Tivoli® IBM Tivoli Monitoring

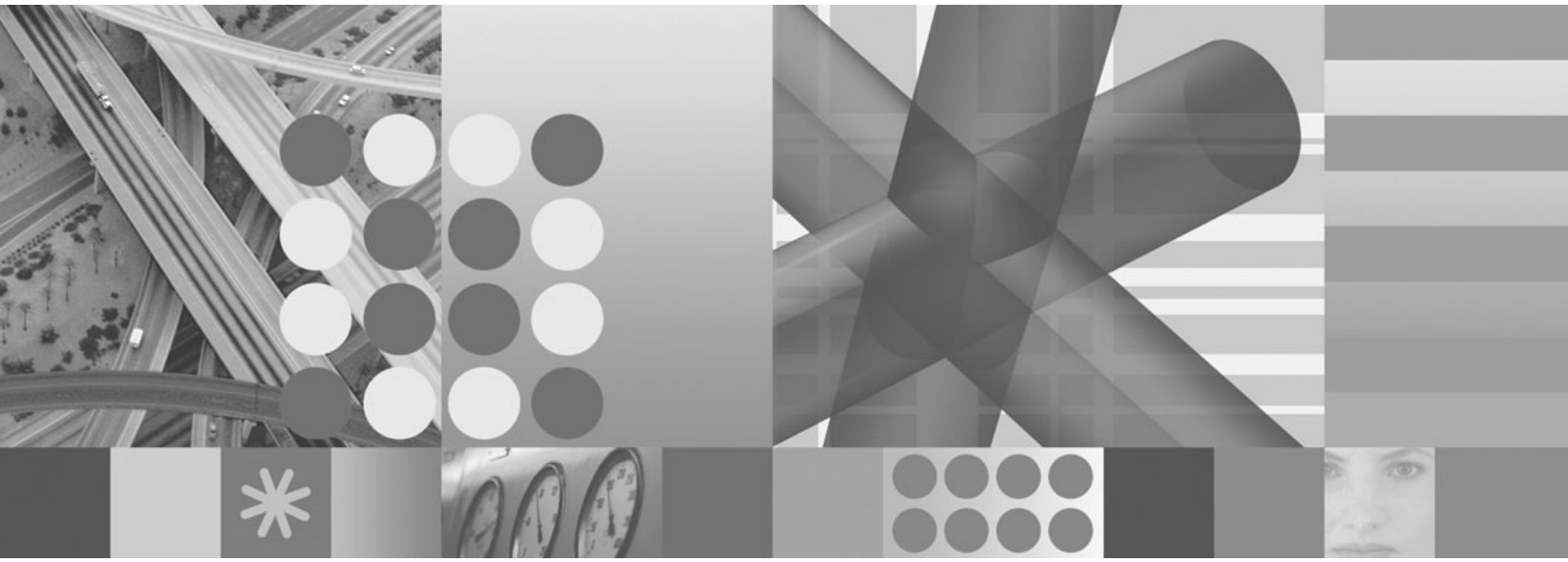
Version 6.1

Fix Pack 005 Readme and Documentation Addendum

SC23-5960-00

Tivoli® IBM Tivoli Monitoring

Version 6.1



Fix Pack 005 Readme and Documentation Addendum

SC23-5960-00

Note
Before using this information and the product it supports, read the information in "Notices," on page 89.

This edition applies to the version 6, release 1, modification 0 of IBM Tivoli Monitoring (product number 5724-C04) and to all subsequent releases and modifications until otherwise indicated in new editions.

© Copyright International Business Machines Corporation 2007. All rights reserved.
US Government Users Restricted Rights – Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.

