring Services Engine.

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

- Failures that result from unsupported Tivoli Monitoring Service 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 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 105 and "SNA service initialization" on page 107.

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 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 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:
About this task

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."
2. Ensure the Name Resolution is successful. See "Name Resolution" on page 106.
3. Ensure the first SEND ran without error. See "The First SEND" on page 107.

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: 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 host name 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 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 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

The 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:
The following 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, it 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

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:
(USCAC001.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). Bind to 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 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 change monitoring server storage parameters using the Configuration Tool?

About this task

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 EnterpriseMonitoring 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 monitoring server create runtime members job.

If you get a `DATA SET NOT FOUND` error when you attempt to create runtime members on your z/OS Tivoli Enterprise Monitoring Server, check that the RTE build job was successful and that the fields were set correctly.

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.

For more information about configuring a z/OSTivoli Enterprise Monitoring Server and the RTE Build job. see the *Configuring the Tivoli Enterprise Monitoring Server on z/OS* (http://pic.dhe.ibm.com/infocenter/tivihelp/v61r1/topic/com.ibm.omegamon_share.doc_6.3.0.1/ztemsconfig/ztemsconfig.htm).

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

About this task

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.

Unable to transfer catalog and attribute files to the monitoring server

If you attempt to copy the catalog and attribute files to a on z/OS using the “FTP Catalog and Attribute Files” option on Linux or UNIX and get an error that the transfer failed, take steps to resolve the error.

To confirm the problem, enter the following command in the logs directory on the portal server: `grep "PORT not allowed after EPSV ALL" itm_config*.trc`.

If the message returned is `sun.net.ftp.FtpProtocolException: PORT :503 EPSV ALL received - PORT not allowed after EPSV ALL`, delete selected catalog and attribute files on the z/OS monitoring server and start the catalog and attribute file transfer again in or with your FTP client.

The monitoring server starts normally in a system with no Integrated Cryptographic Service Facility but does not connect to the portal server

Although Integrated Cryptographic Service Facility (ICSF) provides robust password encryption, you are not required to use it because it can affect compatibility with z/OS OMEGAMON monitoring products.

If you do not have the Integrated Cryptographic Service Facility installed, you need to add USE_EGG1_FLAG=1 to the Tivoli Enterprise Portal Server configuration to enable connection with the Tivoli Enterprise Monitoring Server.

About this task

Complete the following steps so that the monitoring server can connect to the portal server:

Procedure

1. During monitoring server configuration, select **Configure the Tivoli Enterprise Monitoring Server** > **Specify configuration values** > **Integrated Cryptographic Service Facility (ICSF) installed?**and specify **N**(No).
2. After the monitoring server configuration is complete and it is running, 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:
   a. On a new line, type `USE_EGG1_FLAG=1`
   b. Save the file and exit.
   c. Stop the portal server if it is running and restart it.

Backing up the ICAT and CSI environment

Manually merge existing datasets with datasets if IBM Software Support instructs you to do so.

Procedure

1. Back up all of the following datasets:
   - Runtime
   - Target
   - INSTDATA
   - INSTDATW
   - INSTJOBS
   - INSTLIB
   - INSTLIBW
   - INSTQLCK
   - INSTSTAT
2. After installing the product on a new CSI, review 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 to their counterparts in the old Target libraries, ensuring that like-named members are replaced.
   - TKANCMD
   - TKANCUS
   - TKANDATV
   - TKANHENU
   - TKANMAC
   - TKANMOD
   - TKANMODL
   - TKANPAR
   - TKANPENU
   - TKANSAM
   - TKCIINST

- TKNSLOCL

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 Eclipse help server

Kill the javaw tasks associated with the Eclipse help server on the system so that the uninstallation can continue.

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 9. Removing a failed installation on Windows

Goal	Where to find information
Remove a failed installation from a computer that has never had or Candle OMEGAMON installed.	"Removing a failed first time installation"
Remove a failed installation from a computer that you were trying to upgrade from Candle OMEGAMON.	"Removing a failed upgrade" on page 117

Removing a failed first time installation

About this task

Use the following steps to remove a partially installed 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 installation directory (`C:\IBM\ITM` by default).
3. Launch the 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 window, right-click each and click **Advanced** > **Unconfigure**. Repeat this step for all components that are listed. Close the 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 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 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 bookmark from the Windows desktop start menu.

You can now install .

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 installation 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 116. 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 or just install 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 . You must either completely reinstall the previous release and then upgrade to or just install without attempting to upgrade.

Check the Add and Remove Programs tool to see if either your previously installed Candle OMEGAMON or is available.

If neither are available, see "Neither products are available in the Add and Remove Programs tool" on page 118.

If one is available see "One product is available in the Add and Remove Programs utility" on page 118.

If both are available, "Both products are available in the Add and Remove Programs tool" on page 119.

Neither products are available in the Add and Remove Programs tool:
About this task

Use the following steps if neither Candle OMEGAMON or exists in the Add and Remove Programs tool:

1. Open the Windows Explorer and navigate to the 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 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 window, right-click each and click **Advanced** > **Unconfigure**. Repeat this step for all components that are listed.
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 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 119 to verify that you successfully removed the failed upgrade.
17. Remove the 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 bookmark from the Windows desktop start menu.

One product is available in the Add and Remove Programs utility:

If the Windows **Add and Remove Programs** utility has an entry for Candle OMEGAMON or IBM Tivoli Monitoring, attempt to uninstall.

About this task

Use the following steps if an entry for either Candle OMEGAMON or IBM Tivoli Monitoring exists in the **Add and Remove Programs** utility:

1. Attempt to uninstall both releases from the **Add and Remove Programs** entry.
2. If this is successful, proceed to "Verifying the uninstallation."
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 118.
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 <*`install_dir`*`\Install\Ver` directory, where *install_dir* 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, "Logs and data collection for troubleshooting," on page 5 for information on what types of data to collect before contacting IBM Support.

Both products are available in the Add and Remove Programs tool:
About this task

Use the following steps if both the Candle OMEGAMON or IBM Tivoli Monitoring entries exist in the Add and Remove Programs tool:

Procedure

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:
About this task

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 shows error AMXUT7512E

The error AMXUT7512E, which indicates that the agent was not uninstalled, might occur when running the Distributed Monitoring Upgrade Toolkit.

The agent was not uninstalled for one of the following reasons:

- Another uninstallation is 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 10 to determine the exact cause of the problem.

Table 10. 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 11:

Table 11. 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, “Logs and data collection for troubleshooting,” on page 5 for information on what types of data to collect before contacting Support. See the IBM Support Portal (http://www.ibm.com/support/entry/portal/software).

Prompted to uninstall a database that was not running during uninstallation

During uninstallation, when prompted for the DB2 user name and password 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 Enterprise Portal MSSQL/MSDE Database`.

The database was not running and the portal server is installed and configured with a DB2 database and not an MS SQL Server database.

It is likely that the system you are using at one time had an 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

Review the connectivity troubleshooting topics for problems you might experience with logging in, passwords, and communication among IBM Tivoli Monitoring components.

When the Tivoli Enterprise Portal detects a connection error, it can repair the error and your client session can resume unaffected. Use the connectivity topics 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 103 for information about configuration problems affect connectivity.

Cannot log on to the portal server

If you are unable to successfully log on to the portal server to start your Tivoli Enterprise Portal work session, review the symptoms and corrective actions to remedy the problem.

The following table provides resolutions for problems logging in to the .

Table 12. Cannot log in to the

Problem	Corrective action and solution
User authorization failed -OR- `KFWITM215E: Unable to process logon request`	• Ensure that the user ID and password are correct. (The user ID must use 10 or fewer ASCII characters and contain no spaces. The name is limited to 8 characters if user authentication is at the hub monitoring server and uses RACF® security for z/OS.) • 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* (http://pic.dhe.ibm.com/infocenter/tivihelp/v61r1/topic/com.ibm.itm.doc_6.3fp2/install/itm_install.htm) or *IBM Tivoli OMEGAMON XE and Tivoli Management Services on z/OS: Common Planning and Configuration Guide* (http://pic.dhe.ibm.com/infocenter/tivihelp/v61r1/topic/com.ibm.omegamon_share.doc_6.3.0.1/zcommonconfig/zcommonconfig.htm).

`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 "The portal server does not start or stops responding" on page 17.

Table 12. Cannot log in to the (continued)

Problem	Corrective action and solution
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.
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 “Controlling port number assignments” 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 12. Cannot log in to the (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 the portal server

Review the problems and resolutions when you have trouble with the connection to the 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 13. Cannot connect to Tivoli Enterprise Portal Server

Problem	**Resolution**
`KFWITM001W Unable to connect to Tivoli Enterprise Portal Server`	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 portal server attempts to validate the user ID entered in the browser. 2. Restart the database. 3. Attempt the log in again.
`KFWITM215E Unable to process logon request`	

Table 13. 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 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 host name might not resolve to the correct IP address on the local portal server host. To confirm that the host name resolves to the correct IP address, run the following command from the computer on which the 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 portal client is attempting to connect. For example, if your portal server is located on a host with the host name `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 the Tivoli Enterprise Portal Server	1. Select **Start** > **Programs** > **IBM Tivoli Monitoring** > **Manage Tivoli Enterprise Monitoring Services**. 2. Check that the portal server service (`KfwServices.exe`) is running and, if not, restart it. 3. If the portal server is started, see the `KFWRAS1.LOG` for any errors reported by the portal server application. After the portal server starts, an "`event ID 1: KFW0001 - 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 13. 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 portal server stopped and restart it:
	1. On the computer where the portal server is installed, select **Start** > **Programs** > **IBM Tivoli Monitoring** > **Manage Tivoli Enterprise Monitoring 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 portal server is started. Internal portal server commands display in the command prompt window.
	5. Verify that the portal server service is started. The 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 portal server.
	- If it is started, recycle the portal server.

If you are running the portal client in browser mode and reaching the portal server across network, the network system might not be able to resolve the host name.	Do the following on the computer where the 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 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 in 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, “Logs and data collection for troubleshooting,” on page 5 for information on what types of data to collect before contacting Support.

Dashboard data provider connection issues

A connection to the IBM Tivoli Monitoring dashboard data provider must be established in the Dashboard Application Services Hub before you can see data in the Infrastructure Management Dashboards or in custom dashboards.

Review the issues that you might encounter when establishing a connection to the dashboard data provider and viewing the Infrastructure Management Dashboards or custom dashboards.

A dashboard user encounters an ATKRST132E message

Problem

This error can occur while using the Dashboard Application Services Hub to create a connection to the Tivoli Enterprise Portal Server's dashboard data provider in an LDAP/SSO environment. With the **Use the credentials of the user (requires SSO Configuration)** check box selected, you might get an "ATKRST132E Error Message is 'unauthorized'" message after clicking **OK** to establish the connection.

If the connection attempt fails, all requests to the dashboard data provider include the user ID that was specified in the Connection Manager instead of the user ID of the currently logged-in user. As a result, authorization checks are likely to fail and dashboard views show no data.

Diagnoses and Solutions

Here are some possible explanations and solutions for the problem:

There are mismatched LTPA tokens between Dashboard Application Services Hub eWAS (embedded Websphere Application Server) and the Tivoli Enterprise Portal Server extended services (TEPS/e).

Ensure that you exported the LTPA key from the portal server and import the key into the Dashboard Application Services Hub. For more information, see "Importing and exporting LTPA keys" in the *IBM Tivoli Monitoring Administrator's Guide*.

There are mismatched LDAP realm names for the federated repository between the Dashboard Application Services Hub eWAS and the TEPS/e.

The Dashboard Application Services Hub server and portal server must be configured to use the same LDAP realm. Check the LDAP configuration of each server. For details on configuring LDAP for the Dashboard Application Services Hub, see the Jazz for Service Management Information Center (http://pic.dhe.ibm.com/infocenter/tivihelp/v3r1/topic/com.ibm.psc.doc_1.1.0/psc_ic-homepage.html); for details on configuring LDAP for the portal server, see "User authentication through the portal server" in the *IBM Tivoli Monitoring Administrator's Guide*.

An attempt was made to create an SSO-based connection with a user ID that isn't in the shared LDAP registry that the Dashboard Application Services Hub eWAS and the TEPS/e are authenticating against.

Ensure you are logged into Dashboard Application Services Hub with a user ID that is in the shared LDAP registry before attempting to create a connection to the dashboard data provider on the portal server.

It is possible that the LTPA token that is passed from the Dashboard Application Services Hub to the portal server has expired.

The LTPA token expiration can occur if the clock setting is different on each computer. Verify that the date, time, and time zone on the portal server computer and the Dashboard Application Services Hub computer are correctly set relative to Coordinated Universal Time (UTC). For example, the portal server in New York is set to UTC -5:00 and the Dashboard Application Services Hub in Paris is set to UTC+1:00.

Cannot launch the portal client on Windows XP after installation (message KFWITM215E)

After installing IBM Tivoli Monitoring, if you cannot start the Tivoli Enterprise Portal on a Windows XP system and get KFWITM215E message, you might need to adjust your Java settings or firewall configuration.

The message `KFWITM215E: Unable to process logon request occurs`. A firewall setting on the client computer prevents the client from connecting to the Tivoli Enterprise Portal Server. Set the IBM JVM (JavaVirtual Machine) as a trusted program to allow the 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 IBM Tivoli Monitoring components in the access control for the firewall.

Portal server is initializing and is not ready for communications

If you attempt to log in to the Tivoli Enterprise Portal Server, soon after it has started, it is possible the portal server is not ready for requests until initialization is complete.

The portal server is not ready for requests from the portal client until its process, `kfwservices.exe` is fully started. Keep the **Logon** window open and click **OK** after waiting a moment or two.

Portal server is unavailable during a portal client work session

If a message in the Tivoli Enterprise Portal indicates that the Tivoli Enterprise Portal Server is unavailable, suspend activity until a message indicates that the server is available.

When the Tivoli Enterprise Portal Server is available again, your client session is automatically reconnected and you can resume normal interactions.

- If you are running the portal client in browser mode and the portal server is available but the client does not reconnect after several minutes, exit the browser, restart the browser, and log on to the portal server again.
- If you are running the browser client and, from the same window or a tabbed window, log on to a different portal server, the disconnections might continue to occur and you must exit one of the work sessions. Complete one of the following steps to avoid intermittent disconnection:
  - Start another instance of the browser in the same way that you started the first instance, such as from the task bar.
  - Use two different browsers, such as Firefox and Internet Explorer.
  - Use two different portal client types, such as the browser client for one portal server and desktop client for a different portal server.

Portal server does not start after installation

If the Tivoli Enterprise Portal Server does not start after installation or upgrade, review the log files for the cause.

Check the following log files for messages that indicate why the Tivoli Enterprise Portal Server did not start:

kfwras1.log

Look for messages that indicate a failure during upgrade or that the hub Tivoli Enterprise Monitoring Automation Server did not connect.

*install_dir***cnps\sqllib\migrate.log**

Any error.

Portal server is not connecting with the hub monitoring server

If the Tivoli Enterprise Portal Server is not connecting to the hub Tivoli Enterprise Monitoring Server or it was connected and has lost the connection, review the possible causes and solutions for the symptoms you experience.

Tivoli Enterprise Portal Server lost contact with the Tivoli Enterprise Monitoring Server and is attempting to reconnect

This message displays when the portal server has lost its connection to the hub monitoring server, usually because the monitoring server stopped or is recycling. See also KFW_CMW_RECYCLE_DELAY.

Cannot reconnect to the Tivoli Enterprise Monitoring Server

This message is displayed after the monitoring server goes down and attempts to reconnect. The client attempts to log on once again to the session. After a successful logon, the user authorities that were in effect when the original logon occurred are compared with the current user authorities. If any permission is different, you must restart the portal client to ensure that all components are synchronized with your user permissions. Changes to user permissions include changes such as 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 monitoring server. When the 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 portal client session.

Portal server cannot connect to the AIX monitoring server private interface

If the hub monitoring server is installed on an AIX server with a public and a private interface, the portal server cannot connect to the hub. 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 14. 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`

Table 14. Control interface publishing (continued)

Interface control	Environment variable
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.	

Tivoli Enterprise Portal Server is not reconnecting
If the portal server does not reconnect to the hub, recycle the monitoring server and restart the portal server.

DB2 errors when opening a Tivoli Enterprise Portal workspace

If you are able to log in but receive an error message that you cannot open a workspace in the Tivoli Enterprise Portal, verify that the database agent and manager are working correctly. The configuration settings might need updating.

Before you begin

Before completing the steps below, verify with your database administrator that the following conditions 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 the 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.

Procedure

1. On the computer 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
```

What to do next

Restart the portal client.

A monitoring process fails to start on Linux or UNIX 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 and must satisfy certain requirements.

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.

Heartbeat issues when running 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 faster or slower than real world time. If any IBM Tivoli Monitoring products are installed on Linux guests whose clocks are not running correctly, the result can be erratic system behavior.

For example, if the Linux OS monitoring agent 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 because the heartbeats arrive after the time interval has expired.

The VMware company is aware of this issue, and has written several articles that address this problem. Search on “linux guest clock” in the . See also

How to tell if you have this problem:

A simple way for determining whether 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 product to behave erratically if the clock is not fixed.

Chapter 7. Portal client troubleshooting

Review the Tivoli Enterprise Portal troubleshooting symptoms to help you diagnose problems with the portal client.

Portal client startup

Review the Tivoli Enterprise Portal startup topics if the portal client does not start properly, you cannot log on, or you observe unusual behavior during startup.

No logon request in Firefox

If you are not prompted to log on to the Tivoli Enterprise Portal Server after starting the client, the Java plug-in might be disabled by the Firefox browser.

Symptom
After you start the Tivoli Enterprise Portal client in the Firefox browser, the title banner is shown, but the content area remains blank and no logon dialog or workspace is displayed.

Cause The Java plug-in might be disabled by the Firefox browser. Some releases of the IBM and Oracle Java plug-ins contained a reported security vulnerability that required Mozilla to block their execution under Firefox. The following web pages have more information about this issue:

More recent releases of the Oracle Java plug-in correct this problem, and the version of IBM Java shipped with IBM Tivoli Monitoring V6.3 (and later) also contains this fix.

Solution
Uninstall the version of Java that is disabled by Firefox; then install the version of IBM Java supplied with IBM Tivoli Monitoring V6.3, or install a more current version of the Oracle Java available from the Oracle website. If it is not possible to uninstall the version of Java, open the Firefox **Tools** > **Options** > **General** tab and click **Manage Add-ons** to re-enable the Java plug-in as described in the referenced web pages.

Oracle Java download page is displayed

If you have already installed Oracle Java, but the Oracle Java download page is displayed whenever you start the Tivoli Enterprise Portal browser client, you might have multiple Java plug-ins registered.

Symptom
Although the desired Java run-time was configured to use Oracle Java, and the installation of Oracle Java was successful, the Oracle Java download page continues to be shown whenever the Tivoli Enterprise Portal browser client is started.

Cause This problem can occur if you have more than one Java deployment plug-in (such as one from Oracle and another from IBM) registered and enabled in your browser, .

Solution

Check the browser's add-on or plug-in configuration panel to determine if more than one Java deployment entry is enabled. If this condition is found, use the browser's configuration panel to disable the conflicting add-on.

Note: Running Tivoli Enterprise Monitoring Agents at V6.1 and V6.2 on the same computer requires Java 1.4.2 and Java 1.5 on that computer. However, having multiple versions of Java installed on a Windows platform is not a best practice, especially if the browser client is being used on that computer. Refer to your monitoring agent user's guide or consult your administrator before implementing multiple versions of Java.

IBM Java 7 installation on Linux does not succeed

If the installation of IBM Java 7 or above on Linux using the supplied RPM package is unsuccessful, install from the supplied `.tar gzip` archive file.

Diagnosis

By default, if the Tivoli Enterprise Portal browser client on Linux detects that a supported version of Java is not installed, a hyperlink is offered to an RPM-based package containing IBM Java 7 or later. Depending on the configuration of your Linux environment, the RPM package installer might not be available, or installation of the package might not succeed.

Solution

Use the alternative `.tar gzip` archive file containing IBM Java supplied with IBM Tivoli Monitoring. For instructions, see “Method 2: retrieval and extraction of a Linux .tar gzip archive” under “Installing and configuring IBM Java 7” in the *IBM Tivoli Monitoring Installation and Setup Guide*.

Browser client startup on Linux using Firefox is not successful

Although the Java plug-in registration with Firefox was successful, you are not able to successfully start the Tivoli Enterprise Portal browser client.

Diagnosis

Use of the IBM Java plug-in might have been disabled by the Firefox browser on Linux. The plug-in must be enabled for use with the Tivoli Enterprise Portal browser client.

Resolution

1. Launch the Firefox browser on Linux and select **Tools** > **Add-ons**.
2. Select the **Plugins** section from the left-side navigation panel.
3. Locate the “IBM Java(TM) Plug-in” entry in the list. Click the **Enable** button to activate the plug-in.
4. Re-launch the browser client in Firefox.

The client should now launch successfully.

Java exception logging onto the browser client

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`.

"Do you want to run this application?" message when starting Java Web Start client

If you are launching the Tivoli Enterprise Portal Java Web Start client and get a “Security Information” warning message asking if you want to run the application, review the diagnosis and suggested response.

Problem

While launching the Java Web Start portal client, you get a “Security Information” message for the application named, “TEP - <TEPS_HOSTNAME>”. The message asks if you want to run the application.

Diagnosis

If you select the “More Information” link on the panel, there is a warning message about the jnlp deployment descriptor file being unsigned. This is not an error or security concern. All executable content associated with the portal client is digitally signed and verified by IBM.

Resolution

If you want to continue with the download and execution of the portal client, click **Run**. If you don't want to see this message again with subsequent launches of the portal client, select the “Always trust content from this publisher” check box and click **Run** to continue.

"Do you want to run this application?" security message when starting Java Web Start or browser client

If you are launching the Tivoli Enterprise Portal Java Web Start client or browser client and get a “Security Information” warning message asking if you want to run the application, review the diagnosis and suggested response.

Problem

While launching the Java Web Start portal client or browser client, you get a “Security Information” message for the application named, “TEP - <Resource Name>”. The message asks if you want to run the application.

Diagnosis

The code signing certificate that is associated with this downloaded resource has expired. Periodically, IBM renews the expiration date of the code signing certificate used to digitally sign all executable content associated with the Tivoli Enterprise Portal portal client. Occasionally, resource files used by the client that were introduced by Tivoli Monitoring applications shipped and installed independently of the Tivoli Monitoring base offering, were digitally signed using earlier code signing certificates. The digital signing with earlier certificates most often occurs when a new version of the Tivoli Monitoring base product is released, but up-leveled releases of Tivoli Monitoring applications signed with the updated certificates are not immediately available.

It is important to note here that there is no security exposure associated with these downloadable resources. The resources have already been digitally signed and verified by IBM. Typically, within a short period of time after release of the up-leveled version of the Tivoli Monitoring base product, the associated Tivoli Monitoring applications are published with downloadable resources containing non-expired certificates. At that point, this warning message is no longer displayed.

Resolution

If you want to continue with the download and execution of the portal client, click **Run**. If you don't want to see this message again with subsequent launches of the portal client, select the “Always trust content from this publisher” check box and click **Run** to continue.

"Do you want to install the following software?" message when starting Java Web Start or browser client

If you are launching the Tivoli Enterprise Portal Java Web Start client or browser client and get an “Install Java Extension” message, review the diagnosis and suggested response.

Problem

While launching the Java Web Start portal client or browser client, you get a “Install Java Extension” message. The message asks, “Do you want to install the following software?”, named “<Resource Name>”.

Diagnosis

More recent versions of Java check for the existence of certain constraints that are associated with the digital certificate used by IBM to digitally sign all executable content associated with the Tivoli Enterprise Portal client. In some cases, typically with older downloadable resources used by the client, not all these certificate constraints are present.

It is important to note that there is no security exposure associated with these downloadable resources. These resources have already been digitally signed and verified by IBM. The Tivoli Monitoring application associated with the downloadable resource should already have a version of the file that has been updated with all the required certificate constraints.

Resolution

If you want to continue with the download and execution of the portal client, click **Install**. Contact IBM Support for information on acquiring an updated version of the downloadable resource with all the required certificate constraints.

Certificate validation failure when starting Java Web Start client

If you are launching the Tivoli Enterprise Portal Java Web Start client and get a “Warning - Security” message about a failure to validate the certificate, review the diagnosis and suggested response.

Problem

While launching the Java Web Start, you get a “Warning - Security” message for “<Resource Name>”. The message is, “Failed to validate certificate. The application will not be executed.”. The Java Web Start client cannot be successfully started.

Diagnosis

More recent versions of Java check for the existence of certain constraints that are associated with the digital certificate used by IBM to digitally sign all executable content associated with the Tivoli Enterprise Portal client. In some cases, typically with older downloadable resources used by the client, not all these certificate constraints are present.

It is important to note that there is no security exposure associated with these downloadable resources. These resources have already been digitally signed and verified by IBM.

Resolution

Contact IBM Support for information on acquiring an updated version of the downloadable resource with all the required certificate constraints. Both the Tivoli Enterprise Portal desktop and browser clients can be used as alternatives to the Java Web Start client until IBM Support is able to resolve this issue to your satisfaction. (See “Viewing the IBM Support Portal” on page 2.)

"Do you want to run this application?" message when starting Java Web Start client

If you are launching the Tivoli Enterprise Portal Java Web Start client and get a “Security Information” warning message asking if you want to run the application, review the diagnosis and suggested response.

Problem

While launching the Java Web Start portal client, you get a “Security Information” message for the application named, “TEP - <TEPS_HOSTNAME>”. The message asks if you want to run the application.

Diagnosis

If you select the “More Information” link on the panel, there is a warning message about the jnlp deployment descriptor file being unsigned. This is not an error or security concern. All executable content associated with the portal client is digitally signed and verified by IBM.

Resolution

If you want to continue with the download and execution of the portal client, click **Run**. If you don't want to see this message again with subsequent launches of the portal client, select the “Always trust content from this publisher” check box and click **Run** to continue.

Java discovered application components that could indicate a security concern

While using the Tivoli Enterprise Portal browser client V6.3 or later, you might get a warning message that Java has discovered application components that could indicate a security concern. You can safely answer **No** to unblock them.

IBM Java 7 is the preferred default version of Java being shipped with IBM Tivoli MonitoringV6.3 or later. It is possible to get a warning message when you start the browser client if there are application support files that contain unsigned content. These support files typically contain text for areas of the portal client where application-level information is displayed, such as the Physical Navigator view and predefined workspaces.

IBM Java 7 detects the use of downloaded files with unsigned content and, if found, provides a warning message. In the context of the portal client, you must answer **No** to enable the content. Otherwise, the blocked content disables certain portal client displayed text. This typically happens with older versions of the monitoring agents, whereby the application support is at an older level and the code security certificate might have expired.

Portal desktop client called from Java Web Start does not work properly after adding agent support

Review the symptom and possible solution if the Java Web Start-installed Tivoli Enterprise Portal client is getting errors after installing agent application support on the Tivoli Enterprise Portal Server.

Symptom

After starting the portal desktop client, you get a Java exception and an "unable to load resource" message with an accompanying file name.

Solution

1. Exit the portal desktop client if you are logged on.
2. Start Manage Tivoli Enterprise Monitoring Services as described in "Starting Manage Tivoli Enterprise Monitoring Services" on page 3.
3. Right-click Tivoli Enterprise Portal Server and take one of the following steps.

   Windows Click **Reconfigure**, and click **OK** twice to accept the existing configuration.

   Linux UNIX Click **Configure** and accept the defaults settings when prompted for configuration choices.
4. After finalizing the configuration, restart the portal server.
5. Restart the portal desktop client through the Java Web Start

Portal desktop client does not work when exporting DISPLAY

If the Tivoli Enterprise Portal desktop does not work when exporting the DISPLAY from a Linux system to a Windows system running cygwin, edit the portal client startup script for the Java location.

About this task

If you review the log for the Tivoli Enterprise Portal desktop client on the Linux system, `*install_dir*/logs/kcjras1.log`, you see the following error:

```
EXCEPTION: Attempting to load home workspace:
java.lang.IllegalArgumentException: Width (0) and height (0)
```

Take one of the following steps to edit the `cnp.sh` startup file:

Procedure

- Add the Java system property, "`-Dawt.toolkit=sun.awt.motif.MToolkit`":
  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=... .

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.

Logon name not accepted after hub monitoring server change

If the Tivoli Enterprise Portal Server was reconfigured from connecting to a hub Tivoli Enterprise Monitoring Server platform that accepts mixed casing like Linux or UNIX to connecting to a hub platform that requires uppercase letters like Windows, logon credentials can fail.

Problem

A Linux portal server was reconfigured from connecting to a Linux hub monitoring server to connecting to a Windows hub. The users had names such as user1, user2, and so on. After the reconfiguration, the users cannot log on. If you log in to the portal client with the administrator ID, you can see the users in the Administer Users panel. However, when you select a user, an error is displayed that indicate the user is no longer in the user database.

Solution

Recreate the user IDs.

Using an administrator name with non-latin1 characters, cannot log onto the Tivoli Enterprise Portal

About this task

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** > **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.

On an Active Directory Server, sysadmin cannot logon to the Tivoli Enterprise Portal client

About this task

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.

Workspaces

Workspaces display queried data from the monitoring agents that are installed on your monitoring network and from the Tivoli Enterprise Monitoring Servers and Tivoli Enterprise Portal Server. If you observe unusual behavior, get errors, or get no workspace at all, review the possible causes and solutions.

Workspaces opened in browser tabs are not displayed correctly

When running the Tivoli Enterprise Portal in browser mode, you can open multiple workspaces in new tabbed windows. If you don't see the selected workspace or it is not successfully initialized and reporting data, review the solution that corresponds to your problem.

Workspace opened in a new browser tab

Problem

When a workspace is opened in a new browser tab, sometimes the workspace is not displayed.

Diagnosis

For browsers that support viewing pages using tabs, the Tivoli Enterprise Portal supports the ability to open a workspace in a tab by holding the CTRL+SHIFT keys down while you select a workspace from the Navigator view or from any point in the portal where workspace selection is supported. This feature, however, is not reliable if you have configured your browser to use Java 5, or to use Java 6 with the browser plug-in configured for "classic" mode.

Solution

Use IBM Java 7 configured with the next-generation Java plug-in. The version of IBM Java 6 that is delivered with IBM Tivoli Monitoring V6.2.3 FP1 and later automatically defaults to use the next-generation Java plug-in. To verify that the next-generation Java plug-in is registered with your browser, use the following procedure for the platform you are using with the browser client: Windows

1. Select **Start** > **Control Panel**. (On the Windows 7 Control Panel, you might need to change the **View by** selection to show icons to see the Java control panel.)
2. Double-click **IBM Control Panel for Java**. (Click the **Java** tab and click **View** to see the Java Runtime Environment Settings and confirm that the version is 1.6).
3. In the Java control panel, select the **Advanced** tab, expand the **Java Plug-in** branch, and make sure the ☑ **Enable the next-generation Java Plug-in** is selected.
4. Click **Apply** to save your changes, and press **OK** to close the Java control panel.
5. Restart the browser for any Java plug-in change to take effect.

Linux UNIX

1. Open a shell prompt and locate the `plugins` directory associated with your Firefox browser (such as `/usr/lib/mozilla/plugins`). If IBM Java 7 is installed and the next-generation Java plug-in is registered with your Firefox browser, the following shared object file link should be present in the Firefox `/plugins` directory: `libnpjp2.so`. If a link to this file is not in the Firefox `/plugins` directory, continue with the following steps to register the Java plug-in.
2. If the `/plugins` directory has no `libnpjp2.so` file link, but does have a `libjavaplugin_oji.so` link, delete the link with the following command (might require root authority to execute):

   ```
   rm -f libjavaplugin_oji.so
   ```

   The `libjavaplugin_oji.so` file is the link associated with the "classic" Java plug-in and must be removed before attempting to register the next-generation Java plug-in.
3. Register the next-generation Java plug-in by creating a symbolic link to the correct plug-in file using the following command, which assumes that IBM Java 7 was installed in the default directory):

   ```
   ln -s /opt/ibm/java-i386-60/jre/lib/i386/libnpjp2.so
   ```

Browser started with workspaces opened in multiple tabs

Problem

When the browser is opened with multiple workspace tabs, not all the workspaces in those tabs successfully initialize and display data.

Diagnosis

The Tivoli Enterprise Portal browser client does not support the concurrent opening of multiple tabbed workspaces.

Solution

Before closing the browser, make sure that all the Tivoli Enterprise Portal workspace tabs are closed out after terminating the client by selecting the **Logout** link or clicking **File** > **Exit**.

Some browsers support the concept of a tab group, which combines multiple tabbed pages under a single name. The tabbed pages in this group can then be opened and closed as a single set of pages. The browser client does not support tab groups; workspaces should not be included in groups for the purpose of opening and closing them as a set.

CTRL+SHIFT was used to open a tabbed workspace

Problem

You used CTRL+SHIFT to open a workspace in a new tab, but the target workspace does not render successfully or the tab is not selected or given the current keyboard focus.

Diagnosis

Support for tabbed workspaces is less reliable when running the Tivoli Enterprise Portal browser client using Java 1.5 or Java 1.6 in “classic” mode.

Solution

Upgrade the version of Java used with the Tivoli Enterprise Portal browser client to 1.6, configured to use the next-generation Java plug-in. See “Installing IBM Tivoli Monitoring” > Configuring clients, browsers, and JREs, Browser clients > Browser plug-in support for Java applet in the *IBM Tivoli Monitoring Installation and Setup Guide* for information on installing Java 1.6, and “Workspace opened in a new browser tab” on page 142 for information on using the next-generation plug-in.

Tabbed workspace opened in Microsoft Internet Explorer

Problem

When a workspace is opened in a new tab of Microsoft Internet Explorer browser, the new tab is not always given the current keyboard focus automatically and you must manually select the tab.

Diagnosis

For Internet Explorer v8 and v9, this is the default behavior for tabbed windows.

Solution

Using the **Tabbed Browsing Settings** panel in **Tools** > **Internet Options** > **Tabs Settings**, confirm that the ☑ **Always switch to new tabs when they are created** check box option is enabled, and click **OK** on all the opened dialog panels to save the change. The workspaces you open in new tabs should now automatically receive the current keyboard focus, and their contents are displayed.

Data in the portal client is missing and you receive an error

If no data is displayed in a workspace from a monitoring agent on a 64-bit system and you get a `KFWITM217E - SQL1_CreateRequest failed, rc=209` error, check that application support has been added.

Problem
You open a workspace and one or more of the query-based views shows no data and a `SQL1_CreateRequest` error is displayed in the status bar.

Cause The catalog and attribute (cat and atr) files that are installed with application support for a monitoring agent are required for presenting workspaces, online help, and expert advice in the Tivoli Enterprise Portal. It is possible that the hub or remote Tivoli Enterprise Monitoring Server, the Tivoli Enterprise Portal Server, or the desktop client (not if installed with Java Web Start) is missing application support for the monitoring agent.

Solution
Ensure that the hub and remote monitoring servers have application support applied for the monitoring agents that connect to them. See the application support topics under “Installing IBM Tivoli Monitoring” in the *IBM Tivoli Monitoring Installation and Setup Guide* for more information about application support.

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.

Link from Managed System Status workspace

If you get a `KFWITM217E - SQL1_CreateRequest failed, rc=209` error after selecting the Historical Export Statistics workspace link, check that the Tivoli Enterprise Monitoring Server is at V6.3 or later.

Problem
While displaying the Enterprise-level workspace, Managed System Status, you right-click the 🔗 link and select the Historical Export Statistics workspace. Instead of the workspace for the selected managed system opening, you get a `KFWITM217E - SQL1_CreateRequest failed, rc=209` error.

Cause The application support for the monitoring server that the managed system connects to is not at Tivoli Monitoring V6.3 or later.

Solution
Upgrade the monitoring server to V6.3 or later. For more information, see “Workspaces are missing or views are empty” on page 12 and, in the *IBM Tivoli Monitoring Installation and Setup Guide*, see “Upgrading from a previous installation”.

Historical data

Historical reporting is available for any attribute group that has historical data collection configured and started on the associated managed systems. Review the troubleshooting topics for issues with displaying or collecting historical data.

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.

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.

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.

Historical Collection Configuration window error 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 window displays a failure message.