Contents

Chapter 1. Fix Pack 005 overview 1
Supported operating systems 2
Supported databases for Tivoli Enterprise Portal Server and Tivoli Data Warehouse 7

Chapter 2. Planning your fix pack installation 9
Fix pack installation planning worksheets 9
Preserving user customizations 12
Files that are preserved on upgrade 12
Files that are not preserved on upgrade 13
Special exceptions 14
Changes in the behavior of the autostart scripts . . 14
Understanding the GA versions of the IBM Tivoli Monitoring version 6.1 agent CDs for Windows platforms 16
Identifying a refreshed version of IBM Tivoli Monitoring agent CD images 16
Summary of this section 17

Chapter 3. Fix pack installation instructions 19
Locations of installation logs. 21
Before you install this fix pack checklist 22
Single server quick installation checklist 25
Tivoli Enterprise Monitoring Server checklist . . . 27
Tivoli Enterprise Portal Server checklist 31
Tivoli Enterprise Portal desktop client checklist . . 33
Tivoli Enterprise Monitoring Agent checklist - local installation 34
Tivoli Enterprise Monitoring Agent checklist - remote deployment 35
Validating what you installed 37
Sample output for the kincinfo command on Windows 38
Sample output for the cinfo command on UNIX or Linux 40
Installing the fix pack for the i5/OS monitoring agent 42
Special instructions 42
Installing the i5/OS agent fix pack checklist . . 43
Installing the IBM Tivoli Enterprise Console event synchronization fix pack 44
Determining what level of event synchronization is installed. 45
Fix pack prerequisites 46
Notes about rule bases 46
Important information for Windows users . . . 47
Installation instructions 47
Verifying the installation of the event synchronization fix pack 51
Uninstalling the IBM Tivoli Enterprise Console event synchronization 51

Chapter 4. After you install 53
Clearing the Tivoli Enterprise Portal browser cache 53
Determining what components were installed . . . 53
Installing Global Services Kit (GSKit) if you use silent installation 53
Securing your Linux or UNIX IBM Tivoli Monitoring installation 53
Installing the upgrade toolkit on Solaris computers 54
Installing Java Web Start 54
Installing upgrades to monitoring agents 55
Understanding deployment options 55
Exploiting new configuration options for z/OS components 55

Chapter 5. Known problems and limitations 57
General installation component issues 57
Remote deployment issues 58
Tivoli Enterprise Monitoring Agents 60
Tivoli Enterprise Monitoring Server 60
Tivoli Enterprise Monitoring Server on distributed platforms issues 60
Tivoli Enterprise Monitoring Server on z/OS issues 62
Tivoli Enterprise Portal desktop and browser clients 66
Tivoli Enterprise Portal Server 67
Historical data collection issues. 72
Summarization and pruning Agent 73
Warehouse Proxy Agent 74
Universal agent issues 74
Globalization 75
Online help 76

Chapter 6. APARs addressed by this fix pack. 77
Documentation APARs 77
Installation component APARs 78
Tivoli Enterprise Monitoring Agent APARs 79
Tivoli Enterprise Monitoring Server APARs. . . . 80
Tivoli Enterprise Portal APARs 84
Tivoli Enterprise Portal Server APARs 85
Tivoli Data Warehouse APARs 86
i5/OS OS monitoring agent APARs and defects . . 86
Linux OS monitoring agent APARs 86
Universal Agent APARs 87
UNIX Log Agent APARs 87
UNIX OS monitoring agent APARs 87
Windows OS monitoring agent APARs 88

Appendix. Notices 89
Trademarks 90

© Copyright IBM Corp. 2007

Chapter 1. Fix Pack 005 overview

Fix Pack 005 is a cumulative fix pack for IBM® Tivoli® Monitoring, Version 6.1.0. This readme and documentation addendum file provides details about installing the fix pack and information about changes to IBM Tivoli Monitoring in this release. The basic flow of this installation process is shown in Figure 1.

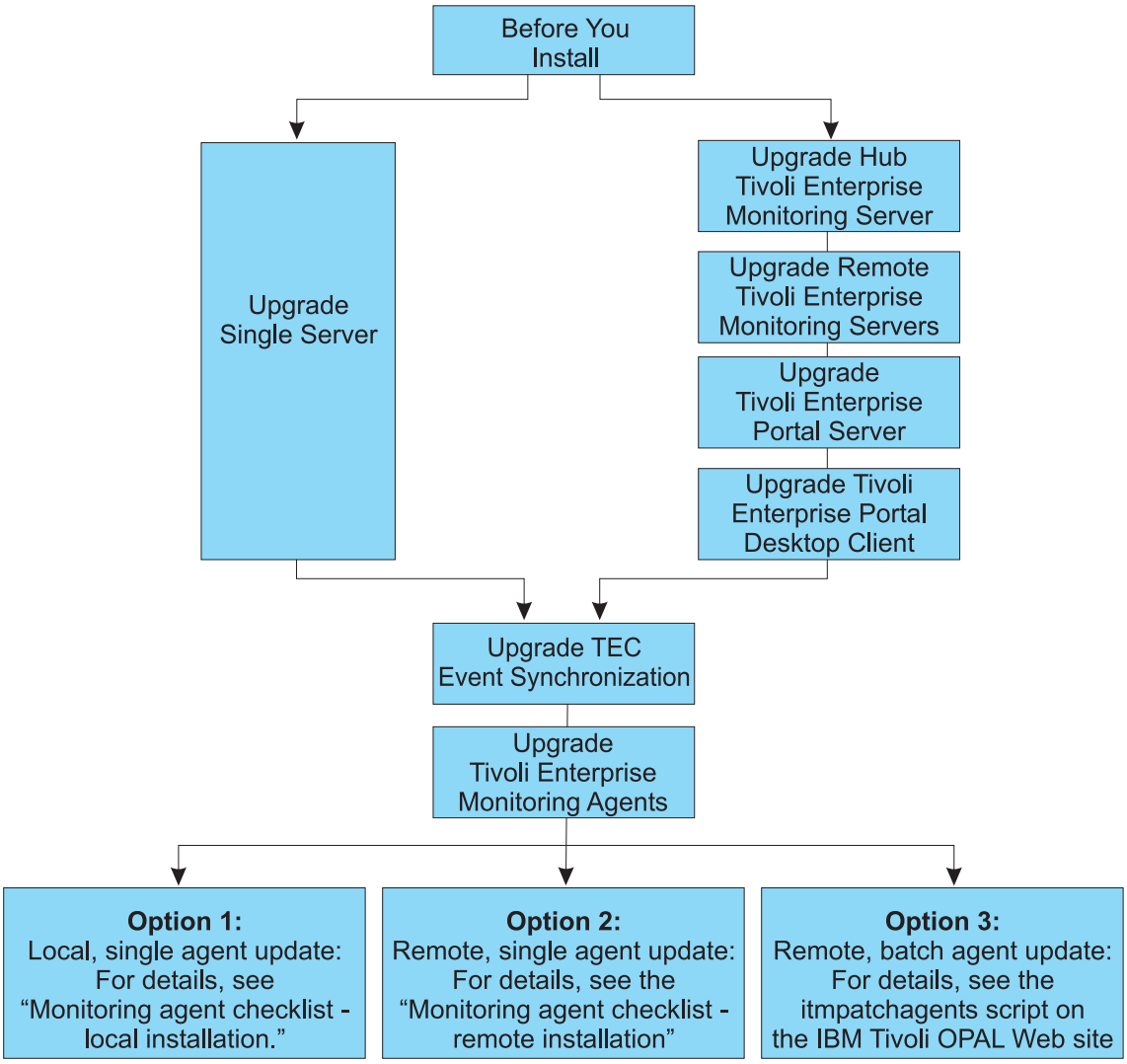


Figure 1. Installation flow for Fix Pack 005

You can download the IBM Tivoli Monitoring, Fix Pack 005 files from Passport Advantage® or from the **Downloads** section of the IBM Software Support Web site: http://www-306.ibm.com/software/sysmgmt/products/support/IBMTivoliMonitoringV6.html. The files listed in Table 1 on page 2 are available on the IBM Software Support Web site. See *IBM Tivoli Monitoring Passport Advantage Readme First* for details on fix pack file names and downloading the files from Passport Advantage.