```
Cannot load Product Configuration data
KFWITM220E Request failed during execution
```

About this task

To remedy this issue, take the following steps.

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.

Situations

Review the Tivoli Enterprise Portal situation troubleshooting scenarios for situations to find a solution to situation and event related problems.

Situations are not firing

About this task

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 an item in the Tivoli Enterprise Portal Navigator view.
- Ensure that the situation condition is true.
- Check the operations log of the agent.

Restarting a situation for pure event does not clear it from console

The Tivoli Enterprise Portal situation event console shows a pure event with an Open status even after the situation that triggered the event has been restarted.

Symptom
A situation that uses attributes that cannot be sampled, those that have no value until something happens, opens a *pure event* when it becomes true. The situation was restarted, but the event still shows with a status of “Open” in the situation event console.

Cause Pure events are not closed automatically like sampled events; they must be closed manually unless an UNTIL clause is included in the situation definition.

Solution
Manually close the pure event or adjust the settings of the following Tivoli Enterprise Portal Server environment variables:

1. KFW_CMW_SITUATION_ADMIN_SUPPRESS=N to prevent an event from appearing in the situation event console after its situation was stopped.
2. KFW_CMW_SITUATION_FANOUT_SUPPRESS=N to prevent the broadcasting of events from situations that have been stopped.

See also “Environment variables” in the *IBM Tivoli Monitoring Installation and Setup Guide*; and “Adding an Until modifier” (Reset Interval Expires option) in the *Tivoli Enterprise Portal User’s Guide*.

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
```

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.

Installation of situation data fails due to I/O on VSAM data sets

About this task

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 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*.

Browser client on multiple monitors

The Tivoli Enterprise Portal client supports multiple monitor configurations.

In a multiple monitor environment, if you move the browser client between monitors, the dialog boxes and messages might not always appear in the same monitor.

Take any of the following actions to synchronize the browser client window and dialog boxes so that they appear on the same monitor:

- Restart the browser client in the monitor that you want to work in.
- Switch to a different workspace.
- Reload the current page (press F5) after moving the browser window to the desired monitor.

Help is not displayed

If the Tivoli Enterprise Portal help does not display when you select if from the Help menu, check your browser settings.

Software to block pop-up ad windows

If the browser toolbar has a software to block pop-up ad windows running, the help does not open whether you select **Help** > **Contents and Index** in the Tivoli Enterprise Portal or click **Help** in a window. Turn off the software to block pop-up ad windows.

On Microsoft Internet Explorer, if “Temporarily Allow Pop-ups” is enabled, change the setting to “Always Allow Pop-ups”.

Internet Explorer shortcut keys the same for the 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, you get help for the Internet Explorer displays instead. Select **Help** > **Contents and Index** from the Tivoli Enterprise Portal menu bar.

Data is not returned to the portal client

If data is not returning to the Tivoli Enterprise Portal, review the possible solutions.

Do the following to ensure that data can return to the Tivoli Enterprise Portal:

- 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)
  ```

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.

Monitoring agents show in an unexpected position in the Navigator

The Tivoli Enterprise Portal Navigator view represents all the monitoring agents in the environment with a top level of "Enterprise".

The default presentation assumes that each monitoring agent type comes from a different IP address and host name. When that is not true, the monitoring agent displays 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.

Additionally, Navigator items are ordered internally on the Tivoli Enterprise Portal and therefore might not reflect a logical ordering in any particular language.

Changes to the agent environment variable **`CTIRA_HOSTNAME`** affect the display name in the workspace but not within the Navigator view. Here is an explanation of how to configure the Tivoli Enterprise Portal Server for desired navigator item display. The portal server has a configuration environment variable that changes the Navigator to depend on the host name instead of the IP address: **`KFW_TOPOLOGY_CLUSTER_LIST`**. This variable is added to *`install_dir`*`\cnps\kfwenv` file in Windows or *`install_dir`*`/config/cq.ini` in Linux and UNIX. Its purpose is to force dependence on the host name 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 host name logic should apply. Here are some affinities for monitoring agents distributed with IBM Tivoli Monitoring:

```
AFF_NT_SYSTEM                  "Windows OS"
AFF_ALL_UNIX                   "UNIX OS"
AFF_LINUX_SYSTEM               "Linux OS"
```

As an example, if you needed to use the host name for Navigator positioning of your Linux OS and UNIX OS 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 `*install_dir*\cnps\affinity.properties` in Windows or `*install_dir*/installdir/arch/cq/data/affinity.properties` in Linux of UNIX. 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. 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 host name, 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 host name instead of the TCP/IP host name.
- Some agents require a different mechanism to change the apparent host name. In the case of the WebSphere MQ Monitoring Agent, for example (AFF_MVS_MQM), update the `mq.cfg` file and add:

  ```
  SET AGENT NAME(hostname)
  ```
- Long host names can create confusion, such as when a host name 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 (*install_dir*\cnps\kfwenv or *install_dir*/config/cq.ini):

```
KFW_TOPOLOGY_KEEP_DOT_IN_NODE_NAMES=Y
```

- Remember, the managed system names are limited to 32 characters, therefore, the *hostname:product* can be truncated and cause accidental duplications. That would be another case where you would need to set the **CTIRA_HOSTNAME**.

HEAPDUMPs and JAVACore files are placed on desktops when running in browser mode

About this task

The Tivoli Enterprise Portal client uses the IBM Java Plug-in, which is automatically installed on your computer with the portal client. 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:

Procedure

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.

Results

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.

Category and Message field of the universal message does not accept DBCS

About this task

To record a DBCS IBM Tivoli Monitoring universal message when a situation is true, following these steps on the Tivoli Enterprise Portal:

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 the last step, 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).

Agents display offline in the portal client but they are still started

The Tivoli Enterprise Portal Navigator Physical view shows that some monitoring agents are offline, but the situations continue to be sampled and agent logs show them to be 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 monitoring agents must include a specific definition for correct agent host names.

Browser client locale configuration

Starting with IBM Tivoli Monitoring V6.3, the administrator can no longer set the locale for the Tivoli Enterprise Portal browser client. The language must be changed through the Java control panel at the client computer.

Problem

When using the portal browser client, the locale is the same as what is set for the operating system. If you normally use a different language for working with the browser client than what the operating system is set for, the browser client no longer shows that language.

Cause

The administrator was able to set the locale of the portal browser client on Tivoli Monitoring versions prior to V6.3 by editing the parameters in the Manage Tivoli Enterprise Monitoring Services utility. The next-generation Java plug-in technology (Java 7 and later), employed by Tivoli Monitoring V6.3 and later, does not allow the portal client parameters **user.language** and **user.region** that were supported by previous Java versions to be passed to the portal client applet.

Solution

Enable the locale of your choosing by adding user properties to the Java plug-in or reconfigure the operating system language settings:

- Add the **user.language** and **user.region** parameters to the Java Control Panel as JVM arguments, which affects all applications that run in the browser. To specify the French locale, for example, add the following two system properties as JVM arguments using the control panel on the computer where the browser is being used:

  ```
  -Duser.language=fr -Duser.region=FR
  ```

  For more information, see the **user.language** and **user.region** parameters in the "Portal client parameter list" in the *IBM Tivoli Monitoring Administrator's Guide*.

- Reconfigure the operating system for the desired locale, which affects all applications on the computer:

  Windows Use the Windows Control Panel (Region and Language) to establish the default locale.

  Linux It depends somewhat on the Linux distribution being used, and involves updating some system-wide environment variables such as **LANG** and **LANGUAGE**.

  When the JVM is launched, it defaults to using the locale configured for the host operating system environment.

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. Portal server troubleshooting

Review the Tivoli Enterprise Portal Servertroubleshooting topics for help with solving problems you encounter with the portal server.

If you do not find the resolution to your problem, review the topics in Chapter 6, “Connectivity troubleshooting,” on page 123.

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 on as sysadmin with portal server LDAP enabled

When LDAP authentication is enabled for the Tivoli Enterprise Monitoring Server, the `sysadmin` ID must be defined in the LDAP server. However, when LDAP is enabled for the Tivoli Enterprise 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 host name

Edit the resulting xml file and change the shortname to the fully qualified host name.

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.

About this task

If you do not want to use Secure Socket Layer communication between 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

About this task

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 in the .

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.

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 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 portal server

The eWAS subcomponent of the Tivoli Enterprise Portal Server , named Tivoli Enterprise Portal Server extension server (TEPS/e) is installed automatically with the portal server. If you need to start or stop the application server instance of eWAS on which the portal server is running, you must do it by starting or stopping the 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 Monitoring Administrator's Guide* for recovery instructions.

Setting the TEPS/e maximum heap size

When the dashboard data provider has been enabled on the Tivoli Enterprise Portal Server, you can use monitoring dashboards in the Dashboard Application Services Hub console. In larger environments, it is possible for the Tivoli Enterprise Portal Server extended services (TEPS/e) Java process to run out of memory when large amounts of data are passed to the Dashboard Application Services Hub.

You can increase the maximum heap size of the TEPS/e JRE to improve server response time and better accommodate a larger monitored environment.

Before you begin

The memory required by the TEPS/e depends on the size of the monitoring environment and on the Java heap size parameters. The default maximum Java heap size is 1500 MB, which is appropriate for 32-bit systems. On 64-bit systems, if you encounter "out of memory" exceptions, you can increase the maximum heap size of the TEPS/e JRE to values greater than 1500 MB to allow more memory usage and accommodate a larger monitored environment.

About this task

Complete the following steps on the computer where the portal server is installed to adjust the TEPS/e maximum heap size.

Procedure

1. At the command prompt, change to the bin directory of your Tivoli Monitoring installation:
   - Windows *install_dir*\cnpsj\profiles\ITMProfile\bin
   - Linux UNIX *install_dir*/*platform*/iw/profiles/ITMProfile/bin
2. Enter the following command to start the eWAS console:
   - Windows **wsadmin.bat**
   - Linux UNIX **wsadmin.sh**
3. At the wsadmin prompt, enter the following command: `$AdminConfig modify [$AdminConfig list JavaVirtualMachine] "{maximumHeapSize 2000}"`
4. Enter the following command to save your changes: `$AdminConfig save`
5. Enter the following command to exit: `quit`

What to do next

Restart the portal server. If you continue to encounter "out of memory" exceptions, try increasing the maximum heap size again.

Chapter 9. Monitoring server troubleshooting

Review the Tivoli Enterprise Monitoring Server topics for help with troubleshooting errors related to the monitoring server.

Related concepts:

Chapter 14, “Command troubleshooting,” on page 251

Installed packages exceed the 512 maximum

If the Tivoli Enterprise Monitoring Server does not start and you receive a message that the number of install packages exceeds the maximum of 512, you must install an uninitialized definition file.

Cause There is a limit of 512 catalog and attribute files that can reside on a monitoring server. After this limit is reached the monitoring server does not start. Deleting older catalog and attribute files does not resolve this issue.

Solution

The only way to resolve this issue is to install an uninitialized `QA1CDSCA` definition file. You can request an unitialized QA1CDSCA definition file from IBM Support staff. Installing the uninitialized `qa1cdsca.def` file creates a new `QA1CDSCA.IDX` and `QA1CDSCA.DB`, which causes the monitoring server to extend the space used for application definitions. After obtaining the `qa1cdsca.def` file, do the following:

1. Save or back up the following files to a safe place: `QA1CDSCA.DB` and `QA1CDSCA.IDX`.
2. Remove the older catalog products (.CAT files) from the following location:
   - Windows c:\ibm\itm\cms\RKDSCATL
   - Linux UNIX /opt/IBM/ITM/tables/*tems_name*/RKDSCATL
3. Create a `TEMP` directory.
4. Copy `qa1cdsca.def` to the `TEMP` directory.
5. Change to the `TEMP` directory and run `kgldbutl.exe` from `TEMP`:
   - Windows c:\ibm\itm\cms\kgldbutl.exe < qa1cdsca.def
   - Linux UNIX /opt/IBM/ITM/*arch*/ms/bin/kgldbutl.exe < qa1cdsca.def (where *arch* is the operating system on which the monitoring server is installed).

   You can see the following output as the files are created:

   ```
   Enter DataBase Utility Command
   Enter DataBase Utility Command
   DataBase file QA1CDSCA created
   Enter DataBase Utility Command
   Index PrimaryIndex,U for database QA1CDSCA created
   Enter DataBase Utility Command
   ```
6. Copy `QA1CDSCA.IDX` and `QA1CDSCA.DB` to the monitoring server directory:
   - Windows c:\ibm\itm\cms
   - Linux UNIX /opt/IBM/ITM/tables/*tems_name*
7. Start the monitoring server.

After the monitoring server starts, a new QA1CDSCA.IDX and QA1CDSCA.DB is created based on the number of currently defined catalog and attribute files.

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 monitoring server problems on distributed systems

The problems described in this section might occur on distributed systems. For information about configuring theTivoli Enterprise Monitoring Server, refer to the *IBM Tivoli Monitoring Installation and Setup Guide* .

SOAP command failures

Review the SOAP command problems that are due to the configuration of or conditions on the Tivoli Enterprise Monitoring Server.

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

All versions of Tivoli Monitoring that incorporate the IBM Tivoli Directory Server Client at the Tivoli Enterprise 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

About this task

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.

High virtual memory usage on Linux 64-bit systems

On 64-bit Linux systems, users who are switching from 32-bit to 64-bit Tivoli Monitoring processes will observe that the 64-bit ITM processes might use more memory than their corresponding 32-bit Tivoli Monitoring processes.

The Linux runtime libraries determine how memory is allocated when Tivoli Monitoring processes request RAM. Tivoli Monitoring does not have control over these algorithms. It has been observed that 64-bit Tivoli Monitoring products might have higher virtual memory usage on Linux systems with large amounts of RAM than on systems with smaller amounts of RAM. This is a Linux system determination.

For more information, see the “Virtual Memory Manager” topic in the Redpaper, *Linux Performance Tuning Guidelines* (http://www.redbooks.ibm.com/redpapers/pdfs/redp4285.pdf).

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.

Monitoring server application support completes all seeding functions but might crash as the program is exiting

The Tivoli Enterprise Monitoring Server seeding program that adds 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 monitoring server application support was added successfully. Since all seeding functions were completed, the 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 monitoring server seeding output files contain 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)`

```
0B000000000000000100000000000000F84CD256887CAE56E8F400570000000048010000EE5
DB656B88B9655A4F700572200000022000000000000000D8F900572CF800578C81C056ACEF00
57C04DD256484DD2563EB4B656C04DD2560000000000F500570100000000000000200000000
2000000879D8B558C81C056A8EF0057
```

The expected seeding completion messages will follow the crash message. The normal seeding messages are checked by the Tivoli Monitoring configuration tool for successful completion of all seeding functions. The crash message always appears in the monitoring server seeding output even if a core or dump file is not produced.

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 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 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.

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.

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).

Monitoring server fails to start, but then does after a reboot

When the Tivoli Enterprise Monitoring Server does not start up properly and you see the following messages in the 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 Tivoli Monitoring processes that might be bound to this port.

Remote monitoring server lost connection to the hub 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 Servers with another time server. Restart the 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 monitoring server during hub failover to Hot Standby

The Tivoli Enterprise 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 monitoring servers are down when they are up

The statusPut process fails periodically, resulting in an incorrect hub Tivoli Enterprise Monitoring Server 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

About this task

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.

Kshsoap client failure on UNIX-based systems

The Tivoli Enterprise Monitoring Server includes a command line utility called *kshsoap*. If the kshsoap http client fails on your UNIX-based system, review the possible cause and solution.

Problem

The kshsoap client fails because of missing libraries on UNIX-based systems. The monitoring server configuration settings must be incorporated into your current shell before you invoke the kshsoap client.

Solution

At the command line, enter `.` *`install_dir`*`/config/`*`hostname`*`_ms_`*`temsname`*`.config`.

To verify this step, you can use the **`*env*`** command to show your environment variables and compare the entries to those in the `.config` file.

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 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 monitoring server entry disrupts them from communicating at all.

When the problem occurs, make sure the hub monitoring server started under the non-root login is not running. Then recycle whichever process shows up first on the Service Index page.

tacmd login fails when monitoring server is configured with LDAP authentication

About this task

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.

Correcting tacmd login error after failover to standby monitoring server

After successfully logging in to the CLI with **tacmd login**, you can no longer log in with the same ID. The user ID being unrecognized can occur in a hot standby environment when the login is to a Tivoli Enterprise Monitoring Server that then goes offline and the hot standby monitoring server is activated. On the monitoring server that you cannot log in to, edit the settings in the Tivoli Monitoring Web Services SOAP server kshxhubs.xml file.

For example, after failover to the standby server, the **tacmd login -s myserver -u sysadmin -t 1440** command returns the following error:

```
Validating user...
KUIC00006E: The specified user name or password is incorrect.
You are not logged in because you specified an incorrect user name or password
or you do not have permission to log in.
Verify the correct user name and password and that you have permission to log in.
```

Procedure

1. On the monitoring server computer that you cannot log in to, open the kshxhubs.xml file in a text editor.
2. Change the setting for <CMS_Name> to specify the IP address. For example, from <CMS_Name>ip.pipe:hub_myserver[1918]</CMS_Name> to <CMS_Name>ip.pipe:9.11.10.188</CMS_Name>.
3. Save and close the kshxhubs.xml file.
4. Restart the monitoring server.

Results

The **tacmd login** command to the server completes successfully if you enter a valid user ID and password.

Tacmd login command fails with error KUIC00017E

If the tacmd login fails with error KUIC00017E even though the hot standby mirror Tivoli Enterprise Monitoring Server is not running, review the cause and solution.

Problem
The **tacmd login** fails with the following error even though standby mirror monitoring server is not running: `KUIC00017E: tacmd is not allowed to connect to a secondary Hub. A secondary HUB has been specified instead of the primary Hub. Please, retry with the primary Hub.`

When the mirror is configured, but is not yet running, this error might occur if you issue the **tacmd login** command immediately after the hub monitoring server is started.

Cause The hub monitoring server has not yet finished initializing its hot standby facility. The KUIC00017E error message is returned instead of a message informing you that the hub has not yet completed its initialization.

Solution

Retry the **`tacmd login`** command after waiting a few seconds for the hub monitoring server to complete its startup. The login should then work properly.

In a hot standby (FTO) environment, commands to a mirror hub might not return hub records after reconnection

Redirect commands to the current hub Tivoli Enterprise Monitoring Server when running the `tacmd listappinstallrecs` command in a hot standby environment

The `tacmd listappinstallrecs` command returns the application support installation records and displays the current self-describing agent product installation status for all Tivoli Enterprise Monitoring Servers in the environment. This command connects to each online monitoring server one-by-one and retrieves the installation records. The command cannot return data for offline monitoring servers.

The mirror hub does not keep accurate node status of any endpoint, whether hub or remote monitoring server. As the `tacmd listappinstallrecs` command presents install records for any monitoring server, if you issue at a mirror, the acting hub might or might not be omitted (as well as any remote monitoring servers in the installation).

Best practice is to run the commands on the current hub.

A deleted object is redisplayed when two hot standby (FTO) hubs reconnect

You might notice that a deleted object, such as a situation or policy, is redisplayed when two FTO hub Tivoli Enterprise Monitoring Servers reconnect. This behavior occurs when the mirror hub has been promoted to serve as the acting hub before reconnecting.

An example of a deleted object is a situation, policy, SDA option, override, or calendar. Either of the following scenarios demonstrates this behavior:

Role switch

The acting hub and mirror were connected initially, and the hub is stopped. The mirror becomes the new acting hub. An object is deleted from the new hub. The original hub is started and becomes the new mirror. Shortly after reconnection, the deleted object reappears on the new hub.

Temporary disconnect

The hub and mirror were connected initially and then lost connection. The disruption lasts long enough for the mirror to promote itself to the role of acting hub. While still disconnected, an object is deleted from the original hub. When the connection is restored, the object reappears on the original hub. The object does not reappear if the mirror had not promoted itself.

Troubleshooting monitoring server problems on z/OS systems

Review the problems you might experience with Tivoli Enterprise Monitoring Server on z/OS and the provided resolutions.

These are problems that occur during runtime that you can resolve with the .

For more information about configuring the monitoring server on z/OS, see *Configuring the Tivoli Enterprise Monitoring Server on z/OS* (http://pic.dhe.ibm.com/infocenter/tivihelp/v61r1/topic/com.ibm.omegamon_share.doc_6.3.0.1/ztemsconfig/ztemsconfig.htm).

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

About this task

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.

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 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

About this task

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)

About this task

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. Automation server troubleshooting

Review the Tivoli Enterprise Monitoring Automation Server topics for help with troubleshooting errors related to the automation server.

Note: If you revert your Registry Services for IBM Jazz™ for Service Management environment or the associated Registry Services database (FRSDB) to a prior state, you must stop and restart any and all running automation servers. Otherwise, any currently running automation server will not be known as a registered service provider, resulting in Registry Services rejecting any HTTP requests made by the automation server.

Log and environment files

Review the MSG2 log file to help diagnose problems related to the Tivoli Enterprise Monitoring Automation Server. You can also review and edit the environment variables to optimize automation server performance.

Log file

The automation server MSG2 log file can help you to isolate where problems might be occurring.

Windows *install_dir*\logs\kasmain.msg

Linux UNIX *install_dir*/logs/*hostname*_AS_*timestamp*.log where *hostname* is the name of the computer where the automation server is installed, and *timestamp* is the log time stamp in hexadecimal.

Environment file

You can edit the automation server environment file from the Manage Tivoli Enterprise Monitoring Services utility or from the command line.

Manage Tivoli Enterprise Monitoring Services

1. Stop the automation server.
2. Start Manage Tivoli Enterprise Monitoring Services using one of the following methods:

   Windows Click **Start** > **Programs** > **IBM Tivoli Monitoring** > **Manage Tivoli Enterprise Monitoring Services**

   Linux UNIX Change to the *install_dir*/bin directory and run ./itmcmd manage [-h *install_dir*]
3. Right-click the Tivoli Enterprise Monitoring Automation Server and select **Advanced** > **Edit ENV File**.
4. After you save and close the environment file, restart the automation server for the changes to take effect.

Command line

1. Stop the automation server.
2. Change to the configuration directory for your operating system and open the following environment file in a text editor:

   Windows *install_dir*\CAS\BIN\KASENV

   Linux UNIX *install_dir*/config/as.ini
3. Restart the automation server.

Note In federated registry environments, the default timeout values might not be sufficient. These are the relevant environment variables. They all have a default timeout value of 120 seconds, which can be adjusted from 15 seconds to 900 seconds:

`KAS_REGISTRY_SERVICES_TIMEOUT_DELETE` sets the HTTP/S DELETE timeout

`KAS_REGISTRY_SERVICES_TIMEOUT_GET` sets the HTTP/S GET timeout

`KAS_REGISTRY_SERVICES_TIMEOUT_POST` sets the HTTP/S POST timeout

For the debugging variable trace settings, see "Setting the trace option for the automation server" on page 50. For a complete list of the automation server environment, see "Tivoli Enterprise Monitoring Automation Server environment variables" in the *IBM Tivoli Monitoring Installation and Setup Guide*.

OSLC-PM service provider fails to connect to Registry Services application

The Open Services Lifecycle Collaboration Performance Monitoring (OSLC-PM) service provider HTTPS connection to the Registry Services application can fail in many ways. Review the possible causes and solutions.

Problem

Connection problems can occur with an HTTPS connection, including the following common connection errors:

- WebSphere Application Server for the Registry Services application is not running
- Registry Services application is not running
- Network outages
- OSLC-PM service provider entries in the Tivoli Enterprise Monitoring Automation Server configuration file have an incorrect or missing protocol for connecting to Registry Services
- OSLC-PM service provider entries in the automation server configuration file have an incorrect host name or IP address that is specified for Registry Services
- OSLC-PM service provider entries in the automation server configuration file have an incorrect port specification for connecting to Registry Services
- OSLC-PM service provider entries in the automation server configuration file have an incorrect or missing user ID or password, or both, that is specified for Registry Services

Diagnosis

You can see OSLC-PM service provider error messages in the automation server MSG2 log file that can help you to isolate where the problem might be occurring. (See "Log and environment files" on page 181 for the file path.)

After you resolve and rule out the common connection issues, investigate further by reviewing the service provider entries in the automation server RAS1 trace file. Search the RAS1 trace file for `KDH1 status` error messages. The most common connection error is KDH1 status `URI authority not` found. This error occurs when the OSLC-PM service provider cannot communicate with the Registry Services application. A sample error message is:

```
(NNNNNNNNN.NNNN-NNN:kassoap.cpp,929,"sendSoapHTTPRequest") KDH1 status
<0x7C4C804E> type <Fail> code <78> phrase <URI authority not found>
http <-1>
```

GSKit client certificate error

URI authority not found can occur when the automation server is using a self-signed certificate. The other error condition is that the WebSphere Application Server for Registry Services does not contain the automation server certificate in its trusted certificates keystore.

Check the automation server environment file. If **ITM_AUTHENTICATE_CLIENT_CERTIFICATE=Y**, verify that the automation server's server certificate is not self-signed or missing from the WebSphere Application Server trusted certificate keystore.

GSKit server certificate error

URI authority not found can occur when the WebSphere Application Server for Registry Services is using a server certificate that is a self-signed certificate. The other error condition is that the automation server does not have the WebSphere Application Server server certificate for Registry Services in the automation server GSKit keystore.

Check the automation server environment file. If **ITM_AUTHENTICATE_SERVER_CERTIFICATE=Y**, verify that the WebSphere Application Server server certificate for Registry Services is not self-signed or missing from the automation server GSKit keystore.

GSKit cipher error

URI authority not found can be caused by a GSKit cipher error. RAS1 trace contains this error message:

```
(NNNNNNNN.NNNN-NNN:kdebeal.c,81,"ssl_provider_open")
GSKit error 422: GSK_ERROR_BAD_V3_CIPHER
```

Review the automation server environment file for an invalid variable setting for the KDEBE_V3_CIPHER_SPECS. The following KDEBE_V3_CIPHER_SPECS values are valid.

Table 15. **KDEBE_V3_CIPHER_SPECS** *valid values*

Short value	Long name
01	**SSL_RSA_WITH_NULL_MD5**
02	**SSL_RSA_WITH_NULL_SHA**
03	**SSL_RSA_EXPORT_WITH_RC4_40_MD5**
04	**SSL_RSA_WITH_RC4_128_MD5**
05	**SSL_RSA_WITH_RC4_128_SHA**
06	**SSL_RSA_EXPORT_WITH_RC2_CBC_40_MD5**
09	**SSL_RSA_WITH_DES_CBC_SHA**
0A	**SSL_RSA_WITH_3DES_EDE_CBC_SHA**
2F	**TLS_RSA_WITH_AES_128_CBC_SHA**
35	**TLS_RSA_WITH_AES_256_CBC_SHA**

Ensure that **`KDEBE_V3_CIPHER_SPECS`** is set one of the short values (such as 09), and not a long name value such as `SSL_RSA_WITH_DES_CBC_SHA`). If you set **`KDEBE_V3_CIPHER_SPECS`**, verify that both the automation server and the WebSphere Application Server for Registry Services are using the same set of ciphers: The “long name” values are used by the WebSphere Application Server for Registry Services; and the “short name” values are used by the automation server.

Solution

Review the automation server environment variables for diagnosis, as described earlier, and edit as needed. (See “Log and environment files” on page 181 for the location of the environment file.)

OSLC-PM service provider fails to start

The Open Services Lifecycle Collaboration Performance Monitoring (OSLC-PM) service provider HTTP or HTTPS connection to the Registry Services application can fail to start for several reasons. Review the possible causes and solutions.

Problem

The service provider can fail to start for the following reasons:

- The OSLC-PM service provider is configured for a Registry Services that is not supported when the hub Tivoli Enterprise Monitoring Server is configured for hot standby.
- The hub monitoring server is configured for hot standby and the hub alias configuration setting for the OSLC-PM service provider was reconfigured, but the new value does not match the acting hub alias that is configured at the acting hub.
- OSLC-PM service provider entries in the automation server configuration file have an incorrect or missing user ID or password, or both, that is specified for Registry Services.
- OSLC-PM service provider local connection information port is being used by another application.

Error messages that display:

Windows When you start the service provider in Manage Tivoli Enterprise Monitoring Services, the service provider fails to start and the following message is displayed: `KCICF5100E Unable to start service, see Event Log for information`.

Linux UNIX When you start the service provider using the **`itmcmd`** agent start command, the service provider fails to start and the following error message is displayed: `KCIIN0198E Unable to start agent. Please, check log file`.

Diagnoses and Solutions

You can see OSLC-PM service provider error messages in the automation server MSG2 log file that can help you to isolate where the problem might be occurring. (See “Log and environment files” on page 181 for the file path.)

Incorrect or missing user ID or password for Registry Services

When OSLC-PM service provider entries in the automation server configuration file have incorrect or missing user ID or password values defined for Registry Services, you see the following error message in the automation server MSG2 log file: `KASPR017E The OSLC-PM Service Provider encountered a Registry Services authorization error`.

Review the user ID and password values that are configured for the OSLC-PM service provider.

OSLC-PM service provider local connection information port is unavailable

When a KDEB_INTERFACELIST is specified in the OSLC-PM service provider configuration file, the service provider binds to a specific interface. If the service provider local connection information port is being used by an application for the specified interface, you see the following error message in the automation server MSG2 log file: `KASE061 Port` *`nnn`* `is not available`.

Specify a different OSLC-PM service provider local connection information port value.

Review and edit the KDBE_INTERFACELIST in the OSLC-PM service provider configuration file as needed. (See "Log and environment files" on page 181 for instructions.)

Registry Services version does not support the hub monitoring server configured for hot standby

When the hub monitoring server is configured for hot standby and the OSLC-PM services provider is configured for a Registry Services that is not the proper version, the following error message is entered in the automation server MSG2 log file:

```
KASPR061E  Registry Services must be at version
1.1.0.1.201306271654 or higher to support FTO.
```

Review the *IBM Tivoli Monitoring Installation and Setup Guide* (http://pic.dhe.ibm.com/infocenter/tivihelp/v61r1/topic/com.ibm.itm.doc_6.3fp2/install/itm_install.htm) and upgrade the Registry Services to support hot standby configuration.

Hub alias setting was changed and does not match the setting for the OSLC-PM service provider at the acting hub

When the setting for the hub alias is modified and does not match the setting at the hub monitoring server that is currently the acting hub, the following error message is entered in the automation server MSG2 log file:

```
KASPR063E: The acting hub alias does not match the value in
use by the OSLC-PM server provider at host myhub.ibm.com.
Shutdown initiated.
```

Update the acting hub alias environment setting and start the automation server.

Metrics are delayed and you get Not Found (404 error) message

Certain conditions affecting the Tivoli Enterprise Monitoring Automation Server can result in health metrics being temporarily unavailable and a Not Found (404 error) message being displayed. Review the possible causes and solutions.

The dependent Tivoli Monitoring OS Agent on the same computer is not online

Tivoli Enterprise Monitoring Automation Server Registry Services health metrics are not available and a Not Found (404 error) error is returned in the following scenarios. If the registration for the monitoring agent depends on another Open Services Lifecycle Collaboration (OSLC) resource that is not online or has not been registered, the health metrics fail with a Not Found/404 request error. The IBM Tivoli Composite Application Manager for Applications autosvr_notfound404_trouble.dita(ITCAM) monitoring agents are dependent on the OSLC Resource Registration for the OS agent located at the same computer. If the OS agent is not running, health metrics are not available for the ITCAM agent.

Verify that the OS agent is online at the hub Tivoli Enterprise Monitoring Server and that it is registered in the JazzSM Registry Services before retrying the request.

The automation server is restarting

During a restart, the OSLC resources for the monitoring agents that are online at the hub monitoring server are reverified and reregistered. During this time, a request for health metrics from a monitoring agent that appears online at the hub monitoring server might fail with a Not Found (404 error) message.

Retry the request after the registration has completed.

During a hot standby failover

Starting with IBM Tivoli Monitoring Version 6.3 Fix Pack 2, the automation server supports a hub monitoring server that is configured for hot standby. If failover is taking place, the *acting hub* has stopped and the *standby hub* is taking over the role as the new acting hub. During this time, health metrics for a monitoring agent might not be available and a Not Found (404 error) message is returned even though the monitoring agent appears online in the Tivoli Monitoring user interfaces such as the Tivoli Enterprise Portal and Manage Tivoli Enterprise Monitoring Services.

Retry the request after the failover to the new hub monitoring server has completed and the monitoring agent has been reregistered in the JazzSM Registry Services by the new acting hub.

Linux automation server fails to start when quickly recycled

If you stop the Tivoli Enterprise Monitoring Automation Server and immediately restart it, it is possible to get a failure on the restart. Review the diagnostic information and solution to resolve the problem.

Problem

After you stop the automation server and immediately restart it, you observe that the server failed to start and a KCIIN0198E message might be displayed at the command line:

```
# ./itmcmd agent start as Processing. Please wait...
Starting Tivoli Enterprise Monitoring Automation Server ...
KCIIN0198E Unable to start agent.
```

Diagnosis

The listening port that is used by the previous `kasmain` process can be slow to release, which causes the new `kasmain` process to fail to start. The following message is found in the KAS MSG2 log (see “Log and environment files” on page 181 for the file location):

```
Mon Nov 26 12:46:52 2012 KASE061    Port 10001 is not available.
```

Solution

Wait a moment for the port to be released by the operating system, and attempt to restart the automation server again.

After a hub failover, the batch URL remap request doesn't complete successfully

After a hub Tivoli Enterprise Monitoring Server failover, registered resources in Registry Services contain URLs that still refer to the Open Services Lifecycle Collaboration Performance Monitoring (OSLC-PM) service provider that is collocated with the prior acting hub.

Symptom

Registry Services was not able to complete the batch URL remap request that was sent by the OSLC-PM service provider. The MSG2 log file shows the following messages:

```
KASPR075I Batch URL remaps in progress at Registry Services. OSLC-PM
Service Provider operation paused.
```

```
KASPR066I Batch URL remaps completed by Registry Services. HTTP
status code: <non-200 status code>
```

A non-200 status code indicates that the batch URL remap request did not complete successfully.

Diagnosis and Solution

If the status code indicates that the request did not complete successfully, the remap timeout period needs to increased. See the “Tivoli Enterprise Monitoring Automation Server environment variables” topic in the *IBM Tivoli Monitoring Installation and Setup Guide* for setting the `KAS_REGISTRY_SERVICES_TIMEOUT_URL_REMAP` value. You must increase the value of the `KAS_REGISTRY_SERVICES_TIMEOUT_URL_REMAP` parameter for the OSLC-PM service provider at each of the hub monitoring services.

OSLC-PM service provider loses connection to Registry Services

If the Open Services Lifecycle Collaboration Performance Monitoring (OSLC-PM) service provider successfully connects to Registry Services, but immediately loses the connection, review the diagnosis and solution.

Symptom

The OSLC-PM service provider can successfully connect to Registry Services, but immediately loses the connection and the following messages repeat in the MSG2 log:

```
KASPR001I The OSLC-PM Service Provider has connected to the Registry
Services server at http://host.domain:16310/oslc/pr. KASPR002E.
The OSLC-PM Service Provider has lost connection to the Registry
Services server at http://host.domain:16310/oslc/pr.
```

Diagnosis

The problem typically occurs when Registry Services returns a hostname for itself that cannot be resolved on the network. The OSLC-PM service provider indicates a disconnect after attempting to use the new hostname that was provided by Registry Services.

You can see OSLC-PM service provider messages in the automation server MSG2 log file that can help you to isolate where the problem might be occurring. (See “Log and environment files” on page 181 for the file path.)

After ruling out the common connection issues, investigate further by reviewing the service provider entries in the automation server RAS1 trace file. Search the RAS1 trace file for `KDH1 status` error messages. The connection error specific to this issue is `KDH1 status URI authority not found`, however, unlike the simple connection failure, the hostname is different in the two error messages. Often the problem is that the Registry Services has provided a short host name that can't be resolved from the OSLC-PM service provider host. Example:

```
(xxxxxxxxxxxxxxxx-xxxxx:kassoap.cpp,729,"sendSoapHTTPRequest")
Error: KDH1_NewActivity failed for 'http://host:16310/oslc/pr/
collection'
(xxxxxxxxxxxxxxxx-xxxxx:kassoap.cpp,935,"sendSoapHTTPRequest") KDH1
status <0x7C4C804D> type <Fail> code <77> phrase <URI authority is
not a recognized network address> http <404>
(xxxxxxxxxxxxxxxx-xxxxx:kassoap.cpp,266,"sendHTTPRequest") Error
<0x7c4c804d>, HTTP <404>: Request failed
(xxxxxxxxxxxxxxxx-xxxxx:kascontr.cpp,5437,"autoTEMSWriteRAS")
registerITMProvider: ERROR: Registry Services is not running.
(xxxxxxxxxxxxxxxx-
xxxxx:prnetwrk.cpp,135,"kas_setRegistryServicesDisconnected") ERROR:
Not connected to Registry Services server http://host.domain:16310/
oslc/pr. Connection lost
```

Solution

Update the network configuration of the OSLC-PM service provider host system and ensure that the host name returned by Registry Services can be resolved.

Reconfigure the Registry Services host system to use a fully qualified domain name that can be resolved by the host system where the OSLC-PM service provider is installed.

Remove the KASSTATE file from the following directory so that the cached version of the provider URL is removed:

Windows *install_dir*\CAS

Linux UNIX *install_dir*/*<interp>*/as

Shutdown takes a long time

The Tivoli Enterprise Monitoring Automation Server sends HTTP requests to the registry to report changes in performance monitoring statistics and resources. If an automation server shutdown is initiated while an HTTP request is in progress, such as to Jazz for Service Management, shutdown is delayed until the HTTP request terminates.

Other factors such as network delays and unresponsive routers can also slow shutdown.

Problem

The automation server fails to stop or does not stop in a timely fashion.

UNIX command to stop the automation server and the response after timeout occurs:

```
./itmcmd agent stop as
Processing. Please wait...
Stopping Tivoli Enterprise Monitoring Automation Server ...
Product as was not stopped. You can use /data/630/d2275a/bin/itmcmd agent
stop command with option -f to force stop product as.
Using this option you may lose/corrupt data! See help for more information.
KCIIN0205E Unable to stop agent or process...
```

Cause If the automation server shutdown request was initiated while an HTTP request is in progress, shutdown processing is delayed until either an HTTP response is received or the HTTP request times out based on the associated **KAS_REGISTRY_SERVICES_TIMEOUT** parameter value, with the automation server stopping after either condition occurs.

Solution

Change the default 120-second timeout period to a lower value, such as 60 seconds. A lower value causes the HTTP request to stop sooner, thereby allowing the shutdown to proceed. See the descriptions for **KAS_REGISTRY_SERVICES_ TIMEOUT_GET**, **KAS_REGISTRY_SERVICES_ TIMEOUT_POST**, and **KAS_REGISTRY_SERVICES_ TIMEOUT_DELETE** in the *IBM Tivoli Monitoring Installation and Setup Guide* “Environment variables” topics.

To access the automation server environment file for editing the timeout variables, see “Log and environment files” on page 181.

Chapter 11. Authorization Policy Server troubleshooting

Use the Tivoli Authorization Policy Server feature for protecting your resources from unauthorized access by users of monitoring dashboards in the Dashboard Application Services Hub. The Authorization Policy Server is installed with the Dashboard Application Services Hub, and the tivcmd Command-Line Interface (CLI) is installed on the computers where administrators create authorization policies.

Review the trace and log information and problem scenarios for guidance with diagnosing Authorization Policy Server issues.

Trace and log information

The Authorization Policy Server feature interoperates with the Infrastructure Management Dashboards and the dashboard data provider. Hence, troubleshooting problems might require collecting trace and log information from more than one of these components.

Setting a trace for the dashboard data provider or policy client

A portion of the Tivoli Authorization Policy feature runs inside the dashboard data provider. This code is referred to as the *policy client*. The dashboard data provider and policy client tracing can be enabled through the TEPS/e administration console using the same procedure. The only difference is the setting for the package trace levels.

Set dashboard data provider tracing when you have trouble with data retrieval to the server dashboards and have been requested by IBM Support. Policy client tracing can be helpful when you are troubleshooting problems involving run-time authorization checks or policy distribution.

Before you begin

The TEPS/e administration console is disabled by default for security reasons and to save system resources. The Tivoli Enterprise Portal Server must be running before you enable the console.

About this task

Take these steps to enable and start the TEPS/e administration console, and set a trace for the dashboard data provider or policy client:

Procedure

1. Enable the TEPS/e administration console :
   - Windows In the Manage Tivoli Enterprise Monitoring Services window, highlight Tivoli Enterprise Portal Server and select **Advanced** > **TEPS/e Administration** > **Enable TEPS/e Administration**.
   - Linux UNIX From the command line, change to the `scripts` directory (Intel Linux: *`install_dir`*`/li6263/iw/scripts`; zLinux:*`install_dir`*`/ls3266/iw/scripts`; AIX®:*`install_dir`*`/aix533/iw/scripts`) and enter the following command, where `true` starts the console and `false` stops the console:

```
./enableISCLite.sh {true/false}
```

The TEPS/e administration console is now enabled for logon and will remain enabled until the portal server is stopped.

2. If this is the first time you are enabling the console, you must set the administration password:
   - Windows In theManage Tivoli Enterprise Monitoring Services window, highlight **Tivoli Enterprise Portal Server** and select **Advanced** > **TEPS/e Administration** > **TEPS/e Administration Password**.
   - Linux UNIX From the `scripts` directory, enter the following command, where *`username`* is `wasadmin`, and *`password`* is the new password:

     ```
     updateTEPSEPass.sh username password
     ```

     Subsequently, entering a TEPS/e administration password resets the password.
3. Enter one of the following URLs in your Internet Explorer or Firefox browser:
   - `http://localhost:15205/ibm/console`
   - `https://localhost:15206/ibm/console`
4. Log on to the console using `wasadmin` for the user ID and the password you entered as the TEPS/e administration password. The TEPS/e administration console window is displayed.
5. Set the trace:
   a. Expand the **Troubleshooting** category and select **Logs and trace**.
   b. Select the server identifier (typically ITMServer).
   c. Under the **General Properties** heading, select **Change log detail levels**.
   d. To change the log settings without recycling the server, select the Runtime tab. If you want to persist the log settings through a server restart, select the **Save runtime changes to the configuration as well** check box.
   e. Set the following package level trace to increase dashboard data provider or policy client logging:

      ```
      *=info:com.ibm.tivoli.monitoring.provider.*=finest
      ```
   f. Select **OK** and save the settings.

What to do next

You can use **`tacmd pdcollect`** to collect the necessary data provider logs from the portal server. For more information about the tacmd commands, see the *IBM Tivoli Monitoring Command Reference* (http://pic.dhe.ibm.com/infocenter/tivihelp/v61r1/topic/com.ibm.itm.doc_6.3fp2/ic/landing_cmdref.htm).

Authorization Policy Server trace setting

The Authorization Policy Server runs on the Jazz for Service Management (JazzSM).

Configure Authorization Policy Server trace settings through the JazzSM console if IBM Support has requested traces.

Procedure

1. Enter the following URL in your browser to start the JazzSM console:
   `https://`*`hostname`*`:`*`admin_host_port`*`/`*`context_root`*`/logon.jsp`
   where

   `hostname` is the fully qualified host name of the JazzSM server.

admin_host_port is the JazzSM administration host port, typically 16316. To find the port number, open the `portdef.props` file in the JazzSM profile properties directory, and locate the **`WC_adminhost_secure`** property.

context_root was configured at installation time. The default is `ibm/console`.

The default URL is `https://`*`hostname`*`:16316/ibm/console/logon.jsp`.

2. After logging into the JazzSM console, expand the **Troubleshooting** category and select **Logs and trace**.
3. Select the server identifier (typically ITMServer).
4. Under the **General Properties** heading, select **Change log detail levels**.
5. To change the log settings without recycling the server, select the Runtime tab. If you want to persist the log settings through a server restart, select the **Save runtime changes to the configuration as well** check box.
6. To increase the logging for the Authorization Policy Server, set the package trace level to "all" for "com.ibm.tivoli.rest.*": `*=info: com.ibm.tivoli.rest.*=all`
7. Select **OK** and save the settings.

What to do next

You can run one of the following scripts to create a `PolicyServerLogs.zip` file in a child `output` directory that contains the log information from the server dashboards and Authorization Policy Server:

Windows *`JazzSM_installdir`*`\AuthPolicyServer\PolicyServer\tools\pdCollect.bat`

Linux UNIX *`JazzSM_installdir`*`/AuthPolicyServer/PolicyServer/tools/pdCollect.sh`

pdcollect tool

Use the pdcollect tool to gather log files, IBM Installation Manager logs, configuration information, version information, properties and other information to help diagnose problems with authorization policies.

The pdcollect tool is used at the command line by running the pdcollect script.

The pdcollect tool is installed with the Tivoli Authorization Policy Server or the tivcmd Command-Line Interface for Authorization Policy (See "Installing and configuring the Tivoli Authorization Policy Server and tivcmd Command-Line Interface for Authorization Policy" in the *IBM Tivoli Monitoring Installation and Setup Guide*.)

pdcollect for Authorization Policy Server

Installation location

Because the Authorization Policy Server is installed with the Dashboard Application Services Hub component of Jazz for Service Management, the pdcollect script is found under the Jazz for Service Management:

Windows *`JazzSM_install_dir`*`\AuthPolicyServer\PolicyServer\tools\pdcollect.bat`

Linux UNIX *`JazzSM_install_dir`*`/AuthPolicyServer/PolicyServer/tools/pdcollect.sh`

After you run the script, the file `PolicyServerLogs-`*`host_name`*`.zip` is created in the system temporary location.

Sample execution

Windows `C:\Program Files\IBM\JazzSM\AuthPolicyServer\PolicyServer\tools\pdcollect.bat` generated `C:\Users\ADMINI~1\AppData\Local\Temp\2\PolicyServerLogs-CO060048.zip`

Linux UNIX `-bash-3.2#./pdcollect.sh` generated `/tmp/PolicyServerLogs-nc051041.zip`

Contents of the PolicyServerLogs-*host_name*.zip

The zip file has the following folder structure:

`JazzSMProfile`
The folder name is based on the WebSphere Application Server profile name that was specified when Jazz for Service Management was installed. The default profile name is `JazzSMProfile`. Within `JazzSMProfile`, are the WebSphere Application Server logs. Importantly, the `SystemErr`, `SystemOut`, native logs, and first failure data capture (FFDC) logs instantly collect events and errors that occur during the WebSphere Application Server runtime. This folder generally contains the logs from the *`JazzSM_installdir`*`//profile/logs` folder.

`logs`
This folder contains the `deployPolicyServer.log` file, which contains output from wsadmin script execution for deploying the Authorization Policy Server application into the WebSphere Application Server

META-INF
This folder contains the Manifest file.

properties
This folder contains the `PolicyServer.properties` and `tipinfo.properties` files.

InstallationManagerLogs.zip
This zip file contains the relevant information for diagnosing issues that are associated with installing the Authorization Policy Server using the IBM Installation Manager.

pdcollect for tivcmd CLI

Installation location

The pdcollect tool is installed with the tivcmd CLI using the IBM Installation Manager. The pdcollect script is located in the following folder:

Windows *`CLI_install_dir`*`\tools\pdcollect.bat`

Linux UNIX *`CLI_install_dir`*`/tools/pdcollect.sh`

After you run the script, the file `PolicyCLILogs-`*`host_name`*`.zip` is created in the system temporary location.

Sample execution

Windows `C:\IBM\TivoliMonitoring\tools\pdcollect.bat` generated `C:\Users\ADMINI~1\AppData\Local\Temp\2\PolicyCLILogs-CO060048.zip`

Linux UNIX `-bash-3.2#./pdcollect.sh` generated `/tmp/PolicyCLILogs-nc051041.zip`

Contents of the PolicyCLILogs-*host_name*.zip

The zip file has the following folder structure:

`logs`
This folder contains the KDQ RAS1 logs, generated from executing tivcmd CLI commands.

property
This folder contains the `KDQENV` file when the pdcollect script is run on Windows, and the `kdqenv.config` file when the script is run on Linux or UNIX.

InstallationManagerLogs.zip
This zip file contains the relevant information for diagnosing issues that are associated with installing the tivcmd CLI using the IBM Installation Manager.

Audit logs for the Authorization Policy Server

Review the examples and explanation of the types of audit log records that are written for Authorization Policy Server policy updates, authorization failures, communication failures, and stale authorization policies.

Audit record for policy updates

The audit log `system.`*`Hub_Name`*`_cq_audit.log`, has an audit record similar to the one shown in the following example. The Policy Distribution Client picks up policy updates.

```
<AuditEvt Domain="" Type="SYSADMIN" Level="Minimum" Ver="110">
   <Who>
      <UserID>SYSTEM</UserID>
      <AuthID>SYSTEM</AuthID>
   </Who>
   <What>
      <Op Name="CreatePolicyStore" Type="" />
      <Msg Text="KDQPD0019I A new policy store [ C:\IBM\ITM\PolicyStore\
      tivoliRoot_1359571094481 ] was created by the policy distribution
      client and is ready to be used by policy clients on this machine."
      RBKey="KDQA0000" />
      <Result>0</Result>
   </What>
   <When>
      <EvtTS MS="1130130133814731" ITM="1130130133814000" />
      <Corr>0</Corr>
      <Seq>19</Seq>
   </When>
   <OnWhat>
      <Obj Type="" Name="C:\IBM\ITM\PolicyStore\tivoliRoot_1359571094481" />
   </OnWhat>
   <Where>
      <Origin>
         <Node Name="Tivoli Enterprise Portal Server" Type="SERVER"
      AddrType="IPv4" Addr="192.168.1.65" Host="perezwin7"
      SYSID="PEREZWIN7:TEPS" />
      </Origin>
      <App Code="KCQ" Ver="XX.XX.XX" Comp="kcj" />
      <SvcPt>system.perezwin7_cq</SvcPt>
   </Where>
   <WhereFrom>
      <Source>
         <Node Name="" SYSID="192.168.1.65" />
      </Source>
   </WhereFrom>
   <WhereTo>
      <Target>
      <Node Name="" Host="perezwin7" />
   </Target>
</WhereTo>
</AuditEvt>
```

Audit log showing authorization failure records

If users are having authorization failures when they attempt to open certain dashboards, review the audit log for the following message text:

```
The User does not have view access to
UISolution.ITMSDNT.ViewModel.NTProcessTable User does not have event
access to any systems for
UISolution.ITMSDBASE.ViewModel.EventCountByMGroup
```

The `UISolution` and `ViewModel` names vary depending on the access restriction.

Audit record generated when the dashboard data provider cannot communicate with the Authorization Policy Server

```
<AuditEvt Domain="" Type="SYSADMIN" Level="Basic" Ver="110">
<Who>
   <UserID>jptipadmin</UserID>
   <AuthID>SYSTEM</AuthID>
</Who>
<What>
   <Op Name="distribute" Type=""/>
   <Msg Text="KDQPD0007E A [ POST ] request was issued to URL
   [ HTTP://localhost2:16310/ibm/tivoli/rest/providers/AUTHZ/
   datasources/authdata/datasets/policies/tasks/GET_DIST_TIMESTAMP ],
   but failed because the URL is unreachable."
   RBKey="KDQA0000"/>
   <Result>0</Result>
</What>
<When>
   <EvtTS MS="1130130135951716" ITM="1130130135951000"/>
   <Corr>0</Corr>
   <Seq>7</Seq>
</When>
<OnWhat>
   <Obj Type="" Name="any"/>
</OnWhat>
<Where>
   <Origin>
      <Node Name="Tivoli Enterprise Portal Server" Type="SERVER"
   AddrType="IPv4" Addr="192.168.1.65" Host="perezwin7"
   SYSID="PEREZWIN7:TEPS"/>
   </Origin>
   <App Code="KCQ" Ver="XX.XX.XX" Comp="kcj"/>
   <SvcPt>system.perezwin7_cq</SvcPt>
</Where>
<WhereFrom>
   <Source>
      <Node Name="" SYSID="192.168.1.65" Addr="192.168.1.65"/>
   </Source>
</WhereFrom>
<WhereTo>
   <Target>
      <Node Name="" Host="perezwin7"/>
   </Target>
</WhereTo>
</AuditEvt>
```

The following example shows the beginning of the audit record that is generated by the Policy Distribution Client when the dashboard data provider cannot communicate with the Authorization Policy Server. The

Policy Distribution Client runs within the dashboard data provider task, The Op Name is “**PolicyUpdateError**”.

```
<AuditEvt Domain="" Type="SECMAINT" Level="Minimum" Ver="110">
<Who>
   <UserID>SYSTEM</UserID>
   <AuthID>SYSTEM</AuthID>
</Who>
<What>
   <Op Name="PolicyUpdateError" Type=""/>
   <Msg Text="SERVER_UNREACHABLE : PolicyMessageInfo ...
```

Audit record generated when the policies become stale

If there is no active policy for user authorization, the dashboards do not populate the charts and table with data but, instead, display a message that “An unexpected error occurred.”

When you view the audit record, the Op Name is “**DeletePolicyStore**”

```
<AuditEvt Domain="" Type="SYSADMIN" Level="Minimum" Ver="110">
<Who>
   <UserID>SYSTEM</UserID>
   <AuthID>SYSTEM</AuthID>
</Who>
<What>
   <Op Name="DeletePolicyStore" Type="" />
   <Msg Text="KDQPC0022W The policy client component detected that there
   is no active policy store against which to authorize.
   The policy client will remain active waiting for a policy store
   to become available. In the meantime, all authorize requests
   will be rejected." RBKey="KDQA0000" />
   <Result>0</Result>
</What>
<When>
   <EvtTS MS="1130130150742533" ITM="1130130150742000"/>
   <Corr>0</Corr>
   <Seq>140</Seq>
</When>
<OnWhat>
   <Obj Type="" Name="" />
</OnWhat>
<Where>
   <Origin>
      <Node Name="Tivoli Enterprise Portal Server" Type="SERVER"
   AddrType="IPv4" Addr="192.168.1.65" Host="perezwin7"
   SYSID="PEREZWIN7:TEPS" />
   </Origin>
   <App Code="KCQ" Ver="XX.XX.XX" Comp="kcj" />
   <SvcPt>system.perezwin7_cq</SvcPt>
</Where>
<WhereFrom>
   <Source>
      <Node Name="" SYSID="192.168.1.65" />
   </Source>
</WhereFrom>
<WhereTo>
   <Target>
      <Node Name="" Host="perezwin7" />
   </Target>
</WhereTo>
</AuditEvt>
```

Validate correct configuration and operation

You can review the Audit Log workspace to confirm that the Authorization Policy Server and Tivoli Enterprise Portal Server were configured correctly and are operational.

The portal server audit log is available in Tivoli Enterprise Portal at the Enterprise-level of the Navigator Physical view. Review the audit log workspace for the following messages:

```
KDQPD0015I The policy distribution client component initialized.
KDQPC0023I The policy client component detected that there is a new policy
store [ PATH To file store ].
KDQPC00201 The policy client component initialized successfully.
Initialization with the Policy Server succeeded.
```

Authorization Policy Server startup failure

If the Authorization Policy Server fails to start, review the known problems, possible causes, and suggested solutions.

Configuration errors KDQPN0006E and KDQPN0007E cause the policy server not to start

If you get either of these errors during configuration, the policy server does not start. These errors usually indicate that a problem occurred during the installation and configuration that prevented critical configuration values from being set. Re-install the policy server. For more information, see “Installing and configuring the Tivoli Authorization Policy Server and tivcmd Command-Line Interface for Authorization Policy” in the *IBM Tivoli Monitoring Installation and Setup Guide*.

A different type of startup error occurs

Check that the Authorization Policy Server configuration variables are set correctly and point to a location that the WAS service can access.

Confirm that the configuration variables are set properly:

1. Enter the following URL in your browser to start the JazzSM console: `https://`*`hostname`*`:`*`admin_host_port`*`/`*`context_root`*`/logon.jsp`
   where

   `hostname` is the fully qualified host name of the JazzSM server.

   `admin_host_port` is the JazzSM administration host port, typically 16316. To find the port number, open the `portdef.props` file in the JazzSM profile properties directory, and locate the **`WC_adminhost_secure`** property.

   `context_root` was configured at installation time. The default is `ibm/console`.

   The default URL is `https://`*`hostname`*`:16316/ibm/console/logon.jsp`.
2. After logging into the JazzSM console, expand the **Resources** category and **Resource Environment** subcategory, and select **Resource Environment Providers**.
3. In the main view, check that the “kdqauthzResourceEnvironmentProvider” resource provider name is present. If the provider name is not there, you should have seen error KDQPN0006E earlier and must re-install the policy server.
4. Select the “kdqauthzResourceEnvironmentProvider” resource provider and click **Additional Properties** > **Resource environment entries**.
5. Select the “AuthzResourceReference” item and click **Additional Properties** > **Custom properties**.
6. Confirm that the following properties are present: XACML_ROOT_DIRECTORY, SEED_ROOT_DIRECTORY, DIST_ROOT_DIRECTORY, DIST_POLL_INTERVAL, AUDIT_ROOT_DIRECTORY, AUDIT_FILE_SIZE, AUDIT_COUNT

7. Confirm that the appropriate directories and the access to those directories exist for the WAS Service.

Authorization failures using the Policy CLI commands

If a user encounters authorization failures when attempting to run tivcmd commands, the user is probably not a member of a role such as `RoleAdministrator` with authority to run Policy CLI commands. You have two options for resolving the problem.

1. Assuming you are a member of `RoleAdministrator` or an equivalent role with full administrator authority, you would execute **`tivcmd addtorole`** to explicitly add the user to the role.
2. Alternatively, you could leverage user groups, which are managed either by LDAP or by an operating system provided User/Group management system. Instead of explicitly adding the user to an administrator role, you would add a user group that the user is a member of to the administrator role. This approach keeps the policy data store from being cluttered with many individual user ID permissions, and you can control policy access levels by adding or removing users from user groups rather than having to run a tivcmd each time.

CLI tivcmd commands for dashboard authorization diagnostics

You can use the command-line interface **`tivcmd`** commands to diagnose dashboard authorization problems, such as resources not being visible to a user.

Review the scenarios to learn more about using tivcmd commands to investigate problems with server dashboards.

Managed system not shown

When determining why a managed system is not shown in the server dashboards for a particular user, you must have the following information: the user ID, the managed system name, and the managed system groups that the managed system is a member of.

You can run the following command to display the list of roles that the user is a member of, either explicitly or through user group role membership:

```
tivcmd listroles -u userid
```

If you suspect that the user is not a member of a role that has permission to view the managed system, you can enter this command to display the complete membership for the role:

```
tivcmd listroles -n role_name -m
```

Either the user can be added to the role, or the user can be added to a group that is already a member of the role.

If the user is already a member of the expected viewing role, ensure that the correct permissions are applied to that role using this command:

```
tivcmd listroles -n role_name -p
```

If the permissions are correct for the role, check to see if the user is a member of a group or role that has been explicitly denied the permission to view the specified managed system. Note that access denials, implemented with **`tivcmd exclude`**, always take priority even if a **`tivcmd`**

grant had been issued for the same resource. The search to find an explicitly denied managed system can be performed with this command:

```
tivcmd listroles -t managedsystem -r managed_system_name -p
```

The command returns all permissions that specify the given managed system for each associated role. If the user is a member of one of those roles and an excluded "view" operation is present, the authorization is either correct or the user was incorrectly added to the role explicitly or through a user group. In that case, one of the following resolutions might solve the problem:

- Remove the user with the `tivcmd removefromrole` command if the membership is explicit, or through the User/Group management system if the membership is implicit.
- Use the `tivcmd revoke` command to remove the denial rule for the resource if you have determined that the rule is no longer needed.

If the problem is that no role currently exists with permission to the given managed system or to the managed system group that it is a member of, the solution might be to create a new role, with the required permissions, and add the user to the role.

Lastly, it might be the case that the role or permissions for viewing the managed system exist and the user has been correctly added to the role, but the policy updates were not distributed to the Tivoli Enterprise Portal Server so that it could make use of the updates. In that case, you might need to take the following steps:

1. Review and possibly shorten the policy **Polling Interval** configured on the portal server if the policy retrievals are not occurring quickly enough. The portal server has a default interval of 30 minutes for checking the Authorization Policy Server for changes. (For details on reconfiguring the portal server authorization policy settings, see "Enabling authorization policies in the portal server" in the *IBM Tivoli Monitoring Administrator's Guide*.)
2. Examine the portal server audit log in the Tivoli Enterprise Portal to see whether a policy distribution error occurred. For more information, see "Audit logging" in the *IBM Tivoli Monitoring Administrator's Guide*.

For more details on these types of errors, see "Policy distribution issues" on page 201.

Managed system group not shown

To determine why a managed system group is missing from a server dashboard, follow the same basic troubleshooting steps as you would for a missing managed system. First, run the following command to list the roles a user is a member of, either explicitly or through role membership.