© Copyright IBM Corp. 2007

Table 1. Fix Pack 005 file names

Fix pack file name	Platform
6.1.0-TIV-ITM_TMV-Windows-FP0005.zip	Windows® platforms
6.1.0-TIV-ITM_TMV-AIX-FP0005.tar	UNIX® platforms - AIX®
6.1.0-TIV-ITM_TMV-HPUXPARISC-FP0005.tar	UNIX platforms - HP-UX Integrity, HP-UX native processors
6.1.0-TIV-ITM_TMV-Solaris-FP0005.tar	UNIX platforms - Solaris
6.1.0-TIV-ITM_TMV-LinuxIA64-LinuxX64-FP0005.tar	Linux® on Intel® Itanium® and AMD Opteron 64-bit processors
6.1.0-TIV-ITM_TMV-Linuxip-FP0005.tar	Linux on pSeries®
6.1.0-TIV-ITM_TMV-Linuxz-FP0005.tar	Linux on zSeries®
6.1.0-TIV-ITM_TMV-LinuxIA32-1-FP0005.tar*	Linux Intel platforms (Part 1 of 2)
6.1.0-TIV-ITM_TMV-LinuxIA32-2-FP0005.tar*	Linux Intel platforms (Part 2 of 2)
PTFs for the Tivoli Enterprise™ Monitoring Server on z/OS®	z/OS
* Because of increases in the size of product components, support for Linux Intel platforms is split into two files. The following is a list of the content of each Linux Intel file. Some components are included on both files due to installation prerequisites. • **6.1.0-TIV-ITM_TMV-LinuxIA32-2-FP005.tar** is used to upgrade computers where the Tivoli Enterprise Portal Server is running. • **6.1.0-TIV-ITM_TMV-LinuxIA32-1-FP005.tar** is used to upgrade all other installations.	

Notes:

1. If you are running your monitoring server on a z/OS system, apply the z/OS Fix Pack 005 PTFs, available from IBM Software Support. See the "Tivoli Enterprise Monitoring Server checklist" on page 27 for more information.
2. There are no updates for help in this fix pack. Likewise, there is no updated language support.
3. The *IBM Tivoli Monitoring Version 6.1: Installation and Setup Guide* (Revised April 2007) (GC32-9407-00) and *IBM Tivoli Monitoring: Problem Determination Guide* (Revised April 2007) (GC32-9458-00) were refreshed for this fix pack. If you have an older version of these documents on your workstation, download the new versions from http://publib.boulder.ibm.com/infocenter/tivihelp/v15r1/index.jsp?toc=/com.ibm.itm.doc/toc.xml.
4. If you are running OMEGAMON® XE products and plan to upgrade to IBM Tivoli Monitoring version 6.1 Fix Pack 005, refer to the **Planning Upgrades** section of the following Web site for OMEGAMON XE recommended maintenance levels: http://www-306.ibm.com/software/sysmgmt/products/support/IBMTivoliMonitoringV6.html

See Chapter 3, "Fix pack installation instructions," on page 19 for detailed installation procedures.

Supported operating systems

Fix Pack 005 adds support for additional operating systems. The following tables show which operating systems are supported for the different IBM Tivoli Monitoring components in this fix pack: monitoring server, portal server, portal client, monitoring agent, Warehouse Proxy, and Warehouse Proxy Summarization and Pruning agent. Support that was added in Fix Pack 005 is marked **New**.

For additional information about the operating systems supported, see http://www-306.ibm.com/software/sysmgmt/products/support/Tivoli_Supported_Platforms.html.

Table 2 shows the support for monitoring components on Windows computers.