```
tivcmd listroles -u user_ID
```

Next, run the following command to display the complete role membership where *role_name* is the distinguished name (for example, tivcmd listroles -u uid=test1ldap,cn=ITMSSORealm,ou=SWG,o=IBM,c=US).

```
tivcmd listroles -n role_name -m
```

The command returns all permissions that specify the given managed system group for each associated role. The user should be a member of one of those roles, either explicitly or implicitly through a group. If that is not the case, you can either add the user to a role that has access to the managed system group or the user can be added to a group that is already a member of the role. Also, ensure that the user is not being denied access to the managed system group because of a previously issued tivcmd exclude.

Lastly, it might be the case that no role exists with permission to the given managed system group, in which case the solution might be to create a new role, grant the required permission, and add the user to the role.

Cannot see events for a managed system

For a user to see events for a managed system, they must be a member of a role that has access on the "event" object type.

For a user to see event details for a managed system, they must be a member of a role that has access on both the "attributegroup" object type and "event" object type.

You can check the permissions of the role that the user belongs to by running the following command:

```
tivcmd listroles -u user_ID -p
```

(Example: tivcmd listroles -u uid=test1ldap,cn=ITMSSORealm,ou=SWG,o=IBM,c=US -p) If the user should be allowed to see the events for a managed system, the "event" permission can be added to the existing role using the **`tivcmd grant`** command, or a new role can be created with the permission and the user added to the new role.

For a description of all the tivcmd commands, see the *IBM Tivoli Monitoring Command Reference* (http://pic.dhe.ibm.com/infocenter/tivihelp/v61r1/topic/com.ibm.itm.doc_6.3fp2/ic/landing_cmdref.htm).

Policy distribution issues

Review the information on troubleshooting why policy updates are not available at the dashboard data provider.

Policy updates never appear at the Tivoli Enterprise Portal Server

Policy updates are implemented with the CLI tivcmd commands and stored on the Authorization Policy Server computer. The portal server uses a polling mechanism to make periodic requests to the Authorization Policy Server to retrieve a local copy of the latest policy store. The local copy gets stored in the `*install_dir*/PolicyStoreArchive/argus.zip` file on the dashboard data provider computer (the portal server). If this file is missing, it confirms that policy distribution is failing. The portal server has a configuration panel for specifying the information needed to connect to the Authorization Policy Server and send it policy retrieval requests. The following configuration information is required:

Authorization Policy Server hostname or IP address

protocol (http or https)

port (port associated with http or https protocol on Authorization Policy Server)

user ID and password

If any of the information is incorrect, the portal server is unable to retrieve policy updates from the Authorization Policy Server. Typical errors:

- The Authorization Policy Server is not active. Make sure the tivcmd CLI can be run successfully; if not, start the start the WebSphere application server where the Authorization Policy Server and Dashboard Application Services Hub are installed: At the command prompt, change to the `C:\Program Files\IBM\JazzSM\profile\bin` directory and enter **`startserver server1`**.
- The wrong host name or port is specified. To verify the host name and port, enter the following URL in your browser: `http://`*`configured_hostname`*`:`*`configured_port`*`/ibm/tivoli/rest/providers/AUTHZ`. If you get an error, check the host name and port number for validity and retry.
- The https protocol is specified, but SSL certificates are not set up properly. (For details on how to set up the SSL certificates, see Configuring TLS/SSL communication with the Authorization Policy Server in the *IBM Tivoli Monitoring Administrator's Guide*.)
- The user ID or password cannot be authenticated with the Authorization Policy Server. For details, see the diagnosis item, "The user name or password that is configured for the portal server connection to the Authorization Policy Server is not correct".
- The user ID has not been granted permission to distribute policies. (For more information, see "Enabling role-based authorization policies" in the *IBM Tivoli Monitoring Administrator's Guide*.)

With regard to a user ID not having permission to distribute policies from the Authorization Policy Server to the dashboard data provider on the portal server, the user ID must be granted permission to retrieve policies. The easiest way to do this is to add the user, or a group that the user belongs to, to the "PolicyDistributor" role. You can verify which users and groups are members of the "PolicyDistributor" role by using the **`tivcmd listroles`** command.

You can see the **User ID** that is configured for the authorization policy download by using the portal server reconfigure function:

> Windows Click **Start** > **Programs** > **IBM Tivoli Monitoring** > **Manage Tivoli Enterprise Monitoring Services**. Right-click the Tivoli Enterprise Portal Server, select **Reconfigure**, and click **OK** to accept the current configuration and open the Authorization Policy Server Configuration dialog box.
>
> Linux UNIX Change to the *`install_dir`*`/bin` directory and run `./itmcmd manage [-h `*`install_dir`*`]`. Right-click the Tivoli Enterprise Portal Server and select **Configure**.

You can also see the user ID in the **`KDQ_GS_POLICY_SERVER_USERID`** environment variable in the portal server environment file:

> Windows Click **Start** > **Programs** > **IBM Tivoli Monitoring** > **Manage Tivoli Enterprise Monitoring Services**. Right-click the Tivoli Enterprise Portal Server and select **Advanced** > **Edit ENV File** to open the kfwenv file.
>
> Linux UNIX Change to the *`install_dir`*`/config` directory and open the `cq.ini` file in a text editor.

To check if the user is a member of the PolicyDistributor role, use the following **`tivcmd`** Command-Line Interface command. A list of members assigned to this role is displayed:

```
tivcmd listroles -n PolicyDistributor -m
```

The user must be explicitly listed or be a member of a group that is explicitly listed. If the user is not explicitly listed or a member of a group that is explicitly listed, the following message is entered in the `SystemOut.log` for the Dashboard Application Services Hub server:

```
KDQPA0044E An authorization error has occurred because you are not
allowed to execute the current command. You must be granted [
distribute ] operation on object type [ role ] for resource [
default ] of resource type [ rolegroup ] to execute the command.
```

The user name or password that is configured for the portal server connection to the Authorization Policy Server is not correct

If the user name or password is incorrect, the following message is entered in the `SystemOut.log` for the Dashboard Application Services Hub server:

```
SECJ0369E: Authentication failed when using LTPA. The exception is
com.ibm.websphere.wim.exception.PasswordCheckFailedException:
CWWIM4529E The password verification for the 'user_name' principal
name failed. Root cause: 'javax.naming.AuthenticationException:
[LDAP: error code 49 - Invalid Credentials]; Resolved object:
'com.sun.jndi.ldap.LdapCtx@825863d4''.
```

As an example, consider a user who has policy authorization enabled on the portal server but encounters the following runtime error when attempting to create a widget:

```
Error: ATKRST100E: An exception occurred, The error message is as
follows:
KFWITM621E The requested resource is currently unavailable, doesn't
exist or authorization is denied.
```

A good first diagnostic step is to look at the portal server audit log, which contains messages about Authorization Policy Server and policy distribution problems.

```
[1/3/13 13:04:26:457 EST] 000000d4 PolicyServer  I
com.ibm.tivoli.monitoring.provider.security.PolicyServer getEntitlements()
Calling getUserResources with allowedOrDenied<true> domain
<itm.HUB_amsntx28>user<cn=svtldap1,ou=users,ou=SWG,o=IBM,c=US>
 user groups<[cn=svtgrp1,cn=svtldap,ou=SWG,o=IBM,c=US]> op<view>
 objType<attributegroup> obj<any>
[1/3/13 13:04:26:458 EST] 000000d4 client        E
com.ibm.tivoli.rest.authz.client.PolicyClientRefreshWrapperImpl
performInitialization Policy store parent root directory has not been set;
the client cannot initialize.
[1/3/13 13:04:26:465 EST] 000000d4 client        E
com.ibm.tivoli.rest.authz.client.PolicyClientRefreshWrapperImpl
getUserResources KDQPC0017E The policy client is not initialized.
The policy client request cannot be processed. The failed policy store
path is [ null ] and the failed policy role path is [ null ] .
[1/3/13 13:04:26:466 EST] 000000d4 PolicyServer  E
com.ibm.tivoli.monitoring.provider.security.PolicyServer
getEntitlements() ERROR:
com.ibm.tivoli.rest.authz.PolicyAuthorizationException
[1/3/13 13:04:26:479 EST] 000000d4 MsysCollectio E
com.ibm.tivoli.monitoring.provider.msys.MsysCollection
getSecurityFilter() getEntitlements using allowed returned empty list
[1/3/13 13:04:26:480 EST] 000000d4 rest          E
com.ibm.tivoli.rest.RestProvidersURI getDatasourceDatasetColumns
unexpected exception:
com.ibm.tivoli.monitoring.provider.navmodel.ITMRuntimeException:
KFWITM621E The requested resource is currently unavailable,
does not exist or authorization is denied       at
com.ibm.tivoli.monitoring.provider.msys.MsysCollection.
getSecurityFilter(MsysCollection.java:298)
```

All of these messages might be a consequence of policy distribution not occurring. To check if the dashboard data provider has authority to download policy information, you can run the following command:

```
tivcmd listroles --rolename PolicyDistributor --showpermissions
--showmembership
```

In this example scenario, assume the following command output:

```
PolicyDistributor
  Users:
  Groups:
  Permissions:
    Domain: any
    Resource Type: rolegroup
    Resource: default
    Object Type: role
    Granted Operations: {distribute}
```

The output indicates that no user has been added to the PolicyDistributor role, which explains why the dashboard data provider could not download policies and why the KFWITM621E message occurred. Note that every time you install a new Authorization Policy Server, you must issue the following command once:

```
 tivcmd addtorole --rolename PolicyDistributor -u "user_configured_for_DP"
```

Latest policy updates not appearing at the portal server

In this scenario, assume that the user configured for the Authorization Policy Server connection was added to the `PolicyDistributor` role, and that policy distribution to the portal server has already occurred successfully one or more times. You notice that the latest policy updates are not available at the portal server. The symptom might be, for example, that a role was recently granted access to a managed system, but the server dashboard continues to prevent a user belonging to that role from viewing the managed system.

When you investigate a problem of this type, it is important to remember that policy updates implemented at the Authorization Policy Server do not appear immediately at the portal server. Two polling intervals influence how quickly the updates are distributed:

- Updates are periodically batched together at the Authorization Policy Server to prepare for subsequent distribution. This process is controlled by the Authorization Policy Server's **`DIST_POLL_INTERVAL`** resource environment property. (For more information, see “Changing the Authorization Policy Server configuration properties after installation and configuration” in the *IBM Tivoli Monitoring Administrator's Guide*.)
- The portal server makes periodic requests to the Authorization Policy Server for the latest updates, as defined by the **`Polling Interval`** parameter in the portal server configuration settings. (For more information, see “Enabling authorization policies in the portal server” in the *IBM Tivoli Monitoring Administrator's Guide*.)

It could take as long as the sum of these two polling intervals for a change made at the Authorization Policy Server to appear at the portal server.

Another potential reason for missing updates at the portal server is that a recent change took effect at the Authorization Policy Server which has impacted policy distribution. Here are some possible changes:

- The password for the Authorization Policy Server user specified in the portal server configuration has expired or was modified and needs to be updated at the portal server.

- The Authorization Policy Server user specified in the portal server configuration is no longer valid or no longer has permission to distribute policies.
- If the https protocol is being used between the portal server and the Authorization Policy Server, the SSL certificates might have expired.

A good first step to determine the cause of the distribution problem is to look at the portal server audit log in the portal client. The audit log might contain messages such as failed login by the Authorization Policy Server user ID, which would indicate that the password for the user ID has expired or been changed.

Another diagnostic step is to check the time stamp of your `*install_dir*/PolicyStoreArchive/argus.zip` file on the dashboard data provider computer (the portal server). After you see a new or current time stamp for `argus.zip`, you can retry the Dashboard command.

Chapter 12. Infrastructure management dashboards troubleshooting

Review these troubleshooting topics for help solving problems related to dashboard display and usage with Infrastructure Management Dashboards for Servers and Infrastructure Management Dashboards for Hypervisors .

Server dashboard trace settings

IBM Infrastructure Management Dashboards for Servers web application has several levels of tracing that you can set while you work with dashboards. You can start a higher level of tracing exactly at the point in the user interface where you are having a problem, then return tracing to a lower level after capturing the necessary log data.

Adjust the trace settings only as directed by your administrator or IBM Support to help diagnose the cause of problems with the server dashboards.

You can set a trace from a server dashboard in the Dashboard Application Services Hub. While displaying the dashboard that you want to change the trace level for, click **Actions** > **Trace level** and select one of the following levels:

- **Verbose** to have all activity logged. Verbose trace level includes Moderate, Light, and Minimal trace logging.
- **Moderate** to have variable changes logged, such as what parameters were passed in and what calculations were made. Moderate trace level includes Light and Minimal trace logging.
- **Light** to log error and variable activity. You might want to set the trace to this level if you have a problem such as no data being returned but the dashboard continues to function. Light trace level includes Minimal trace logging.
- **Minimal** is the default setting and records only unrecoverable errors. You can set the trace level back to minimal after collecting a specific activity sequence. Even if a different trace level was set before logout, the trace is always reset to the lowest level the next time you log in.

The trace is adjusted to the level chosen for this and all subsequent dashboards selected. To keep communications traffic to a minimum, the log messages are transferred in batches to the Dashboard Application Services Hub. A final transfer is made after you log out, whether manually or after a timeout period. (If the browser fails, no final logging is sent.)

The logs are saved on the Dashboard Application Services Hub computer and named *userid*`.log.0` where *userid* is the ID used to log in to the Dashboard Application Services Hub and “0” is the first log. Three log files of 750 KB total are used to record trace data in a cyclical manner: After the *userid*`.log.0` reaches 250 KB, log entries are saved to *userid*`.log.1`; after *userid*`.log.1` reaches 250 KB, log entries go to *userid*`.log.2` until it reaches the maximum, at which time *userid*`.log.0` is cleared and new entries are saved there.

This is the default path to the log files:

Windows `C:\Program Files\IBM\JazzSM\profile\logs\server1`

Linux UNIX `/opt/ibm/JazzSM/profile/logs/server1`

Authentication is required in web application

If you are prompted for a username and password when you access a web page that displays monitoring data, your user id might not be in the federated LDAP registry.

Diagnosis

You are logged in as a user who is not defined in the federated LDAP user registry that is configured for both the Dashboard Application Services Hub and the Tivoli Enterprise Portal Server.

The `SystemOut.log` contains the following error message:

```
SECJ0373E: Cannot create credential for the user <null> due to
failed validation of the LTPA token. The exception is
com.ibm.websphere.wim.exception.EntityNotFoundException: CWWIM4001E
The 'uid=tipadmin,o=defaultWIMFileBasedRealm' entity was not found.
```

Solution

You must log in as a user that is a member of both user repositories. Create a user in the LDAP and log in to the Dashboard Application Services Hub.

Here are some other possible scenarios:

Multiple Dashboard Application Services Hub Servers

When accessing multiple Dashboard Application Services Hub Servers from the same computer, use different browser applications. If you use the same browser in separate tabs or windows, you might be logged out or prompted for authentication in the dashboard that you first logged in to. If you are prompted, select Cancel or enter the single-signon credentials that you used when logging into that dashboard. You will be prompted repeatedly. Close all Dashboard Application Services Hub consoles and Websphere consoles before logging in again.

Unauthorized access or resources unavailable

A common issue is the incomplete configuration of TLS/SSL certificates at the Tivoli Enterprise Portal Server if HTTPS was selected. You might see the following entry in the audit logs:

```
KDQPD0014E A [ POST ] was issued to URL [ HTTPS://[Server
name:16311/ibm/tivoli/rest/providers/AUTHZ/...] SSL_ERROR:
PolicyMessageInfo [ messageId = DIST_SSL_ERROR, ..]
```

Switch to the HTTP protocol by default until certificates are configured. (For details on how to set up the SSL certificates, see Configuring TLS/SSL communication with the Authorization Policy Server in the *IBM Tivoli Monitoring Administrator's Guide*.)

Policy download user not properly authorized

If you are configured for downloading policies but have not been properly authorized to download policies, your user ID must be added to the **`PolicyDistributor`** role. You can optionally use the group that your user ID is also a member of. Use the following command: `tivcmd addtorole -n "PolicyDistributor" -u "[LDAP ID of the user]`

Resource not available or not authorized to see dashboards

If you open the Infrastructure Management Dashboards but get an error message or do not see the dashboard metrics that you expect, review the methods for diagnosing and resolving the issue.

Problem

After logging in to the Dashboard Application Services Hub and selecting **System Status and Health** > **Server Dashboards**, you receive a message saying that you are not authorized to access the view or that the resource does not exist or is not available.

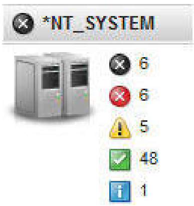
Diagnosis and resolution

The portal server is not able to download authorization policies

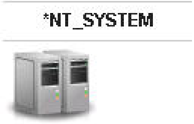
If ☑ **Enable authorization policies** was selected during Tivoli Enterprise Portal Server configuration, but the portal server is not able to retrieve a copy of the policy store from the Authorization Policy Server, dashboard users see error messages instead of dashboard metrics. The diagnosis and resolution for this type of problem are described in "Policy distribution issues" on page 201.

The dashboard user might not be authorized to view event or monitoring data for any managed system groups when authorization policies are enabled

A user with no event access sees no event icons next to the managed system groups, and charts report zero even if real events exist. For example, the following carousel view in the Managed System Groups dashboard shows the *NT_SYSTEM managed system group with a count of situation event severities. The user is authorized to view situation events:



However, in this carousel view of the *NT_SYSTEM managed system group, no events are shown. The user is not authorized to view situation events:



A user with neither event access nor attribute group access for any managed system groups, sees an empty carousel on the Managed System Groups Overview dashboard. You can use the **tivcmd listroles** command to view what roles the user is assigned to and what permissions are assigned to that role:

```
tivcmd listroles -u uid=annette,cn=itm,o=tivoli -p
```

Sample output:

```
NTEventOnly
  Permissions:
    Domain: any
    Resource Type: managedsystemgroup
    Resource: *NT_SYSTEM
    Object Type: event
    Granted Operations: {view}
```

If you determine that the role should have view operation for the **attributegroup** object type, use the **tivcmd grant** command to add this capability:

```
tivcmd grant -n NTEventOnly -t managedsystemgroup -r
*NT_SYSTEM --objecttype attributegroup --operations view
```

Enter **tivcmd listroles** command to view the newly added capability:

```
tivcmd listroles -u uid=jim,cn=itm,o=tivoli -p
```

Sample output:

```
NTEventOnly
  Permissions:
    Domain: any
    Resource Type: managedsystemgroup
    Resource: *NT_SYSTEM
    Object Type: attributegroup
    Granted Operations: {view}
```

If you determine that the role should have view operation for the **event** object type, use the **tivcmd grant** command to add this capability:

```
tivcmd grant -n NTDataOnly -t managedsystemgroup -r
*NT_SYSTEM --objecttype event --operations view
```

If Tivoli Enterprise Portal permissions and application assignments are being used instead of authorization policies, the dashboard user's Tivoli Enterprise Portal user ID might not be assigned any agent applications

If the portal server's environment file has the following variable setting, the system is using portal server authorization: **KDQ_GS_ENABLE_POLICY_AUTH=N**.

You can also use the portal server reconfigure function to see whether the **Enable authorization policies** check box disabled (this is the default).

The dashboards show no situation events or data metrics for any managed system types that are not in the user's Allowed Applications list. If a managed system group contains any managed systems of a type that the user is not allowed to see, the following error is displayed instead of chart and table data:

```
An unexpected error occurred. The error message is as
follows:
'com.ibm.tivoli.monitoring.provider.viewmodel.database.
ViewModelDBExceptionKFWITM633E Exception: KFWITM714E Cannot
get allowed user Affinity'.
```

You can add more managed system types to the Allowed Applications for users by editing their profiles, as described in “Using Tivoli Enterprise Portal user authorization” in the *IBM Tivoli Monitoring Administrator's Guide*.

Situation event results don't display

If you can see events in the Situation Events dashboard but not the event details when you open the situation event results dashboard, you might have limited permissions.

Problem

You are able to see events listed in the Situation Events dashboard and other dashboards with event views. However, when you click the link in the Situation Name column to open the event results, you get the following error, but only if the associated error displays charted data.

```
KFWITM621E The requested resource is currently unavailable, does not
exist or authorization is denied.
```

Diagnosis

Permissions controlled by the Authorization Policy Server
You have not been assigned permission to view monitoring data using authorization policies.

Permissions controlled by the Tivoli Enterprise Portal Server
Your Tivoli Enterprise Portal user ID does not have permission to view events or does not have permission to see the same managed system type that you are attempting to view the situation event results from.

Resolution

Permissions controlled by the Authorization Policy Server
You can use the **tivcmd listroles** command to view what roles the user is assigned to and what permissions are assigned to that role:

```
tivcmd listroles -u uid=annette,cn=itm,o=tivoli -p
```

Sample output:

```
NTEventOnly
  Permissions:
    Domain: any
    Resource Type: managedsystemgroup
    Resource: *NT_SYSTEM
    Object Type: event
    Granted Operations: {view}
```

If you determine that the role should have view operation for the **event** object type, use the **tivcmd grant** command to add this capability:

```
tivcmd grant -n NTDataOnly -t managedsystemgroup -r
*NT_SYSTEM --objecttype event --operations view
```

Enter **tivcmd listroles** command to view the newly added capability:

```
tivcmd listroles -u uid=jim,cn=itm,o=tivoli -p
```

Sample output:

```
NTEventOnly
  Permissions:
    Domain: any
    Resource Type: managedsystemgroup
    Resource: *NT_SYSTEM
    Object Type: attributegroup
    Granted Operations: {view}
```

Permissions controlled by the Tivoli Enterprise Portal Server
Edit your user ID to add Events - View permission and, if applicable, the managed system type included in **Allowed Applications**. For details, see “Using Tivoli Enterprise Portal user authorization” in the *IBM Tivoli Monitoring Administrator's Guide*.

Dashboards and portal client show different resources

If you see different managed resources in the dashboards from what you see in the Tivoli Enterprise Portal, review the possible causes.

The Dashboard Application Services Hub is using a dashboard data provider connection that is not configured to support single sign-on

In this case, dashboard authorization is through the user ID that is configured for the dashboard data provider connection but the Tivoli Enterprise Portal client authorization is using the ID of the user who is logged into the client.

You are using authorization policies to control dashboard access and Tivoli Enterprise Portal permissions to control access for the portal client

This can occur if the permissions are inconsistent or if the authorization policies are more restrictive.

Example of more restrictive authorization policies: Assume users are granted permission to view a subset of Windows OS agents in the Dashboard Application Services Hub using authorization policies and they are assigned the Windows OS application type in their Tivoli Enterprise Portal permissions. The users see the authorized Windows OS agents in the dashboards but they see all Windows OS agents in the Tivoli Enterprise Portal client.

Example of inconsistent permissions: Assume users are granted permission to view a subset of Windows OS agents in the Dashboard Application Services Hub using authorization policies, but they are not assigned the Windows OS application type in their Tivoli Enterprise Portal permissions. The users see their authorized Windows OS agents in the dashboards, but they will see no Windows OS agents when they access the Tivoli Enterprise Portal client.

Authorization is through the Tivoli Enterprise Portal Server or through the Authorization Policy Server

If the portal server's environment file has the following variable setting, the system is using Tivoli Enterprise Portal Server authorization to control resource access for the server dashboards and for the portal client: `KDQ_GS_ENABLE_POLICY_AUTH=N`. The user's permissions are managed through the Administer Users function.

If the portal server environment file has the following variable setting, the system is using Authorization Policy Server policies to control access to resources in the server dashboards and Tivoli Enterprise Portal authorizations to control resource access in the portal client: `KDQ_GS_ENABLE_POLICY_AUTH=Y`. Use the following tivcmd Command-Line Interface command to determine what the permissions are: **`tivcmd listroles -n PolicyDistributor -m`**

No data or only partial data is displayed

While displaying the Infrastructure Management Dashboards for Servers, you see only partial data from a managed system group. When you drill down to details, no data might be displayed.

Diagnosis

There might be a misspelled managed system or managed system group name in an authorization policy. Also managed system names and managed system group names are case sensitive. Therefore, resource name case mismatches between the authorization policies and the names used by the hub Tivoli Enterprise Monitoring Server and Tivoli Enterprise Portal Server can also result in a resource not being displayed in the dashboard.

Check for dashboard error messages and any suggested response, and check permissions if a user is not seeing the expected data in the dashboards.

Solution

Use the following **tivcmd** Command-Line Interface command to list the permissions that are assigned to the roles for a user who is not seeing the expected resources:

```
tivcmd listroles -u username -p
```

Compare the resource names to the names displayed by running the **tacmd listSystems** and **tacmd listSystemList** Command-Line Interface commands.

See the *IBM Tivoli Monitoring Command Reference* (http://pic.dhe.ibm.com/infocenter/tivihelp/v61r1/topic/com.ibm.itm.doc_6.3fp2/ic/landing_cmdref.htm).

User's authorization policy updated but not showing in dashboards

An authorization policy administrator just updated a dashboard user's authorization but the user is not seeing the expected resources and data in the monitoring dashboards.

Diagnosis

Policy updates take place based on to two properties: the Tivoli Enterprise Portal Server polling interval to check for changes, which has a default setting of 30 minutes, and the Authorization Policy Server timer to zip up the policies, which has a default setting of 5 minutes.

Resolution

You can edit the configuration of the Tivoli Enterprise Portal Server or the Authorization Policy Server or both. Policy updates take place based on the following polling intervals:

- The portal server has a default interval of 30 minutes for checking the Authorization Policy Server for changes. (For details on reconfiguring the portal server authorization policy settings, see “Enabling authorization policies in the portal server” in the *IBM Tivoli Monitoring Administrator's Guide*.)
- The Authorization Policy Server uses a Policy distribution polling interval (minutes), which is set to 5 minutes by default. (See “Configuring the Tivoli Authorization Policy Server feature after installation” in the *IBM Tivoli Monitoring Installation and Setup Guide*.)

These are configurable values either at installation time or during post-installation configuration. You can review the portal server audit log, which is available in the Tivoli Enterprise Portal “Audit Log” Enterprise-level workspace. The log shows when the poll to get the latest polices occurred or when the last policy check took place. Based on this information and the existing settings, you can estimate the effective polling intervals.

Situation events not updated after changes to security policy or group membership

After editing a managed system group to add or remove managed systems, you don't see the updates reflected in the Situation Events table. Similarly, although your user security policy was edited, the event listing doesn't change to reflect the current permissions.

Problem
The Situation Events table is not automatically updated after a change to the user security policy or a change to the managed system group membership that might affect the events that the user is able to see.

Resolution
Refresh the dashboards page by clicking the browser Refresh button or log out of the Dashboard Application Services Hub. Log in to the Dashboard Application Services Hub console again, click **System Status and Health** > **Server Dashboards** and select **Situation Events**.

Unable to communicate with data provider

If you get a `CTJSD201E - Unable to establish communications with the data provider server` message when opening a dashboard, review the diagnosis and resolution.

Diagnosis
The `CTJSD201E - Unable to establish communications with the data provider server` message indicates that the dashboard cannot communicate with the IBM Tivoli Monitoring dashboard data provider.

You can open the Dashboard Health Checks to run a health check of your infrastructure management dashboard components and report their status: Click **System Status and Health** > **Dashboard Health Checks**. The connection to the dashboard data provider on the Tivoli Enterprise Portal Server is checked and the results are shown in the Tivoli Monitoring table.

Also, confirm the following settings and condition:

- In the Dashboard Application Services Hub, click ⚙ **Console Settings** > **Connections** and check that the provider ID for the IBM Tivoli Monitoring dashboard data provider is set to **`ITMSD`**.
- Confirm that the Tivoli Enterprise Portal Server `KfwServices` process is running.
- Confirm that the dashboard data provider is enabled in the portal server configuration: In Manage Tivoli Enterprise Monitoring Services, right-click the portal server and click **Reconfigure**. The ☑ **Enable the dashboard data provider** check box should be selected.

If you have not found the problem, investigate connectivity issues between the portal server and the Dashboard Application Services Hub.

Solution
After taking any required actions to ensure that the dashboard data provider ID is set to **`ITMSD`**, the portal server is running, it has been set to enabled the dashboard data provider, and that communications with the Dashboard Application Services Hub is working, close the dashboard open it again to clear the error message.

Chapter 13. Monitoring agent troubleshooting

Review the monitoring agent troubleshooting topics for descriptions of problems you might experience with the monitoring agent deployment 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.

Startup failure with older agents

IBM Tivoli Monitoring V6.3 introduces a new version of IBM GSKit Security Interface 8 (gs). Monitoring agents use IBM Tivoli Monitoring Shared Libraries (ax) to utilize the GSKit library. Only Tivoli Monitoring Shared Libraries V6.3 or later supports GSKit 8.

If you encounter a problem with starting older monitoring agents in a Tivoli Monitoring V6.3 or later environment, verify that all Tivoli Monitoring Shared Libraries are at the 6.3 level.

Problem determination

Check which version of the Tivoli Monitoring Shared Libraries you are using if older monitoring agents are not starting in your V6.3 or later environment. Run the `cinfo -t ax` command. Example of the command and output:

```
# ./cinfo -t ax
***********************************************************
User: root Groups: root bin daemon sys adm disk wheel
Host name : hostname Installer Lvl:06.30.00.00
CandleHome: /opt/IBM/ITM
Version Format: VV.RM.FF.II (V: Version; R: Release; M: Modification;
 F: Fix; I: Interim Fix)
***********************************************************
...Product inventory

PC PRODUCT DESC PLAT VER BUILD INSTALL DATE

ax IBM Tivoli Monitoring Shared Libraries li6263 06.21.04.00 - -
ax IBM Tivoli Monitoring Shared Libraries lx8263 06.21.04.00 - -
ax IBM Tivoli Monitoring Shared Libraries lx8266 06.30.00.00 - -
```

Solution

If at least one component is older than Tivoli Monitoring V6.3 you must upgrade it to latest version. There are two ways to upgrade:

- Start the installer with a Tivoli Monitoring V6.3 or later agents image. Before the component selection menu is displayed, the installer ask you to upgrade the Tivoli Monitoring Shared Libraries to the latest version. Sample display:

  ```
  The following prerequisites should be installed now:
  IBM Tivoli Monitoring Shared Libraries V630R100 @
    Linux Intel R2.6 (32 bit)
  IBM Tivoli Monitoring Shared Libraries V630R100 @
    Linux x86_64 R2.6 (32 bit)

  Do you want to install these prerequisites
    [ 1=Yes, 2=No ; default is "1" ] ?
  ... installing package "axli6263"; please wait.
  ```

```
=> installed package "axli6263".
... installing package "axlx8263"; please wait.