Table 2. Supported Windows operating systems for IBM Tivoli Monitoring V6.1 Fix Pack 005 monitoring components

Operating system	Monitoring server	Portal server	Portal client[1]	OS monitoring agent[2]	Warehouse Proxy	Warehouse Summarization and Pruning agent
Windows 2000 Professional[3]			X	X		X
Windows 2000 Server	X	X	X	X	X	X
Windows 2000 Advanced Server	X	X	X	X	X	X
Windows XP[3]			X	X	X	X
Windows 2003 Server SE (32 bit) with Service Pack 1[4]	X	X	X	X	X	X
Windows 2003 Server EE (32 bit) with Service Pack 1[4]	X	X	X	X	X	X
Windows Server 2003 Data Center (32 bit)				X		
Windows 2003 SE (64 bit)				X		
Windows 2003 EE (64 bit)				X		
Windows Server 2003 Data Center (64 bit)				X[5]		
Windows 2003 Server on Itanium2				X		
Windows 2003 on VMWare ESX Server V2.5.2 **and V3.0**	X	X	X	X	X	X
Windows Vista (32 bit)[3]			X			
Windows Vista (64 bit)[3]			**New**			

Notes:

1. The Tivoli Enterprise Portal desktop client is supported on marked platforms. However, the browser client can be accessed only from Windows computers running Internet Explorer 6 or 7.
2. The **OS monitoring agent** column indicates the platforms on which an operating system monitoring agent is supported. This column does not indicate that any agent runs on any operating system. For example, to monitor a Linux computer, you must use a Linux monitoring agent, not a Windows monitoring agent.

   For information about the operating systems supported for non-OS agents, see the documentation for the specific agents you are using in your environment.
3. For the Windows 2000 Professional, Windows XP, and Windows Vista operating systems, the Microsoft® End User License Agreement (EULA) does not license these operating systems to function as a server. Tivoli products that function as a server on these operating systems are supported for demonstration purposes only.
4. For Windows 2003 Server: If you do not plan to deploy Service Pack 1 in your environment at this time, you must download and install Microsoft Installer 3.1 (KB893803), which is available from the Microsoft Download Web site (www.microsoft.com/downloads).
5. Windows Server 2003 Data Center (64 bit): Supported only for the Tivoli Enterprise Monitoring Agent, not for the OS agent.

Table 3 on page 4 shows the support for monitoring components on UNIX (non-Linux), i5/OS®, and z/OS computers.

Table 3. Supported UNIX, i5/OS, and z/OS operating systems for IBM Tivoli Monitoring V6.1 Fix Pack 005 monitoring components

Operating system	Monitoring server	Portal server	Portal client	OS monitoring agent[1, 2]	Warehouse Proxy	Warehouse Summarization and Pruning agent
AIX V5.1 (32/64 bit)				X		X
AIX V5.2 (32/64 bit)	X			X		X
AIX V5.3 (32/64 bit)	X	X		X	X	X
Solaris Operating Environment V8 (32/64 bit)	X			X		X
Solaris V9 (SPARC)	X			X		X
Solaris V10 (SPARC)	X			X		X
Solaris V10 (x86-64) on AMD Opteron	X			X		
Solaris Zones	X[3]			X[3, 4]		X[3]
HP-UX 11i v1 (B.11.11) abd HP-UX 11i v2 (B.11.23) (32/64) on PA-RISC[5]				X		
HP-UX 11i v3 (B.11.31) (32/64) on PA-RISC				X		
HP-UX 11i v2 (B.11.23) on Integrity (IA64)[8]				X[9]		
OS/400® 5.2				X		
i5/OS 5.3				X		
i5/OS 5.4				X		
z/OS 1.4[6, 7]	X			X		
z/OS 1.5[6, 7]	X			X		
z/OS 1.6[6, 7]	X			X		
z/OS 1.7[6, 7]	X			X		
z/OS 1.8[6, 7]	**New**			**New**		

Table 3. Supported UNIX, i5/OS, and z/OS operating systems for IBM Tivoli Monitoring V6.1 Fix Pack 005 monitoring components (continued)

Operating system	Monitoring server	Portal server	Portal client	OS monitoring agent[1, 2]	Warehouse Proxy	Warehouse Summarization and Pruning agent

Notes:

1. The **OS monitoring agent** column indicates the platforms on which an operating system monitoring agent is supported. This column does not indicate that any agent runs on any operating system. For example, to monitor a Linux computer, you must use a Linux monitoring agent, not a Windows monitoring agent.