=> installed package "axlx8263".
```

Select 1 to upgrade the libraries. You can quit the installation on the next menu.

- Install the Tivoli Enterprise Services User Interface Extensions component. You must force the operating system version during installation. In this example, you must install Tivoli Enterprise Services User Interface Extensions for the following systems: Linux Intel R2.6 (32 bit) and Linux x86_64 R2.6 (32 bit) After completion, all the Tivoli Monitoring Shared Libraries should be at the 6.3 level.

```
# ./cinfo -t ax
***********************************************************
User: root Groups: root bin daemon sys adm disk wheel
Host name : hostname Installer Lvl:06.30.00.00
CandleHome: /opt/IBM/ITM
Version Format: VV.RM.FF.II (V: Version; R: Release; M: Modification;
F: Fix; I: Interim Fix)
***********************************************************
...Product inventory

PC PRODUCT DESC PLAT VER BUILD INSTALL DATE

ax IBM Tivoli Monitoring Shared Libraries li6263 06.30.00.00 - -
ax IBM Tivoli Monitoring Shared Libraries lx8263 06.30.00.00 - -
ax IBM Tivoli Monitoring Shared Libraries lx8266 06.30.00.00 - -
```

Command-line interface

Review the command-line interface troubleshooting descriptions for help with tacmd usage.

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
```

Historical data

If historical data is not being collected in the short-term history file or being warehoused properly or you have other issues with data collection, review the possible cause and solution that correspond to your symptoms

Historical data is not collected for Agent Operations Log and ITM Audit

OMEGAMON XE monitoring agents cannot store short-term historical data for the Agent Operations Log and ITM Audit attribute groups at the agent. Historical collection for these attributes must be stored at the Tivoli Enterprise Monitoring Server; not the agent.

Managing System (TEMS)Managed System (Agent) When configuring historical data collection for an agent type, you set the distribution ITM Historical Data Collection, the following attribute groups can not successfully be stored at the agent when an agent runs on the z/OS platform. CCC Logs - Agent Operations Log CCC Logs - ITM Audit This is a limitation in the current implementation of ITM history collection for these attribute groups that should be fixed in a future release. The following error messages will be visible in the z/OS agent RAS1 log (RKLVLOG) when this problem occurs: 2012.058 19:03:39.69 (0034-D8CDE7B3:kraahbin.cpp,977,"ConnectToPDS") Unable to locate table KRAAUDIT 2012.058 19:03:39.69 (0034-D8CDE7B3:kraahbin.cpp,977,"ConnectToPDS") Unable to locate table OPLOG Work-Around: When history collection data is required from any z/OS agent for either CCC Logs - Agent Operations Log CCC Logs - ITM Audit configure Historical Data Collection for storage at the TEMS rather than the agent.

Take action commands and reflex automation

Attributes differ between the situation action commands and what is displayed in the portal client

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 editor's **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:

```
my_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:

```
my_command Warning too many processes 699 options
```

Using &{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 (\).

IBM Tivoli Monitoring V6.2.2 FP6 IZ98638 does not support reflex actions for OMEGAMON XE agents on z/OS

You might encounter a problem using reflex actions for your OMEGAMON XE agents on z/OS. Note that IBM Tivoli Monitoring V6.2.2 FP6 IZ98638 does not support reflex actions for OMEGAMON XE agents on z/OS.

Take action command names do not accept non-English characters

There is not a workaround at the present time.

Workspaces

Review the monitoring agent workspaces entries for a description of problems in the Tivoli Enterprise Portal with accessing and displaying workspaces.

AMS workspace remains unavailable, even if the OS Agent is started

You might notice that the Agent Management Services (AMS) workspace remains unavailable, even if the OS agent is started. Changes to the behavior of the login process make the Proxy Agent Service (PAS) initialization asynchronous. The AMS workspace remains unavailable until PAS initialization completes. This is an expected behavior.

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.

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.

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.

OS agents

Review the OS agent entries for a description of configuration and usage problems and how to resolve them.

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.

OS agent start command fails

If you receive an error message indicating that your OS agent start command has failed, you might have exceeded the maximum number of supported processes while using the IP.PIPE network protocol.

The host using the IP.PIPE network protocol is limited to 16 Tivoli Monitoring processes.

You can identify the issue by noting the agent server process exiting unexpectedly with the following key messages:

```
(4E85BA02.005E-1:kdcsuse.c,119,"KDCS_UseFamily") status=1c010005,
"cant bind socket", ncs/KDC1_STC_CANT_BIND_SOCK
(4E85BA02.005F-1:krabrreg.cpp,1289,"CTRA_reg_base__Load") Use family failed,
family=34, st=1c010005
(4E85BA02.0060-9:kde12li.c,189,"KDE1_ServerListen") Status 1DE0002C=
KDE1_STC_SERVERNOTBOUND
(4E85BA02.0061-9:kdcs1li.c,126,"Listen") KDE1_ServerListen(0x1DE0002C)
(4E85BA02.0062-1:kraaumsg.cpp,143,"CTRA_msg_server_exit_status")
CTRA Server: exit status, 0
```

These messages indicate that the server cannot bind a socket and that the server is exiting. This behavior is a known limitation.

Specific events are not monitored by the Windows OS agent

You might encounter a problem monitoring specific events with the Windows OS Agent.

When running IBM Tivoli Monitoring V6.2.3 Fix Pack 1 (or later), you have the capability to display events and event data from any event log you are monitoring. However, the `Log Name` and `Log Name (Unicode)` attributes represent input fields, not output fields. Filtering on the event log name is not supported. You must specify the exact name of the event log you want to monitor.

The Windows Registry Editor lists the event log name as a key in either of two paths:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Eventlog
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\WINEVT\
Channels
```

The name of the event log is the key listed under the Eventlog or Channels key. For example, the Internet Explorer event log has the key HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Eventlog\Internet Explorer and the Channels\Microsoft-Windows-TaskScheduler/Operational event log channel has the key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\WINEVT\Channels\Microsoft-Windows-TaskScheduler/Operational

Windows OS agent doesn't connect to the monitoring server

If you have a Windows OS agent V6.2.*x* installed on a 64-bit Windows 2008 system, it connects to the Tivoli Enterprise Monitoring Server only if Windows is started under the Administrator user ID.

Symptom
The agent starts successfully and shows as running in the Manage Tivoli Enterprise Monitoring Services user interface, but remains in the offline state when viewed in the Tivoli Enterprise Portal.

Solution
Start the Windows system where the agent is installed with the Administrator user ID.

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.

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.

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.

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.

Installing backlevel Windows OS agent on existing environment causes 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 target host name, platform, and version information is not displayed for the deployment status in the CLI or the workspace

Target host name, platform, and version information is not displayed for the deployment status in the CLI or the workspace. For group commands, the target host name, 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 : 1222782542297000000015724
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 : 1222782542297000000015724
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
```

Deploy cannot tell if the installation 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.

Warehouse agents

Review the warehouse proxy agent and summarization and pruning agent topics for help with configuration and usage problems.

Configuring the Summarization and Pruning Agent with an incorrect JDBC driver JAR file

If you add an incorrect JDBC driver JAR file when configuring the Summarization and Pruning Agent, an error message is displayed after you click Test Connection. The error message continues to display, even after you have replaced the file with the correct one. This behavior is a known limitation. Close the configuration panel and run the configuration again.

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).

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

When your Tivoli Enterprise Monitoring Agent at V6.2.3 or later is configured to be self-describing, it has all the required application support files to update the Tivoli Management Services servers. You do not have to perform manual support installation steps and recycle each individual server component that will support the agent.

Getting diagnostic information

To troubleshoot any problems with the self-describing agent capability, verify that it is configured correctly and enabled, and that communications are functioning properly.

Procedure

1. Verify that all appropriate self-describing environment variables are enabled.
2. Verify that the remote monitoring server is started and connected to the hub monitoring server.
3. The agent must also be enabled for self-description by packaging application support as part of the agent installation. The agent must use the IBM Tivoli Monitoring V6.2.3 or later agent framework or be installed on a system where the V6.2.3 or later agent framework is already installed. You can tell if an agent is enabled for self-description before installation or after installation. See “Determining if agents are enabled for self-description” in the *IBM Tivoli Monitoring Administrator's Guide*.
4. Run the following **`tacmd`** commands and review the results:

   `tacmd listappinstallrecs`
   The `STATE` column displays the state of the self-describing installation for each product package on each monitoring server. A `STATE` value of `ME` indicates a terminal error and that the installation is not automatically tried again.

   `tacmd listSdaInstallOptions`
   Reports what versions of each product are allowed to perform self-describing installations and what the default setting is. Check the allowed versions.

   `tacmd listSdaStatus`
   Reports the `STATE` and `STATUS` of self-describing enablement at each online monitoring server and reports whether self-describing is suspended.

   `tacmd listSdaOptions`
   Check the self-describing product seed definitions.

   For detailed steps, see “Self-describing agent installation” in the *IBM Tivoli Monitoring Administrator's Guide*. For a detailed description of the tacmd commands and options, see the *IBM Tivoli Monitoring Command Reference* (http://pic.dhe.ibm.com/infocenter/tivihelp/v61r1/topic/com.ibm.itm.doc_6.3fp2/ic/landing_cmdref.htm).
5. Review the appropriate monitoring component audit log:

   Tivoli Enterprise Monitoring Server
   Look at the monitoring server audit log to determine whether

self-description is enabled at the monitoring server that the agent connects to. The monitoring server audit log can inform you if self-description is disabled because of the `KMS_SDA` setting at the local monitoring server or hub monitoring server. There might also be other configuration errors at the local monitoring server or hub monitoring server that are causing a problem.

Tivoli Enterprise Portal Server
Look at the portal server audit log to verify that the agent's self-describing files were processed successfully at the portal server. Install successes or errors are displayed for the application support for the Tivoli Enterprise Portal Server (TPS) and the Tivoli Enterprise Portal browser client (TPW).

Tivoli Enterprise Monitoring Agent
Look at the monitoring agent audit log for any installation errors. For more information, see "Audit logging" in the *IBM Tivoli Monitoring Administrator's Guide*.

Table 16. Audit log messages that might alert you to an agent-related self-describing problem

Return code	Message description
KRAA0008	`Validation failed for Self-Describing Agent manifest file` *`variable`* `PRODUCT` *`variable`*`.` This message indicates that a validation error occurred and that the agent is not able to provide SDA support. See the Audit log and RAS1 for other similar messages that indicate the specific SDA manifest file validation error. After correcting the error, recycle the agent to participate in SDA processing.
KRAA0015	`Self-Describing Agent function disabled for PRODUCT` *`variable`* `due to local SDA file validation error.` This message indicates that agent SDA status is disabled due to manifest file validation error. This condition can occur at agent startup time, or while the agent is running and asked to provide SDA support. After the error condition is corrected, the agent must be recycled to enable its SDA function.
KRAA0016	`Ignoring TEMA_SDA Configuration! Agent SDA package not found for PRODUCT` *`variable`*`.` This message indicates that the TEMA_SDA=Y setting is ignored because the agent SDA package was not found. Set the variable only when an agent is packaged with SDA support files.
KRAA0017	`Self-Describing Agent function disabled, expected TEMA_SDA configuration not found for PRODUCT` *`variable`*`.` This message indicates that SDA is disabled because TEMA_SDA configuration was not set (although the SDA package exists). This variable is required for the agent to provide its SDA support.

See the *IBM Tivoli Monitoring Messages* (http://pic.dhe.ibm.com/infocenter/tivihelp/v61r1/topic/com.ibm.itm.doc_6.3fp2/ic/landing_messages.htm) for detailed information about all the KRAA messages.

Solving common problems

Review the symptoms and solutions if you encounter a problem in an environment where the self-describing capability has been enabled.

About this task

Complete any of the following steps that correspond to your symptoms.

Procedure

- If the situation event console is not available in the Tivoli Enterprise Portal because you chose not to initially install any application support on the Tivoli Enterprise Portal Server, and then application support was added through self-describing agents, reconfigure the portal server.
- If you receive a parsing failure on the Tivoli Enterprise Console because baroc files have become out of sync with the changed attribute and catalog files, complete the following steps:
  1. Copy the baroc files from the monitoring server `<install_dir>/tables/<tems_name>/ TECLIB` file path to the Tivoli Enterprise Console server location.
  2. Import and compile the updated baroc files in the Tivoli Enterprise Console rulebase. See "Installing monitoring agent .baroc files on the event server" in the *IBM Tivoli Monitoring Installation and Setup Guide* (http://pic.dhe.ibm.com/infocenter/tivihelp/v61r1/topic/com.ibm.itm.doc_6.3fp2/install/itm_install.htm).

What to do next

See also “Missing agent managed system group in a hot standby environment” on page 88.

Self-describing agent operations no longer function for remote monitoring server in a hot standby environment

While you are using the self-describing agent tacmd commands in a Tivoli Monitoring V6.3 or later hot standby environment, it is possible for the self-describing agent operations on a V6.3 or later remote Tivoli Enterprise Monitoring Server to stop functioning.

Problem

Your hot standby monitoring environment is at V6.3 and you are running self-describing agent tacmd commands other than **`listSdaInstallOptions`** and **`listSdaStatus`**. It is possible for the self-describing agent operations on a V6.3 remote monitoring server to stop functioning. Self-describing enabled agents connected to this remote monitoring server do not perform the expected self-describing agent installation at the remote monitoring servers or the hub monitoring server.

The results of the **`tacmd listappinstallrecs`** command for this remote monitoring server might show that the running self-describing agents should perform their self-describing agent installation. The eligible self-describing agents might show that their self-describing agent installation has been blocked by this remote monitoring server with the following error message:

```
1130204230238980KRAA0003 Self-Describing Agent Register/Install
failed with STATUS (1024/SDA Install Blocked) for PRODUCT "R4", with
TEMS "RTEMS_amsntx10", VERSION_INFO
"product_vrmf=06230100;tms_package_vrmf=06230100;
tps_package_vrmf=06230100;tpw_package_vrmf=06230100;"
```

This can occur even if the **`tacmd listsdastatus`** command shows that the self-describing agent is operational and not in a suspended state, or the

tacmd listsdainstalloptions command shows that the product should be allowed to install the self-describing agent capability. You can confirm this issue by reviewing the remote monitoring server RAS1 log for the following information:

A remote monitoring server that has switched to a different hot standby hub monitoring server shows the following ko4ib and kdshub1 messages:

```
51097285.0009-B:ko4ib.cpp,10503,"IBInterface::selectHub") Selected
TEMS <HOT_Standby> as the HUB(51097285.000D-
B:kdshub1.c,1407,"CheckHubInitTime") HUB set to nodename:
<HOT_Standby>, socket address: <ip.pipe:#9.12.345.12[1918]>,
initTime: <1359566682>
```

If you can't find the following kfasd* messages subsequently in the log, you likely have this problem.

```
(51097285.000E-17D:kfasdise.c,172,"KFASDM_IsSDMenabledAtHub") HUB
feature level <2>(51097285.000F-
17D:kfasdsrm.c,2773,"KFASDM_ProcessSuspendState") Info: SDA suspend
already set to <YES>. No action taken.
```

Resolution

Recycle the remote monitoring server that is experiencing the problem to resume self-describing agent capability. Note, however, that in the current release the following limitations remain and cannot be corrected:

- The self-describing agents connected to the same monitoring server no longer install product support at the hub monitoring server and the portal server.
- The tacmd commands for the self-describing agent show the wrong results

Local history migration tools move the agent operation logs to multiple agent history locations

If you upgrade your Tivoli Enterprise Monitoring Server and Tivoli Enterprise Portal Server 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
- KRAMESG
- KRAMESG.hdr
- OPLOG
- OPLOG.hdr

Only the agent that records into the specific directory will record history into the file. The other agents 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 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.

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.

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.

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.

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`

The Agent Service Interface is not globalized

This window is only displayed in English. There is not a workaround for this issue.

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.

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 host name. 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 host name 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
```

Agent upgrade and restart using non-root

About this task

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 deployment 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

About this task

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 deployment operations are not completing before the TIMEOUT expires

When you are running agent deployment operations, TIMEOUTs can occur because of slow network connections or slow hardware.

The agent deployment operations can complete if you increase the TIMEOUT value. Some operations can complete even after a timeout is returned.

Table 17. Resolutions for agent deployment 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.

Table 17. Resolutions for agent deployment operations that TIMEOUT (continued)

Problem	Resolution
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`
KUICCN068E error when running tacmd createnode.	Increase the timeout value in seconds by adding "-o TIMEOUT=3600" to the **createnode** command.

An agent does not display in the portal client or in the output from the listSystems command

About this task

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 host name
- Agent product node type

An agent name truncation problem can occur when the network domain name is included in the network host name portion of the agent name. For example, instead of just the host name myhost1 being used, the resulting host name 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\Kproduct_codeCMA.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: `/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 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 `K`*`AGENT_CODE`*`KENV` 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 Kproduct_codeENV.
   - 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 portal client

About this task

This problem has been seen in monitoring 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\Kproduct_codeCMA.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 is displayed when configuring the run-as user name for an agent

The error message KDY1024E is displayed 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* (http://pic.dhe.ibm.com/infocenter/tivihelp/v61r1/topic/com.ibm.itm.doc_6.3fp2/install/itm_install.htm).

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"/>
```

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 portal client Navigator view

TheTivoli Enterprise Portal Navigator does not update automatically when an agent is installed to or uninstalled from the managed system. You must click **Refresh** (or press F5) to display changes.

An agent displays unavailable in the portal client

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 host name 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 host name.

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 item 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 tab of the Properties editor. Whatever expression is assigned to the target workspace property through the Link Wizard will override the Title text entered in the Style tab when the workspace is reached through the link.

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 following `lslpp`: message might be displayed: `Press Enter to continue viewing the licenseagreement, or enter "1" to accept the agreement, "2" to decline it, "3" to print it,"4" to read non-IBM terms, or "99" togo 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 installation normally pauses for a number of seconds, causing a tendency to think the installation 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.

**** MISSING FILE ****

This file was generated during the publishing process

Chapter 14. Command troubleshooting

Review the command troubleshooting topics when you have issues using commands in the CLI or take action commands.

Related concepts:

Chapter 9, "Monitoring server troubleshooting," on page 161

Command line interface cannot be found or started

If you have a browser window open during first-time installation of Tivoli Monitoring components, you cannot log in to the command line interface (tacmd login) after installation is complete.

Symptom

With the same browser window open after the installation is complete, you get one of the following messages after entering the tacmd login command:

```
Unable to locate component
The program can't start because KBB.dll is missing from your computer.
Try reinstalling the program to fix this problem.
```

Solution

Open a new browser window before logging in to the CLI and entering commands.

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 where the short-term history files are stored.

For more information about the krarloff command, see the topic on converting files using the krarloff program in the *IBM Tivoli Monitoring Administrator's Guide* (http://pic.dhe.ibm.com/infocenter/tivihelp/v61r1/topic/com.ibm.itm.doc_6.3fp2/adminuse/itm_admin.htm).

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.
```

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}
```

Take Action command names do not accept non-English characters

There is not a workaround at the present time.

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.

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.

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.

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 commands

When the results of running a tacmd are not what you expected, review the symptoms and possible solutions.

Prerequisite checks

Review the prerequisite checks troubleshooting scenarios if you have trouble with completion of the **tacmd checkprereq** command, **tacmd createnode** command with the **-o EXECPREREQCHECK=Y** option, or the OS Agents Report Prerequisites Scanner report.

Checking prerequisites on Windows Server 2012

If you are running Windows Server 2012, you must have .Net Framework V3.5 (or later) installed to use the **tacmd checkprereq** command or to run the OS Agents Report Prerequisites Scanner report provided by the OS agents report package (see "Tivoli Common Reporting" in the *IBM Tivoli Monitoring Administrator's Guide*).

Checkprereq processes do not complete on Linux or UNIX

If a prerequisite check is executed for an agent on a Linux or UNIX endpoint, either with the **tacmd checkprereq** command or the **tacmd createnode** command with the **-o EXECPREREQCHECK=Y** 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 environment, 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).

Slow tacmd command response in large scale environments

In environments with many managed systems, you might get slow response when running commands such as **tacmd cleanMS** or **tacmd listSystems**.

tacmd cleanMS
: In large-scale environments with a significant number of managed systems (for example, 10-20 thousand), using the **tacmd cleanMS** command or removing a managed system through the Tivoli Enterprise Portal can take several seconds to complete. If the **-a** option is used with the **tacmd cleanMS** command and there are many offline nodes, the command might take many minutes or hours to complete.

tacmd listSytems
: In large-scale environments with many managed systems, high CPU consumption is the expected behavior for the **tacmd listSytems** command

KDH1_RequestActivity unsuccessful, rc: 0x7c4c8001D, in a long-running tacmd

If the tacmd Command-Line Interface fails to complete a command because of a timeout limit, ensure that the hub Tivoli Enterprise Monitoring Server is started before any other IBM Tivoli Monitoring processes on the same system.

Diagnosis

The symptom of this problem is that the kuiras1.log file contains the following error message after a failed tacmd:

```
"KDH1_RequestActivity unsuccessful, rc: 0x7c4c8001,
, type=Fail, status=1, HTTPstatus=0"
```

The error signifies that the command's timeout limit was exceeded. The tacmd CLI program sets a 10 minute timeout to accommodate long-running sub-commands, such as **tacmd viewDepot**, and long-running scripts invoked by **tacmd executecommand**.

However, this timeout problem can still occur if the hub monitoring server does not own the well-known SOAP Server listening ports 1920 and 3661 because another Tivoli Monitoring process on the same system has acquired those ports first. There is a default two minute TCP timeout in effect between the hub monitoring server and the Tivoli Monitoring process that owns 1920 and 3661. The tacmd command failure occurs if that two-minute timeout limit is exceeded.

Resolution

Guarantee that the hub monitoring server is the owner of the 1920 and 3661 ports:

- Ensure that the hub monitoring server is always the first IBM Tivoli Monitoring process started on a system.
- If the hub monitoring server is recycled, other Tivoli Monitoring processes on the same computer must also be recycled, with the hub monitoring server restarted first so that it can acquire the 1920 and 3661 ports.

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.

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.

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.

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>0008000000000000000000000000000000000000000</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>0008000000000000000000000000000000000000000</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 \;
```

Problem running the tacmd listSystems command on Linux and UNIX

When you are running the **`tacmd listSystems`** command on Linux or UNIX, it is possible that no data is returned in environments with a large number of managed systems.

Diagnosis

When running the **`tacmd listSystems`** command on a Linux or UNIX system, you might encounter a situation whereby no data is returned. This can happen in monitored environments that have a large number of managed systems.

Solution

Consider increasing the **`ulimit -d`** setting (**`data size`** or **`data seg size`**). See the system documentation for the command (usually **`ulimit`**) and procedures to make this change permanently across system restarts, or contact your UNIX or Linux System Administrator.

To display the current user limits, use the **`ulimit -a`** command, as described in "Check ulimit settings for open file descriptors" in the *IBM Tivoli Monitoring Installation and Setup Guide*.

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'.

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 website: . Measurement experience has shown that this setting can significantly improve the tacmd command response time on VMWare ESX systems.

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.

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 removeBundles command returns unexpected 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.

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.

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.

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.

Corrupted tacmd responses are displayed in the command-line interface

About this task

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

Procedure

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

Country	Code Page Default Setting	New Code Page Value
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.

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"/>
```

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.

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.

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 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.

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 **addBundles** command.

You can also change the LAN linkspeed and duplex setting from auto detect to 100Mbps/Full Duplex. Then re-start the addbundle process.

tacmd createNode

If the **createNode** command fails, it might be because of the syntax or a connectivity issue. Review the possible causes and resolutions to help you recover.

Windows 7 and Windows 8

You are able to run the **tacmd addBundles** command for the Windows OS agent, but when you try to deploy the agent with **tacmd createNode** on the Windows 7 and Windows 8 computers, the command fails.

Cause

The problem is related to being able to connect to the endpoint.

Solution

1. Enable Remote Registry:
   a. Click **Administrative Tools** > **Services**.
   b. Double-click "Remote Registry" (or right-click it and select **Properties**).
   c. In the **General** tab, set **Startup type** to **Automatic** and click **OK**.
2. Disable password protected sharing:
   a. Click **Control Panel** > **Network and Sharing Center** > **Advanced sharing settings**.
   b. In "Password protected sharing" area, select the **Turn off password protect sharing** radio button and click **Save changes**.
3. If you have a domain user account, ensure that the local and the target machine are both members of a Windows domain.
4. If you are a member of a local administrators group and you use a local user account, complete the following steps on the local computer to enable administrative tasks on the target computer:
   a. Click **Administrative Tools** > **Local Security Policy**.
   b. Expand **Security Settings** > **Local Policies** > **Security Options**
   c. To enable the built-in Administrator account for connecting to the target computer, double-click "Accounts: Administrator account status" and select the **Enabled** radio button.
   d. If a different Administrator user account is to be used to connect to the target computer, double-click "User Account Control: Run all administrators in Admin Approval Mode" and select the **Disabled** radio button.
   e. Click **OK**.

Windows OS agent from a UNIX or Linux host when using the "-d" option and "\" as the path separator

Cause Because tacmd on UNIX and Linux is a wrapper script for the createNode command, the character "\" is removed from the command.

Solution

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:\ITM63\WIN\OSAgent`:

Linux UNIX `c:\\\\ITM63\\\\Win\\\\OSAgent`

Windows `C:/ITM63/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.

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.

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"/>
```

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
```

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.

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 installation 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 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.

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 host name to the fully-qualified host name for example, the host name is itmserver and the fully-qualified host name 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 host name during the createnode deployment using the SERVER=itmserver.raleigh.ibm.com property.

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.

tacmd viewUser

Review the symptoms and resolutions for the **tacmd viewUser** command if you do not get the results that you expect.

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 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.
```

Enter the options in separate command instances.

More applications than were assigned are showing as allowed

After running **tacmd viewUser** with the **-a** option, Universal Agent and Universal Data Provider might show as allowed applications although they were not explicitly assigned. Their inclusion in the allowed applications has no affect on operations and can be disregarded.

itmcmd commands

When the results of running an itmcmd are not what you expected, review the symptoms and possible solutions.

The itmcmd config -A hd command asks for Database Table Partitioning

While configuring the , you are prompted to specify the **Number of future partitions to maintain**, whether you selected **Database Table Partitioning** or not.

You can bypass the prompt and continue with the agent configuration.

**** MISSING FILE ****

This file was generated during the publishing process

Chapter 15. Performance Analyzer troubleshooting

Review the logging instructions and symptoms and solutions for solving problems with the Tivoli Performance Analyzer.

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

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 afterward. The log files for the agent are created in the Windows *install_dir*\TMAITM6\logs or Linux or UNIX *install_dir*/logs directory.

Procedure

1. Stop the Performance Analyzer agent.
   - Windows Click **Start** > **Programs** > **IBM Tivoli Monitoring** > **Manage Tivoli Monitoring Services**, then right-click on **Performance Analyzer** and select **Stop**.
   - Linux UNIX Enter the `itmcmd agent stop pa` command.
2. Open the `init.cfg` file. Depending on your operating system, the file is in the following directory:

   Windows *install_dir*\TMAITM6\config

   Linux *install_dir*/li6263/pa/config

   AIX *install_dir*/aix533/pa/config

   Solaris *install_dir*/sol283/pa/config
3. Update the **LogLevel** and **LogSize** parameters:
   ```
   LogLevel=Debug
   LogSize=10000000
   ```
4. Start the Performance Analyzer agent.
   - Windows Click **Start** > **Programs** > **IBM Tivoli Monitoring** > **Manage Tivoli Enterprise Monitoring Services**, right-click the **Performance Analyzer** entry, and click **Start**.
   - Linux UNIX 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 is displayed 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 monitoring portal

You can turn on logging to discover the cause of any problems with the Performance AnalyzerPerformance Analyzer in the Tivoli Enterprise Portal.

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.

Installation and configuration issues

Review the problems associated with the installation and configuration of the to learn more about the possible causes and solutions.

Reserve 100 MB of free space for temporary files during installation
For installation of the agent for non-linear trending, ensure that the agent

home directory has at least 100 MB of free space to store temporary files. See “Required software and memory requirements for non-linear trending in Tivoli Performance Analyzer” in the *IBM Tivoli Monitoring Installation and Setup Guide*.

“Enable SPSS Configuration” prompt while configuring from the command line

During configuration of the Tivoli from the command line, you get a prompt for “Enable SPSS Configuration”. Even if you select **FALSE**, you might be prompted for the “Local path to the SPSS server installation directory”. (The Forecast Server expert modeler is used for predicting future performance based on historical data.) See also “Silent configuration of the Performance Analyzer” in the *IBM Tivoli Monitoring Installation and Setup Guide*.

Problems after upgrading

If you see irregularities in the Performance Analyzer Configuration window or the Tivoli Enterprise Portal after installing and configuring the , review the symptoms, possible cause, and solution.

The Performance Analyzer configuration dialog box is hanging when you try to save the configuration

The Performance Analyzer configuration dialog box can become unresponsive if your Tivoli Enterprise Portal Server database is installed on a and you have upgraded the Performance Analyzer from V6.2.2 to V6.2.3 Fix Pack 1.

Complete the following steps to enable saving of the Performance Analyzer configuration:

1. Stop the process that is hanging.
2. Rename the file `PAfTepDBConfig.properties` to something like `PAfTepDBConfig.properties.old`.
3. Remove the *hostname*`_pa.cfg` file and restart the Performance Analyzer configuration.

You should now be able to save the configuration.

After an upgrade from Performance Analyzer V6.2.2 to V6.2.3 (or later), custom workspace view titles have changed

After upgrading the Tivoli Performance Analyzer from V6.2.2 to V6.2.3 (or later), some titles in your custom workspaces might have changed. For example, you get “Kpa:KPA1617” for the view title instead of, say, “7 Day Forecast (KB)”. You must update the title key to restore any custom view titles that have changed.

Complete the following steps in the Tivoli Enterprise Portal to restore your customized view titles:

1. In the custom workspace where the view titles are incorrect, click **Properties** to open the Properties editor.
2. Select a view from the navigation tree to open the Properties tabs, and click **Style**.
3. Depending on the view title you are modifying, replace the `Kpa:KPA`*xxxx*entry in the header **Text** box with one of the following keys:
   - For customized OS agent workspace views, `Kp3:KPA`*xxxx*
   - For customized DB2 workspace views, `Kp0:KPA`*xxxx*
   - For customized ORACLE workspace views, `Kp4:KPA`*xxxx*

- For customized ITCAM RT workspace views, `Kpi:KPA`*xxxx*
- For customized SYSTEM P workspace views, `Kp6:KPA`*xxxx*
- For customized VMWARE workspace views, `Kpu:KPA`*xxxx*

4. Click **Apply** to save the title.
5. Repeat steps 2 through 4 until `Kpa` in all views has been updated for the product type.
6. After clicking **OK** to close the Properties editor, verify that the correct titles have been restored.

After an upgrade, the previous version of the Performance Analyzer is shown in the Performance Analyzer Configuration window and task names are not displayed correctly
After and upgrade, the names of workspace groups in the Performance Analyzer Warehouse Agent Navigator item are not displayed correctly

The problem occurs on Windows platforms, when the was running during the upgrade process.

To resolve this issue, you should upgrade again, making sure that portal client is not running.

graphical user interface for fails when downloading tasks list

If your database runs DB2 on an AIX system, and the graphical user interface in fails while loading the tasks list, look in the 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 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 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 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 .
- After installing , 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 and 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 workspaces are not available or not displayed

If the workspaces are not visible at all, the connection to the is not configured correctly.

If the workspaces are visible but unavailable, the ran in the past but conditions have changed: either the agent is no longer running or the connection configuration for has changed.

No chart is visible on the Forecast Details workspace

Configure historical data collection for 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 is the same as the username used by .
- Verify that the user specified during the configuration has the appropriate rights to select data from tables and views in the database schema where tables and views are created.

Nonlinear tasks take too long to complete

If nonlinear tasks are taking too long to complete, you can create indexes on the `_PA` table in the data warehouse. Creating an index reduces the time required to store the results of the analysis in an output attribute table.

To add an index to the `_PA` table, run the appropriate command from the database command prompt on the computer where the Tivoli Data Warehouse is running. Create an index for each of the nonlinear attribute groups:

- DB2

```
CREATE INDEX DB2INST1.ITMIXFCMEM ON DB2INST1.attribute_group_name_PA
("System_Name" ASC) ALLOW REVERSE SCANS
```

- Oracle

  ```
  CREATE INDEX ITMIXFCMEM ON attribute_group_name_PA (System_Name ASC)
  ```
- MS SQL

  ```
  CREATE INDEX ITMIXFCMEM ON attribute_group_name_PA (System_Name ASC)
  ```
- DB2 on z/OS

  ```
  CREATE INDEX ITMIXFCMEM ON attribute_group_name_PA (System_Name ASC)
  ```

Create an index for each of the nonlinear attribute groups, adding the suffix _PA to the name of each group:

- KPA_GENERIC_D32_NLT_STATUS_PA
- KPA_GENERIC_D64_NLT_STATUS_PA
- KPA_GENERIC_I32_NLT_STATUS_PA
- KPA_GENERIC_I64_NLT_STATUS_PA
- KPA_GENERIC_D32_NLT_FCAST_PA
- KPA_GENERIC_D64_NLT_FCAST_PA
- KPA_GENERIC_I32_NLT_FCAST_PA
- KPA_GENERIC_I64_NLT_FCAST_PA
- CPU_Utilization_NLT_Fcast_PA
- Mem_Utilization_NLT_Fcast_PA
- Disk_Utilization_NLT_Fcast_PA
- Net_Traffic_In_NLT_Fcast_PA
- Net_Traffic_Out_NLT_Fcast_PA
- CPU_Utilization_NLT_Status_PA
- Mem_Utilization_NLT_Status_PA
- Disk_Utilization_NLT_Status_PA
- Net_Traffic_In_NLT_Status_PA
- Net_Traffic_Out_NLT_Status_PA

For example, for the KPA_GENERIC_D32_NLT_FCAST attribute group in DB2, use the following command:

```
CREATE INDEX DB2INST1.ITMIXFCMEM ON DB2INST1.KPA_GENERIC_D32_NLT_FCAST_PA
("System_Name" ASC) ALLOW REVERSE SCANS
```

Agent never connects to the monitoring server

In IBM Tivoli Monitoring V6.2.3.x, on 32- and 64-bit Red Hat Linux V5.x systems, the agent never connects to the Tivoli Enterprise Monitoring Server. The agent does not appear to attempt to connect, and there is no message in the error log. Shutdown works only with force option, and restarting does not help.

This problem indicates that the kernel on the machine is not at the required level. To resolve the problem, upgrade the kernel to 2.6.18-274.12.1.el5 or higher. See also the Software Product Compatibility Reports (http://pic.dhe.ibm.com/infocenter/prodguid/v1r0/clarity/index.html).

The Tivoli Enterprise Monitoring Server does not restart after installation of Domain Support

This problem may occur on Windows because of a corrupted catalog database after you install or upgrade 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 .

After completing these two steps, the catalog database is restored and the monitoring server works correctly. No data is lost in the process.

Chapter 16. Database troubleshooting

Review the common problems and resolutions to prevent data loss and solve problems with the Tivoli Data Warehouse and Warehouse agents.

Portal server data loss prevention

Review the data loss prevention topics for information about utilities that you can use to back up and restore Tivoli Enterprise Portal Server databases.

Backing up the TEPS database for recovery purposes

You can use the migrate-export and migrate-import utilities to back up the TEPS 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 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 Portal 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, the original content provided with Tivoli Monitoring is restored to the database.

Tivoli Data Warehouse troubleshooting

Review the Tivoli Data Warehouse topics for symptoms and solutions to known issues with the historical database and components.

Summarization and Pruning agent configuration failure

The Summarization and Pruning configuration window has an option for testing the configuration. If you get a message that the Java Runtime Library version is not supported, review the diagnostic information and solution.

Diagnosis

The Summarization and Pruning configuration windows does not recognize changes made to the list of jar files in the CLASSPATH when you are testing the connection to the Tivoli Data Warehouse. If the wrong JAR file is selected for the SQL Server JDBC driver, you receive a message such as`Java Runtime Library (JRE) version 1.7 is not supported by this driver. Use the class sqljdbc4.jar which provides support for JDBC 4.0 .`

Solution

If you change the classpath to use the correct JAR, the connection test fails with the same error. You must save the configuration change and reconfigure Summarization and Pruning again to test the connection.

If you need to remove some jar files in the list of jar files in the Summarization and Pruning configuration window, you must save the configuration and relaunch it before clicking Test Connection.

Using DB2 V9.1 for z/OS, Warehouse Proxy agent encounters a large number of disconnections

When you use 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 might 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 timeout processing. If timeout 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* in the DB2 Version 9.1 for z/OS information (http://pic.dhe.ibm.com/infocenter/dzichelp/v2r2/topic/com.ibm.db2z9.doc/src/alltoc/db2z_planhome.htm).

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.

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 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 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

About this task

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.

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 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 portal server database user account password.

Note: The following instructions do not apply in UNIX-based systems.

1. On the computer where the 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** > **IBM Tivoli Monitoring** > **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 portal server database user ID.

DB2 pureScale environment

The DB2 pureScale environment has some restrictions on tablespace and table creation on the Tivoli Data Warehouse.

In a DB2 pureScale environment, the Warehouse Proxy Agent can not create the regular tablespace ITMREG8K

The Tivoli Data Warehouse requires one bufferpool and three tablespaces to begin its operation. The bufferpool and tablespaces are created by the warehouse user before the Warehouse Proxy Agent starts, provided the warehouse user has administrative authority to the database. A warehouse user with limited authority cannot create the required bufferpool and tablespaces. Therefore, the procedure to limit the authority of the warehouse user includes steps to create the bufferpool and tablespaces in advance. However, in a DB2 pureScale environment, the Warehouse Proxy agent cannot create the regular tablespace ITMREG8K. The workaround is to connect to the warehouse database with the Warehouse Proxy Agent user, for example, “ITMUser”. Then create the tablespaces using the following SQL statements:

```
db2 create regular tablespace ITMREG8K pagesize 8k managed by automatic storage
bufferpool ITMBUF8k
db2 create user temporary tablespace ITMUSER8K pagesize 8k managed by automatic
storage bufferpool ITMBUF8k
db2 create system temporary tablespace ITMSYS8K pagesize 8k managed by automatic
storage bufferpool ITMBUF8k
```

In a DB2 pureScale environment, the summarization and pruning agent cannot create the table WAREHOUSEMARKER

A dimension is a clustering key for a table. One or more dimensions can be selected for a table. When you have more than one dimension on a table, it is considered to be a multidimensionally clustered table. Such a table is created by using the CREATE TABLE statement with the ORGANIZE BY DIMENSIONS clause.

The DB2 pureScale environment does not support multidimensional clustering table creation. Therefore, you can not use the ORGANIZE BY DIMENSIONS(OBJECT) clause required to create the table WAREHOUSEMARKER. The workaround is to connect to the warehouse database with the Warehouse Proxy Agent user, for example, “ITMUser”. Then create the table using the following SQL statement:

```
CREATE TABLE "WHA_USER"."WAREHOUSEMARKER" ( "ORIGINNODE" CHAR(64) NOT NULL ,
"OBJECT" CHAR(64) NOT NULL , "MARKERTMZDIFF"
INTEGER NOT NULL , "MARKERWRITETIME" CHAR(16) NOT NULL
```

where `"WHA_USER"` represents the Warehouse Proxy Agent user, for example, “ITMUser”.

Receive First Steps error at the end of a DB2 installation

At the end of my DB2 installation, I received an error that First Steps could not initialize because a supported browser was not present on my system. See.

Windows 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.

Procedure

- Continue installing the software, using the following steps to resolve the error:
  1. When the installation 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.
  4.
- If the installation is complete but it does not start, the data source might not be defined. Review 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 to verify whether the data source was created and to 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 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 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: Open the **Properties** window; select the **Log On** tab; and type the new password for the user.

What to do next

For information on how to modify kernel parameters, see "Modifying kernel parameters" (http://pic.dhe.ibm.com/infocenter/db2luw/v9r7/topic/com.ibm.db2.luw.qb.server.doc/doc/t0008238.html)

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.

Database contents are incorrect after installation

Use the `movefrome-m2i.bat` script to migrate the contents of Microsoft SQL Server to Universal Database if you have database migration problems.

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 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 ServerUniversal Database. The `movefrom-m2i.bat`script requires that the Microsoft SQL server database is on the same Windows platform as the monitoring server and the new Universal Database installation. Use this utility only after migration problems and before customizing the monitoring server. The `movefrom-m2i.bat` is only used to migrate the contents of Microsoft SQL Server to Universal Database.

Migration script fails on DB2 for Linux, UNIX and Windows

If the migration step1 script fails on DB2 for Linux, UNIX and Windows with the error SQL0480N, review the problem description and how to resolve it.

Diagnosis

The procedure **`SYSPROC.ADMIN_CMD`** has not yet been called. `SQLSTATE=51030` when using DB2 for Linux, UNIX and Windows indicates a DB2 problem that is resolved by APAR IC89879.

If you experience this behavior, you might be able to find the cause for the LOAD failure by looking at the message file found at the path specified by the **`DB2_UTIL_MSGPATH DB2`** registry variable (if set) or at one of the following locations, depending on the operating system:

Windows XP/2003:`C:\Documents and Settings\All Users\Application Data\IBM\DB2\DB2COPY1\DB2\tmp`

Windows 7/2008: `C:\ProgramData\IBM\DB2\DB2COPY1\DB2\tmp`

Linux UNIX *`instance`*`/sqllib/tmp`

The file will be named something like `LOAD_QFEBJ1_DB2ADMIN`.

Resolution

The contents of the message file needs to be investigated by the database administrator and be corrected before the migration can succeed. Rerun the migration step1 script after the problem has been resolved. The files can be deleted from the DB2 directory manually to free the space occupied.

Errors when migrating non-partitioned tables to partitioned tables

Errors can occur when migrating your non-partitioned tables to partitioned tables.

Error messages are displayed in the trace file if any configuration errors are detected in filter variables such as KSY_PRODUCT_FILTER, KSY_TABLE_FILTER, or KSY_SUMMARIZATION_SELECTION. Such messages indicate which table or product do not exist in the application support or if the summarization selection is incorrect.

If the filters are configured correctly but errors are detected at the database level, such as tables already partitioned or tables do not exist in the database, the migration tool generates only the SQL statements for the tables that can be migrated and error messages are logged in the trace file for the tables that cannot be migrated. When these errors occur, the following message appears on the standard output:

```
Warning: One or more tables may not have migration steps generated.
See the log file for additional information.
```

When the migration tool has generated all the scripts successfully with a warning, the following message appears on the standard output:

```
Tool requests completed, RC= 2
```

When the migration tool has generated all the scripts successfully without warnings, the following message appears on the standard output:

```
Tool requests completed, RC= 0
```

Status tables

You can review the status tables to help you troubleshoot your errors.

The tdw_migrate_setup.sql script creates the following status tables:

WAREHOUSE_MIGRATION_STATUS table for DB2 for Linux, UNIX, and Windows

This table provides the following information:

- The name of the table being migrated. This is the attribute group name and short name.
- The current status of the migration.
  - 0: Migrated successfully
  - 1: Migration started; need to rename source table
  - 2: Source renamed; need to create target table
  - 3: Target partitioned table created; need to load data
  - 4: Data loaded; need to rename source table
- The SQL code of the last statement executed.
- Number of rows read during the load operation.

- Number of rows skipped before the load operation started. This information is returned for a single-partition database only.
- Number of rows loaded into the target table. This information is returned for a single-partition database only.
- Number of rows that could not be loaded into the target table.
- Number of duplicate rows that were not loaded into the target table. This information is returned for a single-partition database only.
- Total number of rows processed. This is the number of rows successfully loaded into the target table, plus the number of skipped and rejected rows. This information is returned for a single-partition database only.
- Number of rows distributed by all database distributing agents. This information is returned for a multi-partition database only.
- Number of entries returned in the second result set for a multi-partitioned database. This is the number of agent information entries produced by the load operation. This information is returned for multi-partitioned databases only.
- The SQL state of the last statement executed.
- The SQL required to retrieve the load utility messages.
- The SQL required to remove the load utility messages.
- Timestamp when the status row was created.
- Timestamp when the status row was last updated.
- Timestamp when step 1 started.
- Timestamp when step 1 successfully completed.
- Timestamp when step 2 started.
- Timestamp when step 2 successfully completed.
- Timestamp when step 3 started.
- Timestamp when step 3 successfully completed.
- Timestamp when step 4 started.
- Timestamp when step 4 successfully completed.

WAREHOUSE_MIGRATION_STATUS for DB2 on z/OS

This table provides the following information:

- The schema name of the table migrated.
- The name of the table being migrated. This is the attribute group name.
- The short name of the table migrated.
- The job ID when a JCL job is used.
- The current status of the migration.
  - 0: Migrated successfully
  - 1: Migration started; need to rename source table
  - 2: Source renamed; need to create target table
  - 3: Target partitioned table created; need to create and submit JCL job
  - 4: JCL job to migrate data create and submitted; need to query job status
  - 5: JCL migrate job status available; if the job execute successfully, need to fetch the job output
  - 6: Job output fetched line by line; parse each line to find out if migration executed successfully
  - 7: JCL migrate job purged

  - 8: Source table renamed
- Error message if anything failed.
- The last SQL statement that had an error.
- The SQL code of the last error.
- The SQL state of the last error.
- Timestamp when the status row was created.
- Timestamp when the status row was last updated.
- Timestamp when step 1, 2, 3, 4, 5, 6, or 7 started.
- Timestamp when step 1, 2, 3, 4, 5, 6, or 7 successfully completed.
- Timestamp when step 2 successfully completed.

WAREHOUSE_JCLJOB_MIGRATION_STATUS for DB2 on z/OS

This table is only created for DB2 on z/OS. This table provides the following information:

- The JCL job ID.
- The JCL job administrator stored procedure that was used.
- The stored procedure return code.
- The time the stored procedure was executed.
- The JCL job status.
- The job error message.
- The job completion code.
- The job completion type.
  - 0: No completion information is available
  - 1: Job ended normally
  - 2: Job ended by completion code
  - 3: Job had a JCL error
  - 4: Job was canceled
  - 5: Job terminated abnormally
  - 6: Converter terminated abnormally while processing the job
  - 7: Job failed security checks
  - 8: Job failed in end-of-memory
- The system abend code if an abnormal termination occurs.
- The user abend code if an abnormal termination occurs.

The tdw_migrate_step1.sql script provides the return codes based on your database type. Refer to the *IBM Tivoli Monitoring Administrator's Guide* for a complete list of return codes.

Return codes 1, 2, and 4 for the tdw_migrate_step1.sql script on DB2 for Linux, UNIX, and Windows

When migrating a table on DB2 for Linux, UNIX, or Windows, you might receive return codes 1, 2, or 4.

1: Indicates that the source table could not be renamed to MIGRATING_*.

2: Indicates that the partitioned table could not be created.

4: Indicates that the table MIGRATING_* could not be renamed to DONE_*.

To determine the cause of each of these errors, note the SQL code and SQL state values that are provided in the output when the table is migrated. To get more information about an SQL code, refer to the DB2 error code documentation or issue the `db2 ? <SQL CODE>` command.

The SQL code and SQL state values are also stored in the WAREHOUSE_MIGRATION_STATUS table. To retrieve the values:

1. Start the DB2 command line processor. Do not issue SQL from the operating system's command line to avoid having to escape quotes in SQL text.
2. Connect to the Tivoli Data Warehouse database as the Tivoli Data Warehouse user:
   ```
   connect to <TDW database> user <TDW user ID> using <password>
   ```
3. Issue the SQL:
   ```
   SELECT sqlcode, sqlstate  FROM WAREHOUSE_MIGRATION_STATUS WHERE tablename =
   '<name of table being migrated>'
   ```
   For example:
   ```
   SELECT sqlcode, sqlstate  FROM WAREHOUSE_MIGRATION_STATUS WHERE
   tablename = 'NT_Process_64'
   ```
4. Once the cause of the error is resolved, the migration script tdw_migrate_step1.sql can be rerun.

Return code 3 for the tdw_migrate_step1.sql script on DB2 for Linux, UNIX, and Windows

When migrating a table on DB2 for Linux, UNIX, or Windows, a return code of 3 indicates the load step has failed. This means there was a failure calling the LOAD stored procedure in the tdw_migrate_step1.sql script for a given table. The load step could fail for many different reasons including:

- The Tivoli Data Warehouse user doesn't have sufficient privileges to run the load utility.
- Insufficient space in the migrated table's tablespace for the data being loaded.

To determine why the load failed:

1. Start the DB2 command line processor. Do not issue SQL from the operating system's command line to avoid having to escape quotes in SQL text.
2. Connect to the Tivoli Data Warehouse database as the Tivoli Data Warehouse user:
   ```
   connect to <TDW database> user <TDW user ID> using <password>
   ```
3. Issue the SQL:
   ```
   SELECT msgretrieval FROM WAREHOUSE_MIGRATION_STATUS WHERE tablename
   = '<name of table being migrated>'
   ```
   For example:
   ```
   SELECT msgretrieval FROM WAREHOUSE_MIGRATION_STATUS WHERE tablename =
   'NT_Process_64'
   ```
   Returns:
   ```

   MSGRETRIEVAL
   -------------------------------------------------------------------
   SELECT SQLCODE, MSG FROM TABLE(SYSPROC.ADMIN_GET_MSGS('32727_ITMUSER'))
   AS MSG
   ```
4. Issue the SQL query that was returned in step 3. This displays the messages from the DB2 LOAD utility.

In this example, there were no errors in the load step of the migration:

```
SELECT SQLCODE, MSG FROM TABLE(SYSPROC.ADMIN_GET_MSGS('32727_ITMUSER'))
AS MSG

SQLCODE   MSG
-------   ---------------------------------------------------------
SQL3501W  The table space(s) in which the table resides will not be
 placed in backup pending state since forward recovery is disabled
 for the database.
SQL1193I  The utility is beginning to load data from the SQL statement
 "SELECT * FROM ITMUSER."MIGRATING_NTPROCESS"".
SQL3500W  The utility is beginning the "LOAD" phase at time
 "01/14/2013 11:26:47.793424".
SQL3519W  Begin Load Consistency Point. Input record count = "0".
SQL3520W  Load Consistency Point was successful.
SQL3110N  The utility has completed processing. "96785" rows were
 read from the input file.
SQL3519W  Begin Load Consistency Point. Input record count = "96785".
SQL3520W  Load Consistency Point was successful.
SQL3515W  The utility has finished the "LOAD" phase at time
 "01/14/2013 11:26:59.426438".
9 record(s) selected.
```

5. Fix the problems mentioned in the load utility's message files and re-execute the tdw_migrate_step1.sql script.

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 17. 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 18. 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* (http://pic.dhe.ibm.com/infocenter/tivihelp/v61r1/topic/com.ibm.itm.doc_6.3fp2/install/itm_install.htm).
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 18. Resolving problems sending events to Netcool/OMNIbus (continued)

<table>
<tr><th>Cause</th><th>Resolution</th></tr>
<tr><td>Configuration of the EIF destination is incorrect.</td><td>

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
```

</td></tr>
</table>

Table 18. 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 290 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 19. 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 19. 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 19. 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 -namenco -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 290 to determine the names and locations of the log files and how to enable additional debugging.

Table 19. 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 host name 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 20. 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 20. 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 20. 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.

See also the technote, technote

Tivoli Enterprise Console integration troubleshooting

Review the fundamental Tivoli Enterprise Console troubleshooting tasks for guidance with solving integration problems with the Tivoli Enterprise Console.

- 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 theTivoli Enterprise Portal desktop client:
    1. Log off the Tivoli Enterprise Portal Server.
    2. Log on to the Tivoli Enterprise Portal Server.
    3. Log into a different IBM Tivoli Enterprise Console server.
  - From the browser client:

    Recycle the browser.
- For more Tivoli Enterprise Console event integration troubleshooting topics, see .
- For a listing of product messages, see *IBM Tivoli Monitoring Messages* (http://pic.dhe.ibm.com/infocenter/tivihelp/v61r1/topic/com.ibm.itm.doc_6.3fp2/ic/landing_messages.htm).

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_valuevalue to 30000.

Chapter 18. Tivoli Common Reporting troubleshooting

If you cannot display reports, consider the issues and review the recommendations for the messages you receive.

When a report fails to generate or generates incorrectly, click **View the report with errors** to make diagnosis of the underlying problem easier.

When troubleshooting Tivoli Common Reporting problems, enable detailed logging as instructed in the Tivoli Common Reporting information center topic, .

Installation and configuration

Review the descriptions of errors or anomalies that can occur during installation or configuration for diagnosis and instructions for resolution.

out of memory error after installation

If core files are created and you get a out of memory error after installing common reporting, delete the core files and increase the memory allocation.

Symptom

After installing Tivoli Common Reporting Reports for Tivoli OS Agents or product agents such as Performance Analyzer , core files are created and a `OutOfMemoryError` appeared during installation. Example of core files that were created on a Linux system (time stamp not shown):

```
-rw-rw-r-- 1 root root    368500 javacore.20120123.004307.8587.0002.txt
-rw-rw-r-- 1 root root 163932213 heapdump.20120123.004307.8587.0001.phd
-rw-r--r-- 1 root root     67996 Snap.20120123.004307.8587.0003.trc
-rw-r--r-- 1 root root     67980 Snap.20120123.013937.11219.0003.trc
-rw-rw-r-- 1 root root    368926 javacore.20120123.013937.11219.0002.txt
-rw-rw-r-- 1 root root 163909461 heapdump.20120123.013937.11219.0001.phd
```

Example of an out of memory error in a Linux environment while running the **`trcmd`** command to list reports:

```
root@TIP-TCR-Server:/root/rahuls/10-feb-12-logs]/opt/IBM/tivoli/
tipv2Components/TCRComponent/bin/trcmd.sh -username tipadmin -password
tippass  -list -reports
JVMDUMP006I Processing dump event "systhrow", detai
l "java/lang/OutOfMemoryError"  - please wait.
JVMDUMP032I JVM requested Heap dump using '/root/rahuls/10-feb-12-logs/
heapdump.20120213.203152.17478.0001.phd' in response to an event
JVMDUMP010I Heap dump written to /root/rahuls/10-feb-12-logs/heapdump.
20120213.203152.17478.0001.phd
JVMDUMP032I JVM requested Java dump using '/root/rahuls/10-feb-12-logs/
javacore.20120213.203152.17478.0002.txt' in response to an event
JVMDUMP010I Java dump written to /root/rahuls/10-feb-12-logs/javacore.
20120213.203152.17478.0002.txt
JVMDUMP032I JVM requested Snap dump using '/root/rahuls/10-feb-12-logs/Snap.
20120213.203152.17478.0003.trc' in response to an event
JVMDUMP010I Snap dump written to /root/rahuls/10-feb-12-logs/Snap.20120213.
203152.17478.0003.trc
JVMDUMP013I Processed dump event "systhrow", detail
 "java/lang/OutOfMemoryError".
CTGTRQ010E Processing has ended because of an unexpected error.
```

Cause The runtime environment requires more than 512 MB maximum memory for the processing Tivoli Common Reporting **`trcmd`** commands.

Solution

Delete any core files that were created.

Increase JVM heap size for the **trcmd** commands: In the trcmd script file (trcmd.sh on Linux or UNIX), modify the JAVA_ARGS variable by adding following options -Xms64m -Xmx768m, or -Xms64m -Xmx1024m if the problem persists. Example of JAVA_ARGS after setting the maximum heap size:

```
JAVA_ARGS="-Dtcr.command.libs=${COG_LIB}:${TCR_LIB}:${BIRT_LIB}
-Xms64m -Xmx768m -Djava.util.logging.config.file=${TCR_CONF}/
reporting.logging.properties -Dlog4j.configuration=file://
${TCR_CONF}/log4j.properties.xml
-Dcom.ibm.tivoli.reporting.installdir=${TCR_HOME}
-Duser.home=${TCR_HOME}
-Dcom.ibm.tivoli.reporting.scenario=embedded"
```

Failure to extract reports from TAR on AIX server

If you get a tar failure when attempting to extract monitoring agent reports on the AIX server, you might be using the native tar utility on AIX, which does not support long file names.

Symptom

Attempts to extract the Cognos-based OS Agent Reports only produces a small list of files and directories. The following example shows that setup.bat and setup.sh installation files are missing, and the packages, db_script, and gui directories are also missing.

```
# tar -xvf 6.2.2-TIV-ITM_TMV-Agent-Reports-FP0004.tar
-rwxrwxrwx 1 root system 8905516 Mar 25 15:22 report_installer.jar
-rwxrwxrwx 1 root system 3994 Mar 25 15:22 osagents_tcr_install.properties
drwxrwxrwx 3 root system 256 Mar 25 17:30 lib
```

Cause The native tar utility on AIX might truncate long file names, causing the extracting process to not extract all files included in the Tivoli monitoring agent reports tar.

Solution

Install GNU tar version 1.14 or later, which is included with the AIX Toolbox. This tar version ensures that the reports can be properly extracted on the AIX server.

1. Download tar*.rpm from and save to your AIX server.
2. Confirm the location where GNU tar will be installed.

   ```
   # rpm -qlp tar*.rpm
   ```

   In this example, the above command lists the location as /usr/linux/bin/tar
3. Install on AIX server using the rpm command.

   ```
   rpm -ihv tar*.rpm
   ```
4. Using the newly installed GNU tar utility, extract the contents of the monitoring agent reports tar. Example:

   ```
   /usr/linux/bin/tar -xf 6.2.2-TIV-ITM_TMV-Agent-Reports-FP0004.tar
   ```

OS agent reports fail after repeat installations

If the Cognos IBM Tivoli Monitoring OS Agent Reports fail after installing, uninstalling, and reinstalling the reports, remove any remaining .rtm files before installing again.

Symptom

After installing the OS Agent Reports using the Report Installer, uninstalling from the Tivoli Integrated Portal, and reinstalling the reports, you cannot complete the installation. The reports fail with error number 28: `UT-DEF-0074 Unable to complete the write operation.`

Cause Some `.rtm` files were not removed from the previous installation. The `.rtm` files are the Cognos data models, and the OS agent data model has 200 MB of `.rtm` files. These files are working copies generated by Cognos, each with a unique name. Thus, each reinstallation of the OS Agent Reports adds a set of unique files to the `.rtm` files that remain from the previous installation.

Solution

Delete the `.rtm` files from the `/RTModels` subdirectory:

Windows `C:\Program Files (x86)\IBM\WebSphere\AppServerComponents\TCRComponent\cognos\data\cqe\RTModels` where `C:\Program Files (x86)\IBM\` is the *install_dir*.

Linux UNIX `/opt/IBM/WebSphere/AppServerComponents/TCRComponent/cognos/data/cqe/RTModels` where `/opt/IBM/` is the *install_dir*.

Schema Publication Tool errors

The schema publication tool is used to create the dimension tables required by Tivoli Common Reporting and IBM Tivoli Monitoring.

If you get errors while running the `tdw_schema_insert.sql` script against a DB2 database, review the options for resolving the issue.

Symptom

You receive errors while running the `tdw_schema_insert.sql` script against a DB2 database to insert data, indicating that the transaction log is full.

Solution

Take one of the following actions to resolve the issue:

- Reduce the transaction by changing the call to create a smaller range of dates.
- Increase the transaction log space:
  1. Connect to the `WAREHOUS` database with the DB2 administrator user ID. Example:
     ```
     db2 connect to WAREHOUS user DB2_administrator_user_ID using pw
     ```
  2. Get the current LOG settings. Example:
     ```
     db2 get db cfg for WAREHOUS |grep LOG
     ```
  3. Change one or all of the **`LOGFILSIZ`**, **`LOGPRIMARY`**, and **`LOGSECOND`** settings. For example:
     ```
     LOGFILSIZ=5000, LOGPRIMARY=100,  LOGSECOND=12
     ```

Run the script again with the `ITMUSER` user ID. Disregard any errors about the insertion of data in `MONTH_LOOKUP` and `WEEKDAY_LOOKUP`, because that data was inserted correctly the first time the script was executed.

Localized reports

Review the descriptions of errors or anomalies that can occur during Tivoli Common Reporting installation or configuration for diagnosis and instructions for resolution.

Date, time, and other text in Tivoli Monitoring OS Agents reports are not localized

Chart axis timestamps

The timestamps shown in the axis of the charts are not globalized. The format for every locale is *YYYY-MM-DD HH:MM:SS*.

Date and time format in Internet Explorer 7

When displaying 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* 12-hour format, instead.

Connection and Viewer title bars are not translated

"Connection" and "Viewer" title bars are not shown in the localized language but remain in English.

Start and end dates are not reported for custom date range

If you are running Tivoli Common Reporting for OS agent reports in a browser that is set for a language other than English, such as Italian, use the predefined date settings, such as last 2 weeks. Customized date ranges are not reported. For example, if you specify from July 29, 2013 to August 5, 2013, the dates are not reported in the generated report.

Reports and other pages show in English instead of pt_BR locale

In the Brazilian Portuguese locale, most content except the title shows in English. As well, the "Parameters Selection" page of the OS agent reports is displayed in a mix of English and Portuguese. If you encounter the symptom, set the Tivoli Common Reporting user language to Portuguese (Brazil):

1. After logging into the Dashboard Application Services Hub, select **Common Reporting**.
2. Click **My Preferences** under My Area Options.
3. In the Regional option, change the Content language to Portuguese (Brazil).

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.

The prompt page of a Cognos report 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.

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.

Locations of log files

Several logs 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, 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. See "Troubleshooting Tivoli Common Reporting" (http://pic.dhe.ibm.com/infocenter/tivihelp/v3r1/topic/com.ibm.psc.doc_1.1.0/tshoot/tcr_c_tshoot.html)
- 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.

Tivoli Common Reporting 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.

Tivoli Common Reporting V2.1.1

Review the issues that can occur when running reports on Tivoli Common Reporting V2.1.1 and the solutions.

Running OS Cognos Reports 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 accommodates temporary data to generate reports on the Tivoli Common Reporting Server when you use Tivoli Monitoring provided reports.

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.

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 cannot 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

Message CTGTRW1000E is often displayed after you start a session and click in the navigation tree. You can disregard the message.

Click **OK** to dismiss the error message; and the and reports 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 306 for the locations of log files.

Your report fails to generate with unexpected error messages displayed

If you attempt to run a report after defining the parameters but receive errors after a long wait, you might need to increase the Java heap size.

Before you begin

As well as the following scenario, consider that if you are generating reports for more than 5,000 agents, especially from multiple days of history, you will also get Java out-of-memory errors.

About this task

In this scenario, the report parameters were defined for an OMEGAMON XE or NetView® for z/OS report. After clicking **Run**, the user received the following messages:

```
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, complete the following steps:

Procedure

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:
3. Stop Tivoli Common Reporting.
4. Edit the `startServer.bat` file, usually found in this location: On Windows Systems: `C:\Program Files\IBM\tivoli\tip\bin`
5. Locate this instruction about half way through the bat file:
```
"%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%
```
6. 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%
```
7. Re-start the Tivoli Common Reporting server and try generating the report again.

Reports against many agents fail with Out of Memory Error

If you are generating reports for more than 5,000 agents, especially if you are including many days of historical monitoring data, the reports might fail and the COGNOS process returns an out-of-memory error.

Symptom
After attempting to run Tivoli Common Reporting Reports of many Tivoli Enterprise Monitoring Agents over a long period of time, the reports fail and an `OutOfMemoryError` is logged.

Cause
The large amount of data from many monitoring agents or many days of historical data causes an out-of-memory failure of the COGNOS process (C++).

Solution
If your Tivoli Data Warehouse has a lot of data, consider reducing the number of monitoring agents included in the report or reducing the amount of time included in the report. For example, if you run a CPU Utilization report for 5,000 monitoring agents for the past 30 days, the out-of-memory failure might arise. As an alternative, run the report twice with 2,500 monitoring agents each time, or run the report with 15 days of monitoring data.

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 cannot 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, historical collection has been configured and enabled , and 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.

Lineage option shows an exception

The Lineage report gives a blank error page.

In Tivoli Common Reporting V2.2 and V3.1, the OS agent Lineage reports are not working.

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 19. Auditing facility troubleshooting

The 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.

For more information about common logging, see “Audit logging” in the *IBM Tivoli Monitoring Administrator's Guide*.

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 that are 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.

Only audit events that were created since the component was started are displayed.

If you want to display audit records for events that occurred 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 Tivoli Monitoring components. See “Managed System Status workspace” in the *Tivoli Enterprise Portal User's Guide* for a description of the Audit Log workspace and instructions for 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 that are 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 Tivoli Monitoring components.

On distributed systems, you can also examine the component's XML-formatted audit log to access audit records that were generated before the latest restart. These logs are on the component computer in the `*install_dir*/auditlogs` directory. See “Audit logging” in the *IBM Tivoli Monitoring Administrator's Guide* for more information.

Tivoli Monitoring components in a z/OS environment can enable the SMF audit facility to collect ITM Audit records. See *IBM Tivoli OMEGAMON XE and Tivoli Management Services on z/OS Common Planning and Configuration* (http://pic.dhe.ibm.com/infocenter/tivihelp/v61r1/topic/com.ibm.omegamon_share.doc_6.3.0.1/zcommonconfig/zcommonconfig.htm) for the specific component.

Chapter 20. OMEGAMON Enhanced 3270 user interface troubleshooting

Review the OMEGAMON Enhanced 3270 user interface troubleshooting topics for a description of a problem you might experience with rendering OMEGAMON monitoring agent data on the OMEGAMON Enhanced 3270 user interface.

If you do not find the resolution to the problem you experience with the interface, refer to the *IBM OMEGAMON Enhanced 3270 User Interface Guide* for more information.

No data condition on the OMEGAMON enhanced 3270 user interface

The OMEGAMON enhanced 3270 user interface has been installed and configured. The OMEGAMON enhanced 3270 user interface address space has been started and you are able to log on, but your enhanced 3270 user interface is displaying an empty workspace.

OMEGAMON Enhanced 3270 user interface component summary

The following OMEGAMON components facilitate the display of data in the OMEGAMON enhanced 3270 user interface:

Tivoli OMEGAMON XE Agents

The OMEGAMON XE V5.1.0 (for example, OMEGAMON XE for CICS on z/OS or OMEGAMON XE on z/OS, among others) deliver capability that builds on the OMEGAMON enhanced 3270 user interface infrastructure to provide OMEGAMON capability on the OMEGAMON enhanced 3270 user interface.

Hub Tivoli Enterprise Monitoring Server

Monitoring servers are part of the Tivoli Management Services infrastructure shared by OMEGAMON XE agents. The OMEGAMON enhanced 3270 user interface requires Tivoli Management Services V6.2.3 or higher.

The master monitoring server is called the *hub monitoring server*. The hub monitoring server acts as the focal point for data collection and distribution; it communicates with monitoring agents, with the OMEGAMON enhanced 3270 user interface, and with other Tivoli Management Services components.

Monitoring servers that communicate only with the monitoring agents that report to them and with the hub monitoring server are referred to as *remote monitoring servers*. The hub monitoring server receives data requests from the OMEGAMON enhanced 3270 user interface through the data retrieval agent (KOBAGENT) and drives OMEGAMON agents for data collection and retrieval. The hub monitoring must be seeded with OMEGAMON XE V5.1.0 agent data.

OMEGAMON Enhanced 3270 User Interface address space

The OMEGAMON enhanced 3270 user interface address space provides data retrieval and user interface 3270 interaction functions. One or more OMEGAMON enhanced 3270 user interfaces can deployed in a given z/OS Sysplex.

OMEGAMON Enhanced 3270 user interface data retrieval agent (KOBAGENT)

This component runs in any z/OS monitoring server or Tivoli OMEGAMON XE Agent address space. The OMEGAMON Enhanced 3270 user interface data retrieval agent receives data requests from the OMEGAMON Enhanced 3270 user interface and connects to the hub monitoring server to drive data collection by OMEGAMON V5.1.0 monitoring agents.

There must be at least one OMEGAMON Enhanced 3270 user interface data retrieval agent deployed and running in the Sysplex where components of a given configuration (hub or remote monitoring servers and agents) are running to enable OMEGAMON Enhanced 3270 user interface data retrieval and display. The OMEGAMON Enhanced 3270 user interface must also run in the same Sysplex as the OMEGAMON Enhanced 3270 user interface data retrieval agent.

The aforementioned components must be installed, configured, started, and running to enable successful rendering of OMEGAMON agent data on the OMEGAMON Enhanced 3270 user interface. The OMEGAMON agent configuration step adding support for the V5.1.0 monitoring agent to the hub monitoring server must be performed to enable successful rendering of OMEGAMON agent data on the OMEGAMON Enhanced 3270 user interface.

Communications and data retrieval

The OMEGAMON Enhanced 3270 user interface uses WLM Services to discover Data Retrieval Agents that are running in its Sysplex. The interface uses TCP/IP services to communicate with Data Retrieval Agents.

The Data Retrieval Agent uses TCP/IP services to communicate with the hub monitoring server. The Data Retrieval Agent uses WLM Services to register or publish their existence within the Sysplex.

The OMEGAMON XE monitoring agents use TCP/IP or SNA services to communicate with the monitoring servers. The monitoring agents register with the hub monitoring server as part of the startup process.

The OMEGAMON Enhanced 3270 user interface uses VTAM services to enable you to log on and communicate with the interface. You log on to the OMEGAMON Enhanced 3270 user interface through a VTAM Appl ID that is opened during startup of the interface.

The following figure shows the OMEGAMON configuration including deployment of these enhanced 3270 interface components:

- OMEGAMON Enhanced 3270 user interface address space
- OMEGAMON Enhanced 3270 user interface Data Retrieval Agent (KOBAGENT)

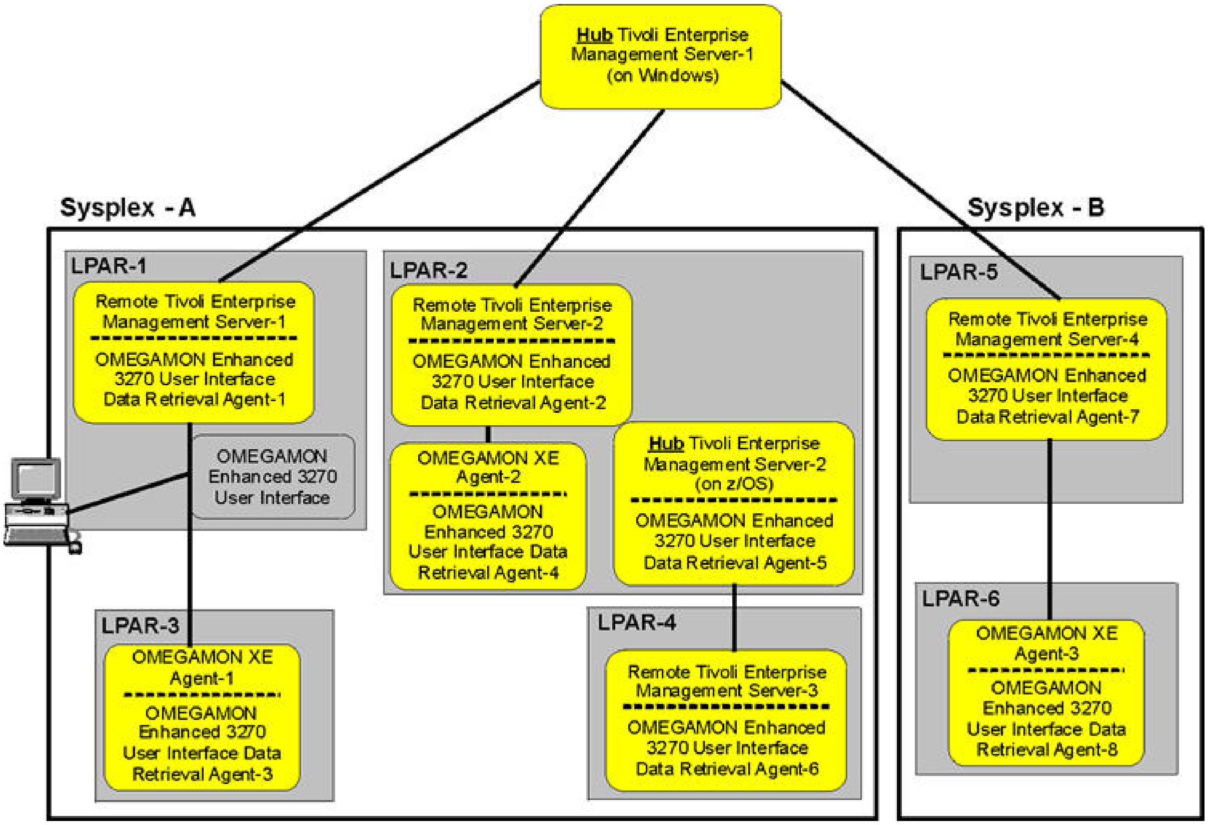

Hub Tivoli Enterprise Management Server-1 (on Windows)
Sysplex - A
Sysplex - B
LPAR-1
Remote Tivoli Enterprise Management Server-1
OMEGAMON Enhanced 3270 User Interface Data Retrieval Agent-1
OMEGAMON Enhanced 3270 User Interface
LPAR-2
Remote Tivoli Enterprise Management Server-2
OMEGAMON Enhanced 3270 User Interface Data Retrieval Agent-2
OMEGAMON XE Agent-2
OMEGAMON Enhanced 3270 User Interface Data Retrieval Agent-4
Hub Tivoli Enterprise Management Server-2 (on z/OS)
OMEGAMON Enhanced 3270 User Interface Data Retrieval Agent-5
LPAR-3
OMEGAMON XE Agent-1
OMEGAMON Enhanced 3270 User Interface Data Retrieval Agent-3
LPAR-4
Remote Tivoli Enterprise Management Server-3
OMEGAMON Enhanced 3270 User Interface Data Retrieval Agent-6
LPAR-5
Remote Tivoli Enterprise Management Server-4
OMEGAMON Enhanced 3270 User Interface Data Retrieval Agent-7
LPAR-6
OMEGAMON XE Agent-3
OMEGAMON Enhanced 3270 User Interface Data Retrieval Agent-8

Figure 1. OMEGAMON configuration including deployment of the enhanced 3270 interface components

Minimal configuration considerations

The following minimal configuration considerations must be addressed to enable the OMEGAMON Enhanced 3270 user interface to select and connect to a hub monitoring server:

OMEGAMON Enhanced 3270 user interface log on profile

You must create one or more custom log on profiles. These profiles specify the settings for the hub monitoring server from which data is collected. The RKOBPROF DD statement in the OMEGAMON Enhanced 3270 user interface started task JCL procedure specifies the data set that contains the site and user log on profile settings. The customized site or user profiles are stored as members of the *rte.UKOBDATF* data set. When you log on, the OMEGAMON Enhanced 3270 user interface looks for a profile member named *user_id* (the ID of the logged on user) or CUASITE (a site-customized profile) to establish profile settings for the session.

You can establish a site or *user_id* named log on profile member by copying (and renaming) the KOBCUA product provided profile member from the target *thilev.TKOBDATF* library or the runtime *rte.TKOBDATF* data set to the runtime *rte.UKOBDATF* data set.

Hub monitoring server settings

The settings for the hub monitoring server settings are specified in the log on profile member. By default, the settings are provided as commented statements:

```
/* HUBNAME=HUBNAME
/* HUBIPADDRESS=::ffff:HUBADDRESS
/* HUBPORTNUMBER=HUBPORTNUMBER
```

Edit the profile member copy to specify the desired hub settings; locate, uncomment and update the statements; for example, remove the leading /* and move the setting statements to begin in column one.

For example:

```
HUBNAME=HUB1:CMS
HUBIPADDRESS=::ffff:9.44.44.22
HUBPORTNUMBER=55555
```

HUBNAME
The configured name of the hub monitoring server. The monitoring server might be configured to run on the z/OS or distributed system; for example, Linux. Often a hub monitoring server is configured to run on distributed systems that employs a mixed-case or all lower case naming convention. The value specified in your profile setting statements *must* match the case of the configured value.

HUBIPADDRESS
The TCP/IP address of the host system where the hub monitoring server runs. The setting *must* be an TCP/IP address as shown in the preceding example; do not specify a TCP/IP Host name.

HUBPORTNUMBER
The TCP/IP port number of the configured hub monitoring server. The default port number is 1918.

Component startup and operation

The following components comprise the startup and operation environment for the OMEGAMON Enhanced 3270 user interface and the OMEGAMON agents:

OMEGAMON Enhanced 3270 user interface address space
Although startup of the OMEGAMON Enhanced 3270 user interface address space is relatively fast, it should probably be the last component in the startup sequence; because the interface requires that all other components in its environment (the OMEGAMON monitoring agents, the Data Retrieval Agent, and the hub and or remote monitoring servers) be initialized and running before it is able to retrieve data.

OMEGAMON Enhanced 3270 user interface local registry
The OMEGAMON Enhanced 3270 user interface startup process discovers registered Data Retrieval Agents and connects to related hub monitoring servers in order to establish a local registry of data source information; that is, managed systems names and managed system lists. After startup, by default, the registry is refreshed on a five minute interval.

OMEGAMON agent and OMEGAMON Enhanced 3270 user interface Data Retrieval Agent
The OMEGAMON XE V5.1.0 agent address spaces run both an instance of the product agent and also an instance of a OMEGAMON Enhanced 3270 user interface Data Retrieval Agent. The Data Retrieval Agent uses WLM services to publish or register its existence. The product agent registers with the hub monitoring server; these registration processes facilitate OMEGAMON Enhanced 3270 user interface discovery of OMEGAMON agents. Note that some OMEGAMON agents, such as OMEGAMON XE on z/OS, run under a remote z/OS monitoring server; the OMEGAMON Enhanced 3270 user interface; the Data Retrieval Agent also runs under remote z/OS monitoring servers.

OMEGAMON agent startup process

There might be cases where an OMEGAMON agent startup process requires up to 10 minutes to complete startup and registration. As a result, the OMEGAMON Enhanced 3270 user interface will not be able to retrieve data for that agent during this period.

OMEGAMON agent recycle

There might be cases where an OMEGAMON agent address space is terminated (for example, LPAR shutdown, goes offline) and, in some cases, the agent is performing the role of a "proxy agent." As a result, the OMEGAMON Enhanced 3270 user interface will not be able to retrieve data for that agent until the offline agent condition is resolved; for example, in a multi-LPAR configuration another agent will assume the “proxy-agent” role.

Hub Tivoli Enterprise Monitoring Server

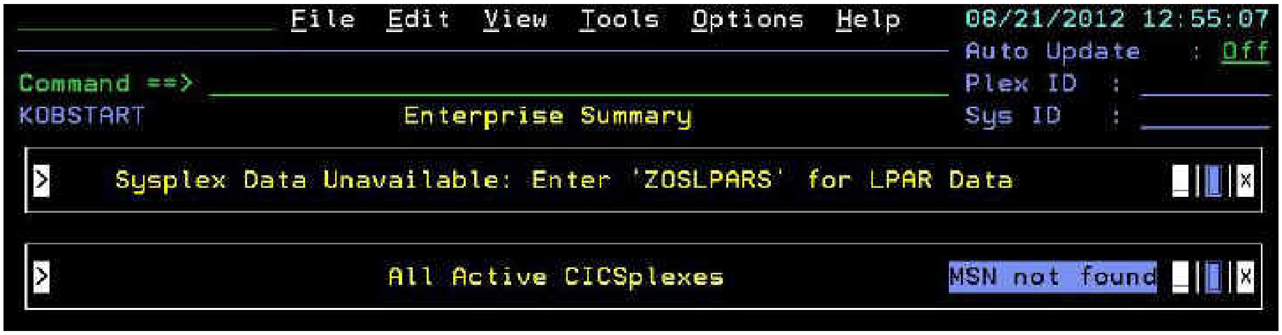
To enable the OMEGAMON Enhanced 3270 user interface data retrieval, the hub Tivoli Enterprise Monitoring Server must be:

- Running Tivoli Management Services V6.2.3 or higher
- Seeded with OMEGAMON for *xxx* on z/OS V5.1.0 or higher agent data
- Started and connectable through TCP/IP; listening on the configured TCP/IP port
- Have connected or online OMEGAMON for *xxx* on z/OS V5.1.0 or higher agents

Possible causes for the no data condition

There are a few causes for the no data condition after the initial log on to the OMEGAMON Enhanced 3270 user interface.

The following figure provides an example of the OMEGAMON Enhanced 3270 user interface initial workspace, KOBSTART, depicting a case of no data after the initial log on:



```
                                                       08/21/2012 12:55:07
                                                       Auto Update   : Off
Command ==>                                            Plex ID   :
KOBSTART               Enterprise Summary              Sys ID    :

 >    Sysplex Data Unavailable: Enter 'ZOSLPARS' for LPAR Data

 >                All Active CICSplexes           MSN not found
```

Figure 2. OMEGAMON Enhanced 3270 user interface workspace depicting a case of no data after the initial log on

Note: The initial workspace parameter setting is specified in the log on profile with the **FIRSTWS** parameter.

You can use the capability in the OMEGAMON Enhanced 3270 user interface for investigating the root cause of the no data condition.

No custom log on profiles have been created or the hub monitoring server settings have not been configured

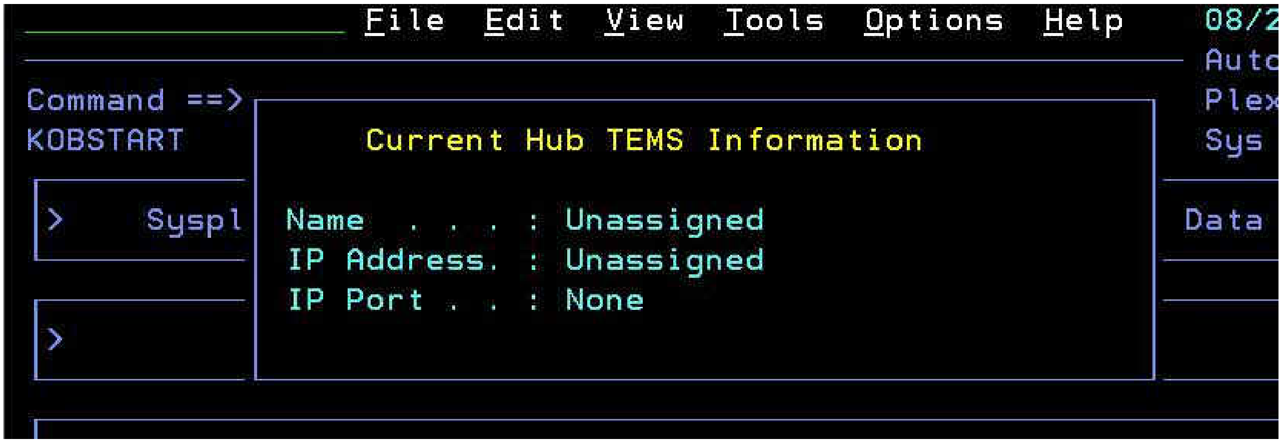
Verify that you have created your site and or user_ID named log on profile members.

About this task

Use the OMEGAMON Enhanced 3270 user interface to assign values for your site and or user ID named log on profile.

Procedure

1. From the OMEGAMON Enhanced 3270 user interface, select **View > 2. Hub Information**. The Current Hub TEMS Information panel is displayed. If you see a panel similar to the following panel indicating that no values are assigned, either no site and or user ID-named log on profile has been created, or the profile for this session has not been customized to specify hub monitoring server settings.



```
Command ==>
KOBSTART
        Current Hub TEMS Information

 Name . . . : Unassigned
 IP Address. : Unassigned
 IP Port . . : None
```

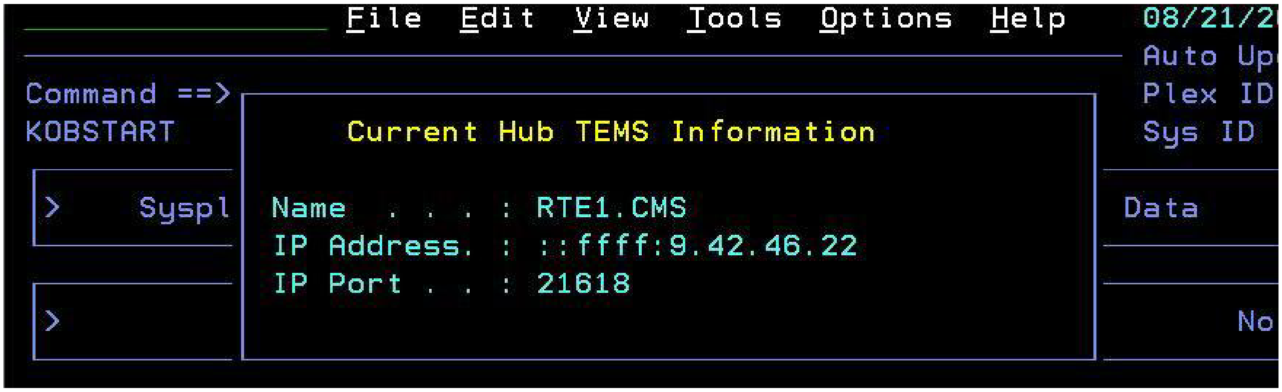
Figure 3. Tivoli Enterprise Monitoring Server information with no settings specified

   a. Verify that a site (CUASITE) or user_ID named data set member exists in *rte.UKOBDATF* .
   b. Verify that the hub monitoring server settings in the profile for the current session have been customized to specify the required hub monitoring server configured values. For example, see Figure 4 on page 323.

2. After you customize the log on profile member, log off the OMEGAMON Enhanced 3270 user interface and log on to pickup the profile changes.

Results

If you repeat Step 1, you will see the hub settings you have specified as shown in the following panel.



```
_______________  File  Edit  View  Tools  Options  Help     08/21/2
                                                            Auto Up
Command ==>                                                 Plex ID
KOBSTART       Current Hub TEMS Information                 Sys ID

 >    Syspl  Name  . . . : RTE1.CMS                        Data
             IP Address. : ::ffff:9.42.46.22
             IP Port . . : 21618
 >                                                              No
```

Figure 4. Current hub Tivoli Enterprise Monitoring Server settings

The hub monitoring server settings in the log on profile do not match the hub monitoring server configured values

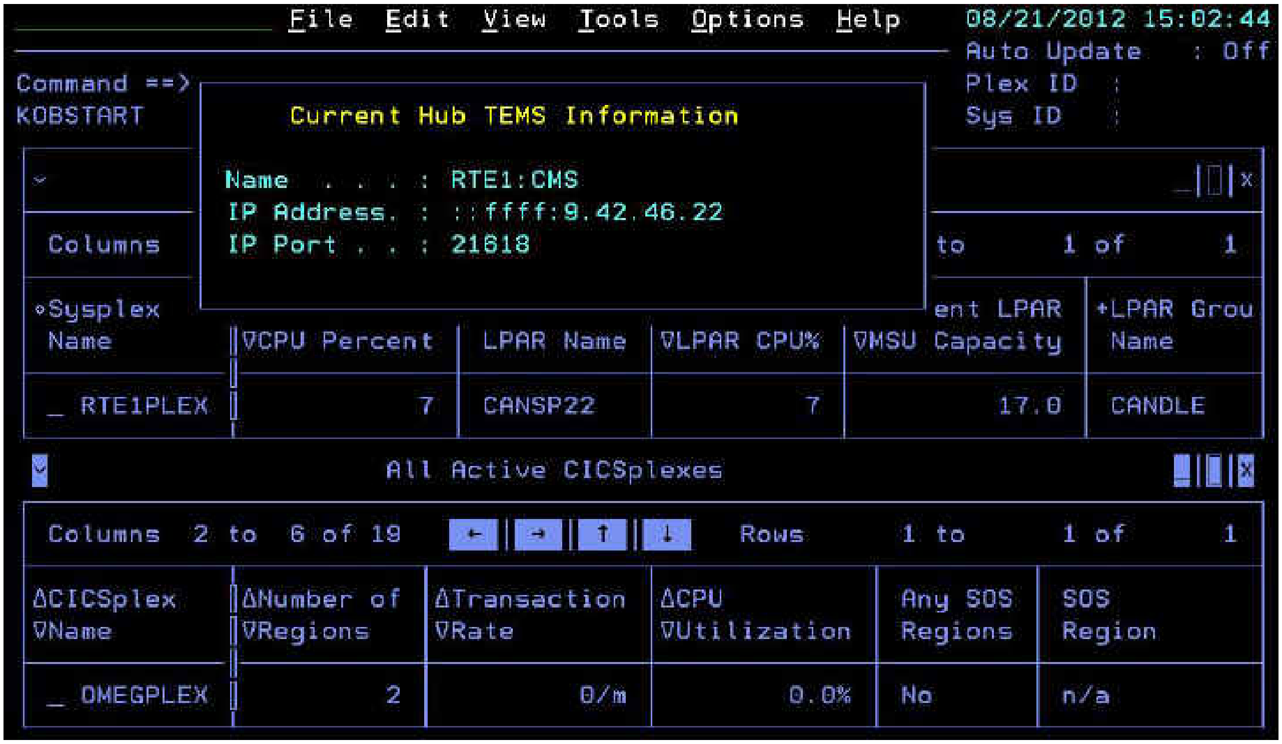
Verify that the *rte.UKOBDATF* profile members specify the configured hub monitoring server settings and that these settings match the hub monitoring server configured values.

The settings that are displayed in the Current Hub TEMS information panel in figure 4 indicate that a custom profile member has been created and customized; however, the no data condition persists. Inspect the profile for the current session to determine if the specified settings match the configured hub monitoring server settings.

For example, Figure 4shows that the server name is set to `RTE1.CMS` , with a period. However, the actual configured hub monitoring server name is `RTE1:CMS` , with a colon.

Correct the settings in the *rte.UKOBDATF* profile member, then log off and log on to the OMEGAMON Enhanced 3270 user interface to pickup the profile changes.

The Current Hub TEMS Information panel will display the correct settings as shown in the following example:



```
_______________  File  Edit  View  Tools  Options  Help      08/21/2012 15:02:44
                                                              Auto Update   : Off
Command ==>                                                   Plex ID       :
KOBSTART        Current Hub TEMS Information                  Sys ID        :

                Name . . . . : RTE1:CMS                                   _|▯|x
                IP Address. : ::ffff:9.42.46.22
 Columns        IP Port . . : 21618                           to       1 of      1

 ∘Sysplex                                                     ent LPAR   +LPAR Grou
  Name          |∇CPU Percent | LPAR Name | ∇LPAR CPU% |∇MSU Capacity|  Name

 _ RTE1PLEX     |           7 | CANSP22   |          7 |         17.0|  CANDLE

 ⌄                      All Active CICSplexes                             _|▯|x

 Columns  2 to  6 of 19   ← | → | ↑ | ↓    Rows      1 to      1 of      1

 ΔCICSplex      |ΔNumber of |ΔTransaction |ΔCPU          |Any SOS  |SOS
 ∇Name          |∇Regions   |∇Rate        |∇Utilization  |Regions  |Region

 _ OMEGPLEX     |          2|          0/m|          0.0%|No       |n/a
```

Figure 5. The current hub Tivoli Enterprise Monitoring Server information with the correct server name

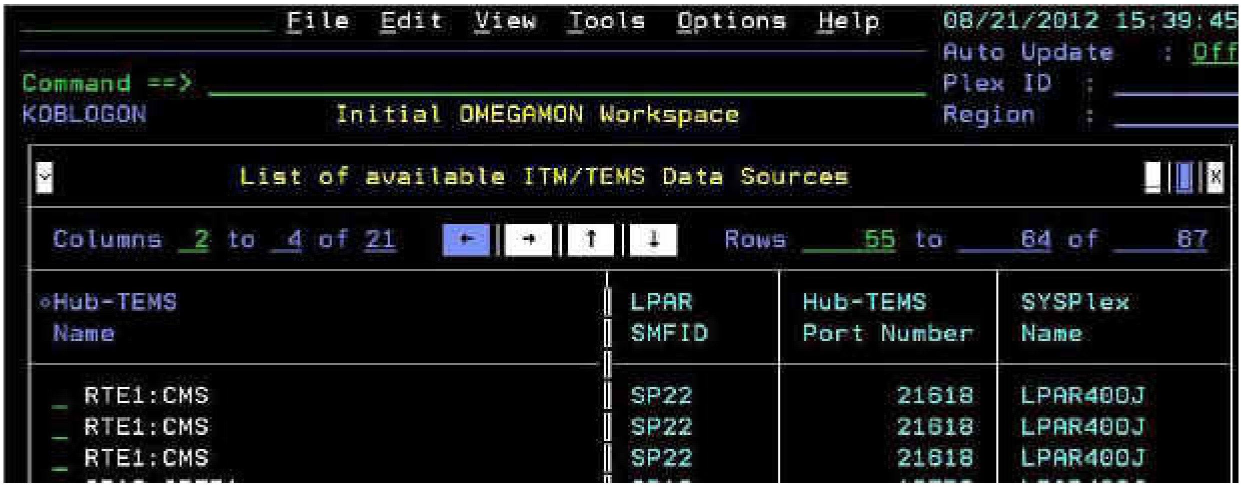
There are no OMEGAMON Enhanced 3270 user interface data retrieval agents registered

Verify that there are registered OMEGAMON Enhanced 3270 user interface data retrieval agents online.

The OMEGAMON Enhanced 3270 user interface startup process discovers WLM-registered data retrieval agents and connects to the data retrieval agents to retrieve hub monitoring server information about OMEGAMON agent data sources. This information is stored in the OMEGAMON Enhanced 3270 user interface local registry. By default, the registry information is refreshed every five minutes.

If you have verified the existence of a custom profile, in which the hub monitoring server settings are correctly specified, but the no data condition persists, you need to verify that there are registered data retrieval agents.

From the OMEGAMON Enhanced 3270 user interface, select **View > 3. Data Retrieval Agents**. The KOBLOGON workspace, and, in particular the List of available ITM/TEMS Data Sources panel, is opened and lists all the available data retrieval agents and their associated hub server as shown in the following panel.