   For information about the operating systems supported for non-OS agents, see the documentation for the specific agents you are using in your environment.
2. If you are installing the OMEGAMON XE for Messaging agent on a 64-bit operating system, you must install the 32-bit version of the agent framework. See the OMEGAMON XE for Messaging bullet in Chapter 5, "Known problems and limitations," on page 57 for details on installing this framework.
3. The monitoring server and the Warehouse Summarization and Pruning agent can run in both local and global zones on Solaris; however, the OS monitoring agent can run only in global zones.
4. You cannot use the remote deployment function for the agents on this operating system, which applies to both fresh installations and upgrades. Instead, you must install locally.
5. For HP-UX, patch PHSS_30970 is required.
6. For information about installing the monitoring server on z/OS, refer to the program directory that comes with that product.
7. The OS monitoring agent for z/OS computers is part of the IBM Tivoli OMEGAMON for z/OS product.
8. The following footnotes apply to HP-UX 11i v2 (B.11.23) on Integrity (IA64):
   - Fix Pack 005 does not support remote deployment for HP-UX 11i v2 on Integrity computers.
   - You cannot upgrade either the OS or Log Alert agents that you currently have running on an HP-UX 11i v2 (B.11.23) on Integrity (IA64) computer in PA-RISC mode prior to Fix Pack 004. Fix Packs prior to Fix Pack 004 did not run in native 64-bit mode by default. You must first uninstall the agent if the version is previous to the Fix Pack 004 version.
9. HP-UX 11i v2 (B.11.23) on Integrity (IA64) native 64-bit support was new for Fix Pack 004.

Table 4 shows the monitoring components supported on Linux operating systems.

Table 4. Supported Linux operating systems for IBM Tivoli Monitoring V6.1 Fix Pack 005 monitoring components

Operating system	Monitoring server	Portal server	Portal client[1]	OS monitoring agent[2, 7]	Warehouse Proxy	Warehouse Summarization and Pruning agent
Asianux 2.0 for Intel	**New**	**New**	**New**	**New**	**New**	**New**
Asianux 2.0 on Itanium 64				**New**		
Red Flag 4.1 for Intel	X	X	X	X	X	X
Red Flag 5.1 for Intel	**New**	**New**	**New**	**New**	**New**	**New**
RedHat Enterprise Linux 2.1 Intel				X		X
RedHat Enterprise Linux 3 on Intel				X	X	X
RedHat Enterprise Linux 3 on zSeries 31 bit				X	X	X
RedHat Enterprise Linux 3 on zSeries 64 bit				X	X	X

Table 4. Supported Linux operating systems for IBM Tivoli Monitoring V6.1 Fix Pack 005 monitoring components (continued)

Operating system	Monitoring server	Portal server	Portal client[1]	OS monitoring agent[2, 7]	Warehouse Proxy	Warehouse Summarization and Pruning agent
RedHat Enterprise and Desktop Linux 4 Intel	X	X	X	X	X	X
RedHat Enterprise Linux 4 on AMD64/EM64T				X		
RedHat Enterprise Linux 4 on Itanium 64-bit				X		
RedHat Enterprise Linux 4 on iSeries™ and pSeries				X		
RedHat Enterprise Linux 4 on zSeries 31 bit	X	X		X	X	X
RedHat Enterprise Linux 4 on zSeries 64 bit	X[4]	X[4, 6]		X	X	X
RedHat Enterprise Linux 4 for Intel on VMWare ESX Server V2.5.2 and **V3.0**	X	X	X	X	X	X
RedHat Enterprise and Desktop Linux 5 Intel	**New**	**New**	**New**	**New**	**New**	**New**
RedHat Enterprise Linux 5 on AMD64/EM64T				**New**		
RedHat Enterprise Linux 5 on Itanium 64 bit				**New**		
RedHat Enterprise Linux 5 on iSeries and pSeries				**New**		
RedHat Enterprise Linux 5 for z/Series 64-bit	**New**[4]	**New**[4, 6]		**New**[7]	**New**	**New**
SUSE Linux Enterprise Server 8 Intel				X	X	X
SUSE Linux Enterprise Server 8 for z/Series 31-bit				X	X	X
SUSE Linux Enterprise Server 8 for z/Series 64-bit				X	X	X
SUSE Linux Enterprise Server 9 Intel	X	X	X	X	X	X
SUSE Linux Enterprise Server 9 on AMD64/EM64T				X		
SUSE Linux Enterprise Server 9 on Itanium 64-bit[3]				X		
SUSE Linux Enterprise Server 9 for iSeries and pSeries				X		
SUSE Linux Enterprise Server 9 for z/Series 31-bit	X	X		X	X	X
SUSE Linux Enterprise Server 9 for z/Series 64-bit	X[4]	X[4, 6]		X	X	X

Table 4. Supported Linux operating systems for IBM Tivoli Monitoring V6.1 Fix Pack 005 monitoring components (continued)

Operating system	Monitoring server	Portal server	Portal client[1]	OS monitoring agent[2, 7]	Warehouse Proxy	Warehouse Summarization and Pruning agent
SUSE Linux Enterprise Server 10 Intel	X	X	X	X	X	X
SUSE Linux Enterprise Server 10 on AMD64/EM64T[5]				X		
SUSE Linux Enterprise Server 10 on Itanium 64-bit[3, 5]				X		
SUSE Linux Enterprise Server 10 for iSeries and pSeries[5]				X		
SUSE Linux Enterprise Server 10 for z/Series 64-bit[5]	X[4]	**New**[4, 6]		X	X	X

Notes:

1. The Tivoli Enterprise Portal desktop client is supported on marked platforms. However, the browser client can be accessed only from Windows computers running Internet Explorer 6 or 7.
2. The **OS monitoring agent** column indicates the platforms on which an agent is supported. This column does not indicate that any agent runs on any operating system. For example, to monitor a Linux computer, you must use a Linux monitoring agent, not a Windows monitoring agent.
3. You cannot use the remote deployment function for the OS agent on this operating system, which applies to both fresh installations and upgrades. Instead, you must install locally.

   If you try to use the remote deployment function, you will receive the following error:

   ```
   KUICCN064E An appropriate installation image for the target platform, LINUX,
   could not be found on the local server.
   ```
4. This component supports the operating system in 64-bit tolerance mode.
5. See Technote 1247529 at http://www-1.ibm.com/support/docview.wss?uid=swg21247529 for minor known problems and workarounds for SUSE Linux Enterprise Server 10 on 64-bit operating systems.
6. You must install the Tivoli Enterprise Portal Server and its IBM DB2® database in a 31-bit mode session. Each time you start the Tivoli Enterprise Portal Server, you must be in a 31-bit mode session. To enter a 31-bit mode session, type `s390 sh` at the command line. The s390 command is included in the s390-32 rpm package and the 31-bit libraries.
   Note: SUSE Linux Enterprise Server 9 must be at SP3 or higher.
7. The Linux OS Monitoring Agent requires the installation of the latest versions of the following libraries:

   ```
   libstdc++
   libgcc
   compat-libstdc++
   libXp
   ```

   These libraries are available on the Linux operating system installation media and Service Packs. Each library can have multiple packages, and each must be installed.

Supported databases for Tivoli Enterprise Portal Server and Tivoli Data Warehouse

The following tables show the supported databases for the portal server and the Tivoli Data Warehouse.