```
____________________ File  Edit  View  Tools  Options  Help      08/21/2012 15:39:45
                                                                 Auto Update   : Off
Command ==> ______________________________________________________ Plex ID  : ________
KOBLOGON              Initial OMEGAMON Workspace                 Region   : ________

  List of available ITM/TEMS Data Sources

  Columns  2 to  4 of 21   ←  →  ↑  ↓    Rows ____55 to ____64 of ____87

 ◦Hub-TEMS                                 LPAR     Hub-TEMS      SYSPlex
  Name                                     SMFID    Port Number   Name

 _  RTE1:CMS                               SP22           21618   LPAR400J
 _  RTE1:CMS                               SP22           21618   LPAR400J
 _  RTE1:CMS                               SP22           21618   LPAR400J
```

Figure 6. Sample display of local registry with available data sources

The three rows shown in figure 6 list the hub monitoring server as `RTE1:CMS`; this is an indication that there are three registered data retrieval agents running in the *same* Sysplex as the OMEGAMON Enhanced 3270 user interface address space. Assuming that there are no problems with agent data collection, the OMEGAMON Enhanced 3270 user interface is able to connect to any one of these data retrieval agents to retrieve OMEGAMON data from a V5.1.0 monitoring agent that is connected to the `RTE1:CMS` hub monitoring server.

If there are no data retrieval agents registered for a given hub monitoring server, the KOBLOGON workspace will either be empty or, if there are multiple hub monitoring servers configured, it might contain data retrieval agent rows for other monitoring servers running in the Sysplex.

If the KOBLOGON workspace list does *not* contain the hub monitoring server that is specified in the OMEGAMON Enhanced 3270 user interface log on profile, there is a high probability that the OMEGAMON XE on z/OS agent(s) and or related monitoring server address space are off line.

The hub monitoring server is off line; verify initialization and data request reception

Verify the hub monitoring server is started, initialized, and prepared to receive data requests; listening on the configured TCP/IP port.

Your hub monitoring server might be running on either a z/OS LPAR or on a distributed system. Verify that the monitoring server has been started and has successfully completed initialization.

The following monitoring server log messages are a good indication regarding the health of hub monitoring server operations:

```
..
KDSMA001 Tivoli Enterprise Monitoring Server (TEMS) data collection server started
...
KO4SRV032 Tivoli Enterprise Monitoring Server (TEMS) startup complete
..
```

If you cannot find these messages in the hub monitoring server log, examine the log for indications of potential problems. For example:

- The monitoring server startup is in progress and initialization has not completed
- The monitoring server initialization failed; for example, the monitoring server was not able to bind to its configured TCP/IP port
- The monitoring server is not properly configured
- Unexpected messages in the monitoring server log

See the "Monitoring server troubleshooting" section of this book for more information.

Application product support (seed data) has not been added to the hub monitoring server

Verify the hub monitoring server has the product version (for example, V5.1.0) application support (seed data) loaded.

If you did not complete this configuration step, your OMEGAMON Enhanced 3270 user interface might be missing data for one or more OMEGAMON products.

For a hub monitoring server on a z/OS system, see the "Adding application support to a monitor server on z/OS" section in the *IBM Tivoli Monitoring Installation and Setup Guide*.

For a hub monitoring server on a distributed system, see the "Installing application support on monitoring server" section in the *IBM Tivoli Monitoring Installation and Setup Guide*.

Note: The following message, which shows an example of the OMEGAMON XE for CICS on z/OS log, might appear in the OMEGAMON Enhanced 3270 user interface when the add application support configuration step has not been completed; this might also be true when the add application support step was completed after the initial startup of the product agent. For the later case, the hub Tivoli Enterprise Monitoring Server and agent should be recycled after performing the add application support step.

```
...
RRUIA-DMSL: MSL "KCP_CICSplex_CICSPLXS" does not exist or contains no online
accessible MSNs.
...
```

Note: The V5.1.0 product application support files must also be loaded in the run time environment libraries that are associated with the OMEGAMON Enhanced 3270 user interface started task. For a new or upgraded run time environment, the run time environment load configuration step updates the application support.

You will see the following messages in the OMEGAMON Enhanced 3270 user interface log file when the application support files are back-leveled or missing:

```
...
KOBUIGP1I Source ODI does not contain table Kppxxxxx ...
KOBUIGP9I ERROR: No ODI will cause an erroneous display ...
KOBUIGP1W ODI Failure ignoring SORTCOLS='...
...
```

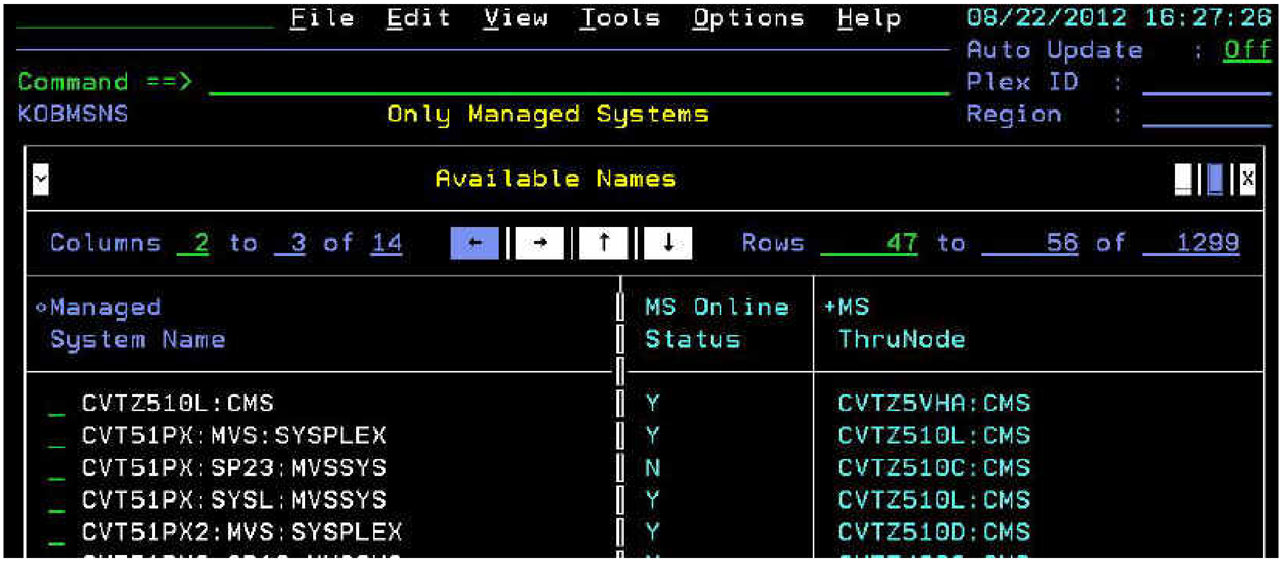
Also, see “The OMEGAMON Enhanced 3270 user interface local registry does not contain required agent information” on page 328.

The OMEGAMON monitoring agent is off line or has not been started

There are multiple methods that can be employed to investigate the online status of an OMEGAMON agent.

One method is to examine the content of the local registry.

From the OMEGAMON Enhanced 3270 user interface, select **View > 4. Managed Systems**. The Only Managed Systems panel is displayed and lists the available names of the local registry managed systems.



```
_______________  File  Edit  View  Tools  Options  Help    08/22/2012 16:27:26
                                                           Auto Update   : Off
Command ==> _________________________________________       Plex ID   : ________
KOBMSNS                 Only Managed Systems               Region    : ________

                              Available Names

 Columns _2 to _3 of 14   ←  →  ↑  ↓     Rows ____47 to ____56 of ____1299

 ◦Managed                                    MS Online   +MS
  System Name                                Status       ThruNode

 _  CVTZ510L:CMS                             Y            CVTZ5VHA:CMS
 _  CVT51PX:MVS:SYSPLEX                      Y            CVTZ510L:CMS
 _  CVT51PX:SP23:MVSSYS                      N            CVTZ510C:CMS
 _  CVT51PX:SYSL:MVSSYS                      Y            CVTZ510L:CMS
 _  CVT51PX2:MVS:SYSPLEX                     Y            CVTZ510D:CMS
```

Figure 7. Only Managed Systems panel listing the available names of the local registry

The various OMEGAMON monitoring agents employ unique conventions to identify agents and managed systems. For example, in the previous figure, the rows that display names ending in *:MVSSYS* and *:SYSPLEX* along with a **Y** in the **MS Online Status** column are an indication that there are OMEGAMON XE on z/OS agents on line, which means the interface should retrieve data for the product.

The following table lists the conventions used by individual OMEGAMON products to compose managed system names.

Product name	Managed System naming convention
OMEGAMON XE on z/OS	• SYSPLEX:SYSPLEX:PLEXVIEW • sysplex_name:MVS:SYSPLEX • sysplex_name:lpar_smfID:MVSSYS
OMEGAMON XE for CICS on z/OS	• cics_region_name:lpar_smfID:CPIRA • cics_region_name:lpar_smfID:CEIRA • cics_tg_ID:lpar_smfID:CICSTG
OMEGAMON XE for DB2 PE	• DB2plex:DB2plex:Plexview • db2_ID:lpar_smfid:DB2 • XEDB2:lpar_smfid

Product name	Managed System naming convention
OMEGAMON XE for IMS on z/OS	• IMSplex:IMSplex:Plexview • ims_ID:lpar_smfid:CONNECT • ims_ID:sysplex_name:SQGROUP • ims_ID:lpar_smfid:IMS • XEIMS:lpar_smfid:MVS
OMEGAMON XE for Mainframe Networks	• agent_jobname:lpar_smfid:KN3AGENT • tcpip_ID:lpar_smfid • vtam_ID:lpar_smfid
OMEGAMON XE for Messaging	• mq_ID:lpar_smfid:MQESA
OMEGAMON XE for Storage on z/OS	• agent_jobname:lpar_smfid:STORAGE

When you examine the Only Managed Systems (KOBMSNS) workspace content and it indicates there are no online agents for a given product, then examine the agent address space to verify that it has been started and it has successfully initialized on line. In some cases, it might be necessary to verify that the corresponding monitored systems or subsystems (for example, CICS regions) are also running.

The OMEGAMON Enhanced 3270 user interface local registry does not contain required agent information

The OMEGAMON Enhanced 3270 user interface local registry must have accurate information about the configuration of the environment to enable the composition and routing of data queries to appropriate OMEGAMON agent managed systems.

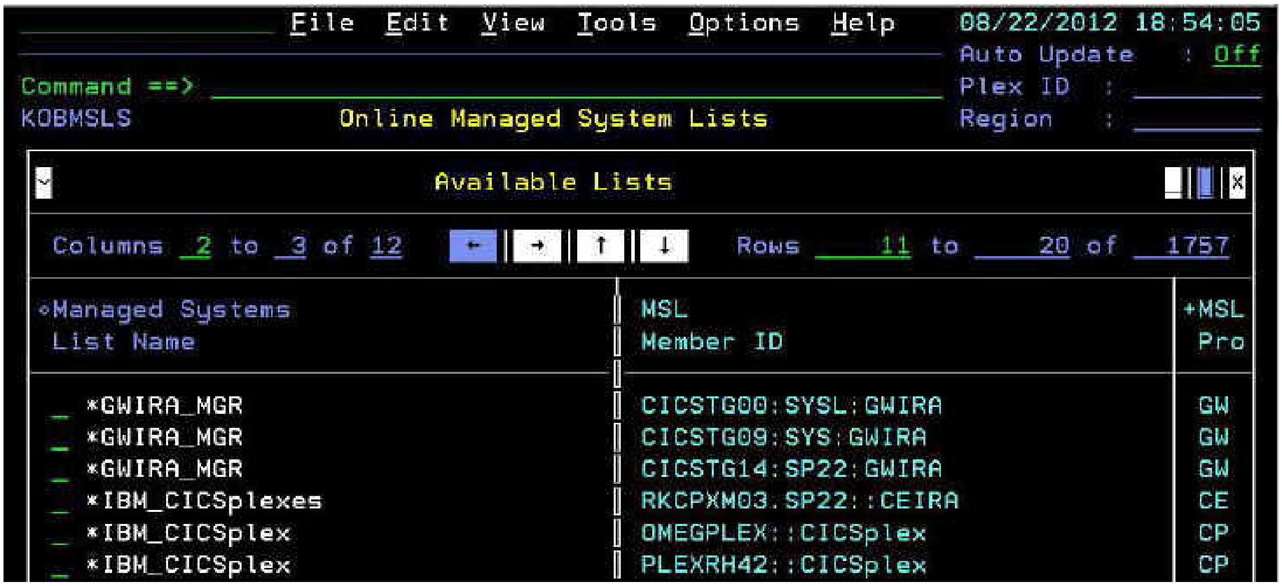
The registry is initially populated during the address space initialization process and thereafter, by default, at five minute intervals.

Given the startup considerations for OMEGAMON monitoring components and monitored systems and or subsystem, it is possible for the local registry content to take up to 10 minutes to stabilize; assuming you have fairly stable configuration.

Use the OMEGAMON Enhanced 3270 user interface Options menu to examine the local registry.

Examine the following items:

- Verify the existence of the online registered OMEGAMON Enhanced 3270 user interface data retrieval agents by selecting the **View > 3. Data Retrieval Agents**. The Initial OMEGAMON Workspace (KOBLOGON) panel must contain a minimum of one data retrieval agent row to enable data retrieval.
- Verify the existence of the OMEGAMON agent list for managed systems by selecting **View > 5. Managed Systems Lists**. For example:



```
                  File  Edit  View  Tools  Options  Help    08/22/2012 18:54:05
                                                            Auto Update   : Off
Command ==> ________________________________________        Plex ID   : ________
KOBMSLS               Online Managed System Lists           Region    : ________

                        Available Lists

 Columns  2 to  3 of 12   ←  →  ↑  ↓      Rows    11 to    20 of   1757

 ◇Managed Systems                    | MSL                        | +MSL
  List Name                          | Member ID                  |  Pro

 _ *GWIRA_MGR                        | CICSTG00:SYSL:GWIRA        |  GW
 _ *GWIRA_MGR                        | CICSTG09:SYS:GWIRA         |  GW
 _ *GWIRA_MGR                        | CICSTG14:SP22:GWIRA        |  GW
 _ *IBM_CICSplexes                   | RKCPXM03.SP22::CEIRA       |  CE
 _ *IBM_CICSplex                     | OMEGPLEX::CICSplex         |  CP
 _ *IBM_CICSplex                     | PLEXRH42::CICSplex         |  CP
```

Figure 8. Online Managed Systems Lists panel of the local registry

The Online Managed Systems Lists workspace lists the rows with managed system list names.

The following table lists the naming conventions for the OMEGAMON products of the managed systems list names:

Product	Managed System List naming convention
OMEGAMON XE on z/OS	• *MVS_SYSPLEX • *MVS_SYSTEM
OMEGAMON XE for CICS on z/OS	• *CPIRA_MGR *GWIRA_MGR • *IBM_CICSplexes • *IBM_CICSplex • *MVS_CICSTG • *MVS_CICS • KCP_CICSplex_plex_name
OMEGAMON XE for DB2 PE	*MVS_DB2
OMEGAMON XE for IMS on z/OS	• *MVS_IMSPLEX • KIP_ims_system_IMS
OMEGAMON XE for Mainframe Networks	• *OMEGAMONXE_MAINFRAME_NTWK_TCP • *OMEGAMONXE_MAINFRAME_NTWK_VTAM • *OMEGAMONXE_MAINFRAME_NTWK
OMEGAMON XE for Messaging	mq_ID:lpar_smfid:MQESA
OMEGAMON XE for Storage on z/OS	agent_jobname:lpar_smfid:STORAGE

- Verify the existence of online OMEGAMON agents managed systems by selecting **View > 4. Managed Systems**. The Only Managed Systems workspace (KOBMSNS) shows rows with managed system names. See “The OMEGAMON monitoring agent is off line or has not been started” on page 327.

  Note: In a case where the configuration is running multiple versions of the OMEGAMON XE on z/OS agents (V4.2.0 and V5.1.0), only remote server address spaces that have been upgraded to the latest version can be configured as Sysplex-proxy-eligible. You might get a workspace notice that says, `Sysplex Data Unavailable: Enter 'ZOSLPARS' for LAPR Data` for the case where the Sysplex proxy has started in a back-leveled remote server address space. The result is that the OMEGAMON Enhanced 3270 user interface is unable to render Sysplex data.

Note: In the case where there are multiple instances of IBM Tivoli Monitoring configurations running in a common Sysplex, the configurations must be configured with unique names; at least one of the configurations must provide an override Sysplex name (pseudo name) so that both configurations are able to start a Sysplex proxy (and agent). The workspace notice, `Sysplex Data Unavailable: Enter 'ZOSLPARS' for LAPR Data` depicts the case where perhaps this has not been done and the Sysplex proxy is unable to start in one of the configurations; the result is that the OMEGAMON Enhanced 3270 user interface is unable to render Sysplex data for that Sysplex.

Data retrieval delays/time-outs causing no data conditions

OMEGAMON Enhanced 3270 user interface logs are written to the address space SYSPRINT DD statement.

By default, the OMEGAMON Enhanced 3270 user interface is configured with the request time out parameters shown in the following table:

Parameter name	Description	Defaults and overrides
QUERYTIMEOUT=	User interface workspace query time out	Default is 10 seconds. **Note:** Some workspace queries are delivered with an time out override; where the composition of data requests anticipates an elongated response.
PNG_TIMEOUT	DRA ping health check (endpoint ping) time out	Two seconds
SO_TIMEOUT	DRA data request (socket) time out	15 seconds
DIS_TIMEOUT	Registry refresh (discovery data request time out	Two seconds

These parameter defaults have been established for reasonable or normal operational conditions. There might be unique operational conditions in your environment where the defaults are not optimal. In that case, you can modify the defaults by creating customized OMEGAMON Enhanced 3270 user interface workspaces and or specifying parameter overrides in the OMEGAMON Enhanced 3270 user interface environment parameters file (*rte.RKANPARU(KOBENV)* that is referenced by the address space RKANPAR DD statement.

Elongated response times when interacting with the OMEGAMON Enhanced 3270 user interface might be a symptom of time out conditions. For example, during log on, the initial Enterprise Summary (KOBSTART) workspace might take a significant amount of time (more than a few seconds) to render and or the workspace is rendered with partial or no data.

Note: The following message is written to the SYSPRINT log files when request time-outs occur:

```
KOBCM0010E: conduit manager Recv Error, rc = -1, microseconds = nnnnnnnn
```

The following items identify the common causes for delay and or time out conditions. Investigation of these conditions might be complex, this information provides you with some hints for further investigation:

- The hub monitoring server is running under degraded system conditions (heavy system workload or an under-capacity system) and is being delayed when attempting to service OMEGAMON Enhanced 3270 user interface data requests. In this example, examine the availability and priority of the system resources provided to the hub monitoring server.
- The OMEGAMON agent is running under degraded system conditions (heavy system workload or an under-capacity system) and is being delayed when attempting to service OMEGAMON Enhanced 3270 user interface data requests. In this example, examine the availability and priority of the system resources provided to the OMEGAMON agent.
- Data requests submitted from the OMEGAMON Enhanced 3270 user interface to a given Data Retrieval Agent, thorough a TCP/IP conduit, are being impacted by degraded network conditions. In this case, the availability, priority, and configuration of network resources and paths associated with communications between the OMEGAMON Enhanced 3270 user interface and the hub monitoring server and OMEGAMON agents should be examined.
- An OMEGAMON component (monitoring server or agent) that played a role in a given data request path has gone off-line; the LPAR was terminated, or the address space was terminated. In this case, "The OMEGAMON Enhanced 3270 user interface local registry does not contain required agent information" on page 328 to investigate the status of OMEGAMON components, (Managed Systems: on line or off line).
- The hub and or a remote monitoring server is experiencing operational issues and is being delayed when attempting to service OMEGAMON Enhanced 3270 user interface data requests. A misconfiguration or a special site or environmental configuration requirements might lead to operational issues.

  For example:

  - Operational issues might arise if a monitoring server running on a z/OS operating system is experiencing problems writing to its' Historical Persistent Datastore files.
  - Operational issues might occur if a monitoring server is unable to bind to its configured TCP/IP port number.
- The IP domain name resolution is not fully configured on the z/OS operating system where the OMEGAMON Enhanced 3270 user interface, Tivoli Enterprise Monitoring Server and or agent address spaces are running. Also, there might be more than one TCP/IP task running on the z/OS operating system; for these cases, the OMEGAMON address spaces, the OMEGAMON Enhanced 3270 user interface, Tivoli Enterprise Monitoring Server and or agent started task JCL procedures must specify the IP name resolution configuration data set to be specified through the SYSTCPD DDNAME statement.
- The hub Tivoli Enterprise Monitoring Server is running on a system that has multiple network interfaces and perhaps the preferred and or universally known interface is not being employed; this results in IP connection issues that manifest on the interface as a possible sporadic, no data condition. Refer to the following tech note for more information related to this type of configuration; the use of the **KDEB_INTERFACELIST** parameter. See http://www-01.ibm.com/support/docview.wss?uid=swg21282474.

Appendix. IBM Tivoli Monitoring processes

Look up the IBM Tivoli Monitoring process names when you want to confirm that a process is indeed running and review the resources used.

Table 21. 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
Tivoli Authorization Policy Server	java.exe[1]	java.exe[1]
Tivoli Enterprise Monitoring Automation Server	kasmain.exe	kasmain
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

[1] The application runs under the Websphere Application Server, which is part of Jazz for Service Management (JazzSM).

Documentation library

Various publications are relevant to the use of 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

Documentation is delivered in the IBM Tivoli Monitoring and OMEGAMON XE Information Center at http://pic.dhe.ibm.com/infocenter/tivihelp/v61r1/index.jsp and also in the **Files** section of the Application Performance Management community.

For information about accessing and using the publications, select IBM Tivoli Monitoring → **Using the publications** in the **Contents** pane of the IBM Tivoli Monitoring and OMEGAMON XE Information Center at http://pic.dhe.ibm.com/infocenter/tivihelp/v61r1/index.jsp.

To find a list of new and changed publications, click the **New in this release** topic on the IBM Tivoli Monitoring welcome page. 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 IBM Tivoli Monitoring library provides information about the commonly shared components of Tivoli Management Services.

- *Quick Start Guide*

  Introduces the components of IBM Tivoli Monitoring.
- *Installation and Setup Guide*, SC22-5445

  Provides instructions for installing and configuring IBM Tivoli Monitoring components on Windows, Linux, and UNIX systems.
- *High Availability Guide for Distributed Systems*, SC22-5455

  Gives instructions for several methods of ensuring the availability of the IBM Tivoli Monitoring components.
- *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.
- *Administrator's Guide*, SC22-5446

  Describes the support tasks and functions required for the Tivoli Enterprise Portal Server and clients, including Tivoli Enterprise Portal user administration.
- *Command Reference* available on Service Management Connect

  Provides detailed syntax and parameter information, as well as examples, for the commands you can use in IBM Tivoli Monitoring.
- *Messages* available on Service Management Connect

  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).

- *Troubleshooting Guide* available on Service Management Connect

  Provides information to help you troubleshoot problems with the software.
- *Tivoli Enterprise Portal User's Guide* available on Service Management Connect

  Complements the Tivoli Enterprise Portal online help. The guide provides hands-on lessons and detailed instructions for all Tivoli Enterprise Portal features.
- 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.

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.

- 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
- OS agent documentation is delivered in the following locations:

  Agent Installation and Configuration Guide

  Available in the Information Center:
  - *IBM i OS Agent Installation and Configuration Guide*, SC27-5653
  - *Linux OS Agent Installation and Configuration Guide*, SC27-5652
  - *UNIX OS Agent Installation and Configuration Guide*, SC27-5651
  - *Windows OS Agent Installation and Configuration Guide*, SC27-5650

  Agent Reference

  Available on Service Management Connect

  Agent Troubleshooting Guide

  Available on Service Management Connect
- Warehouse agent documentation is delivered in the following locations:

  Agent Installation and Configuration Guide

  Available in the Information Center:
  - *Warehouse Proxy Agent Installation and Configuration Guide*, SC27-5655
  - *Warehouse Summarization and Pruning Agent Installation and Configuration Guide*, SC27-5654

  Agent Reference

  Available on Service Management Connect

  Agent Troubleshooting Guide

  Available on Service Management Connect
- 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
  - *Agent Builder User's Guide*, SC32-1921
  - *Performance Analyzer User's Guide*, SC27-4004
  - *Systems Director base Agent User's Guide*, SC27-2872
  - *Tivoli Log File Agent User's Guide*, SC14-7484
  - *Tivoli zEnterprise Monitoring Agent User's Guide*, SC14-7359 and the *Tivoli zEnterprise Monitoring Agent Installation and Configuration Guide*, SC14-7358

Related publications

For information about related products and publications select **OMEGAMON XE shared publications** or other entries in the **Contents** pane of the IBM Tivoli Monitoring and OMEGAMON XE Information Center.

You can access the IBM Tivoli Monitoring and OMEGAMON XE Information Center at http://pic.dhe.ibm.com/infocenter/tivihelp/v61r1/index.jsp .

You can also access other information centers at IBM Tivoli Documentation Central (https://www.ibm.com/developerworks/community/wikis/home?lang=en#!/wiki/Tivoli%20Documentation%20Central).

Tivoli Monitoring community on Service Management Connect

Connect, learn, and share with Service Management professionals: product support technical experts who provide their perspectives and expertise.

For information about Tivoli products, see the Application Performance Management community on SMC at IBM Service Management Connect > Application Performance Management (http://www.ibm.com/developerworks/servicemanagement/apm).

For introductory information, see IBM Service Management Connect (http://www.ibm.com/developerworks/servicemanagement).

Use Service Management Connect in the following ways:

- Become involved with transparent development, an ongoing, open engagement between other users and IBM developers of Tivoli products. You can access early designs, sprint demonstrations, product roadmaps, and prerelease code.
- Connect one-on-one with the experts to collaborate and network about Tivoli and the (enter your community name here) community.
- Read blogs to benefit from the expertise and experience of others.
- Use wikis and forums to collaborate with the broader user community.

Other sources of documentation

You can obtain additional technical documentation about monitoring products from other sources.

- Tivoli wikis

IBM Service Management Connect > Application Performance Management (http://www.ibm.com/developerworks/servicemanagement/apm) includes a list of relevant Tivoli wikis that offer best practices and scenarios for using Tivoli products, 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:

- The IBM Tivoli Monitoring Wiki (https://www.ibm.com/developerworks/community/wikis/home?lang=en#!/wiki/Tivoli%20Monitoring) provides information about IBM Tivoli Monitoring and related distributed products, including IBM Tivoli Composite Application Management products.
- The Tivoli System z® Monitoring and Application Management Wiki 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.

- IBM Integrated Service Management Library

  http://www.ibm.com/software/brandcatalog/ismlibrary/

  IBM 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/.

Support information

If you have a problem with your IBM software, you want to resolve it quickly. IBM provides ways for you to obtain the support you need.

Online

The following sites contain troubleshooting information:

- Go to the IBM Support Portal (http://www.ibm.com/support/entry/portal/software) and follow the instructions.
- Go to IBM Service Management Connect > Application Performance Management (http://www.ibm.com/developerworks/servicemanagement/apm) and select the appropriate wiki.

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 IBM Support Assistant (http://www-01.ibm.com/software/support/isa).

Troubleshooting Guide

For more information about resolving problems, see the product's Troubleshooting Guide.

Using 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.

The IBM Support Assistant saves you the time it takes to search the product, support, and educational resources. The IBM Support Assistant helps you gather support information when you need to open a problem management record (PMR), which you can then use to track the problem.

The product-specific plug-in modules provide you with the following resources:

- Support links
- Education links
- Ability to submit problem management reports

For more information, and to download the IBM Support Assistant, see http://www.ibm.com/software/support/isa. After you download and install the IBM Support Assistant, follow these steps to install the plug-in for your Tivoli product:

1. Start the IBM Support Assistant application.
2. Select **Updater** on the Welcome page.
3. Select **New Properties and Tools** or select the **New Plug-ins** tab (depending on the version of IBM Support Assistant installed).
4. Under **Tivoli**, select your product, and then click **Install**. Be sure to read the license and description.

If your product is not included on the list under **Tivoli**, no plug-in is available yet for the product.

5. Read the license and description, and click **I agree**.
6. Restart the IBM Support Assistant.

Obtaining fixes

A product fix might be available to resolve your problem. To determine which fixes are available for your Tivoli software product, follow these steps:

1. Go to the IBM Software Support website at http://www.ibm.com/software/support.
2. Under **Select a brand and/or product**, select **Tivoli**.

   If you click **Go**, the **Search within all of Tivoli support** section is displayed. If you don't click **Go**, you see the **Select a product** section.
3. Select your product and click **Go**.
4. Under **Download**, click the name of a fix to read its description and, optionally, to download it.

   If there is no **Download** heading for your product, supply a search term, error code, or APAR number in the field provided under **Search Support (this product)**, and click **Search**.

For more information about the types of fixes that are available, see the *IBM Software Support Handbook* at http://www14.software.ibm.com/webapp/set2/sas/f/handbook/home.html.

Receiving weekly support updates

To receive weekly e-mail notifications about fixes and other software support news, follow these steps:

1. Go to the IBM Software Support website at http://www.ibm.com/software/support.
2. Click **My support** in the far upper-right corner of the page under **Personalized support**.
3. If you have already registered for **My support**, sign in and skip to the next step. If you have not registered, click **register now**. Complete the registration form using your e-mail address as your IBM ID and click **Submit**.
4. The **Edit profile** tab is displayed.
5. In the first list under **Products**, select **Software**. In the second list, select a product category (for example, **Systems and Asset Management**). In the third list, select a product sub-category (for example, **Application Performance & Availability** or **Systems Performance**). A list of applicable products is displayed.
6. Select the products for which you want to receive updates.
7. Click **Add products**.
8. After selecting all products that are of interest to you, click **Subscribe to email** on the **Edit profile** tab.
9. In the **Documents** list, select **Software**.
10. Select **Please send these documents by weekly email**.
11. Update your e-mail address as needed.
12. Select the types of documents you want to receive.
13. Click **Update**.

If you experience problems with the **My support** feature, you can obtain help in one of the following ways:

Online
Send an e-mail message to erchelp@ca.ibm.com, describing your problem.

By phone
Call 1-800-IBM-4You (1-800-426-4968).

Contacting IBM Software Support

IBM Software Support provides assistance with product defects. The easiest way to obtain that assistance is to open a PMR or ETR directly from the IBM Support Assistant.

Before contacting IBM Software Support, your company must have an active IBM software maintenance contract, and you must be authorized to submit problems to IBM. The type of software maintenance contract that you need depends on the type of product you have:

- For IBM distributed software products (including, but not limited to, Tivoli, Lotus®, and Rational® products, as well as DB2 and WebSphere products that run on Windows or UNIX operating systems), enroll in Passport Advantage® in one of the following ways:

  Online
  Go to the Passport Advantage website at http://www-306.ibm.com/software/howtobuy/passportadvantage/pao_customers.htm .

  By telephone
  For the telephone number to call in your country, go to the IBM Software Support website at http://techsupport.services.ibm.com/guides/contacts.html and click the name of your geographic region.
- For customers with Subscription and Support (S & S) contracts, go to the Software Service Request website at https://techsupport.services.ibm.com/ssr/login.
- For customers with Linux, iSeries®, pSeries, zSeries, and other support agreements, go to the IBM Support Line website at http://www.ibm.com/services/us/index.wss/so/its/a1000030/dt006.
- For IBM eServer™ software products (including, but not limited to, DB2 and WebSphere products that run in zSeries, pSeries, and iSeries environments), you can purchase a software maintenance agreement by working directly with an IBM sales representative or an IBM Business Partner. For more information about support for eServer software products, go to the IBM Technical Support Advantage website at http://www.ibm.com/servers/eserver/techsupport.html.

If you are not sure what type of software maintenance contract you need, call 1-800-IBMSERV (1-800-426-7378) in the United States. From other countries, go to the contacts page of the *IBM Software Support Handbook* on the web at http://www14.software.ibm.com/webapp/set2/sas/f/handbook/home.html and click the name of your geographic region for telephone numbers of people who provide support for your location.

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.
19-21, Nihonbashi-Hakozakicho, Chuo-ku
Tokyo 103-8510, 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. 2013. All rights reserved.

If you are viewing this information in softcopy form, the photographs and color illustrations might not be displayed.

Index

Printed in USA