Table 5 on page 8 shows the supported databases for the portal server. Note that the database and the portal server must be installed on the same computer.

Table 5. Supported databases for the portal server

Portal server operating system	Portal server database (″TEPS″)	
	IBM DB2*	**MS SQL**
AIX	IBM DB2 UDB V8.1 with Fix Pack 10 or higher fix packs and V8.2 with Fix Pack 3 or higher fix packs	
Linux	IBM DB2 UDB V8.1, with Fix Pack 10 or higher fix packs and V8.2 with Fix Pack 3 or higher fix packs.	
Windows	IBM DB2 UDB V8.1, with Fix Pack 10 or higher fix packs, V8.2 with Fix Pack 3 or higher fix packs, and V9.1* and fix packs.	MS SQL 2000 SP3

- ″TEPS″ is the default database name for the database used by the portal server.
- Support is for 32- or 64-bit databases.
- Your portal server database must be located on the computer where the portal server is installed.

* Support for IBM DB2 UDB V9.1 was added in Fix Pack 004. Support is for 32-bit only. 64-bit is not supported.

Table 6 shows the supported databases for the Tivoli Data Warehouse.

Table 6. Supported databases for the Tivoli Data Warehouse

Tivoli Data Warehouse database (″WAREHOUS″)		
IBM DB2[1]	**MS SQL**	**Oracle[2]**
IBM DB2 UDB V8.1, Fix Pack 10 and higher fix packs, V8.2, Fix Pack 3 and higher fix packs, and V9.1[4] and fix packs on the following operating systems: • AIX V5.3 • Solaris 10 • Windows 2003 Server • SUSE Linux Enterprise Server 9 and 10 for Intel • RedHat Enterprise Linux 4 for Intel	MS SQL 2000 **EE**[3] MS SQL 2005[3]	Oracle V9.2, 10g Release 1, and 10g Release 2 on the following operating systems: • AIX V5.3 • Solaris 10 • Windows 2003 Server • SUSE Linux Enterprise Server 9 and 10 for Intel • RedHat Enterprise Linux 4 for Intel

- ″WAREHOUS″ is the default database name for the database used by Tivoli Data Warehouse.
- Support is for 32- or 64-bit databases.
- Your Tivoli Data Warehouse database can be located on the same computer as your portal server or on a remote computer.

Notes:

1. Support for IBM DB2 UDB V9.1 was added beginning with Fix Pack 004. (Fix packs are cumulative.)
2. See the Oracle company support Web site (www.oracle.com) for information about installing and configuring Oracle on Solaris V10.
3. The Tivoli Enterprise Portal Server supports connecting to a Microsoft SQL Warehouse database only when the Tivoli Enterprise Portal Server is running on a Windows system
4. Support for DB2 V9.1 is 32-bit database only. 64-bit database is not supported.

Chapter 2. Planning your fix pack installation

The following table outlines the steps required to install the fix pack in your environment.

Table 7. Overall planning steps for Fix Pack 005

Goal	Where to find information
Gather the information you need to perform the installation.	"Fix pack installation planning worksheets"
Learn how to preserve your customizations	"Preserving user customizations" on page 12
Understand how the autostart script works	"Changes in the behavior of the autostart scripts" on page 14
Understand issues about the Windows versions of GA CDs	"Understanding the GA versions of the IBM Tivoli Monitoring version 6.1 agent CDs for Windows platforms" on page 16

Fix pack installation planning worksheets

Use the following worksheets to gather information about your monitoring environment.

Also, consider printing a list of all the computers in your environment; you can check off each computer as you update it, ensuring that you do not miss any.

© Copyright IBM Corp. 2007

Table 8. Fix pack planning worksheet

IBM Tivoli Monitoring installation directory (CANDLEHOME environment variable): **Note:** This directory is referred to as *ITMinstall_dir* in this document.				
Fix pack installation directory (where you extract the fix pack files): **Note:** This directory is referred to as *patch_dir* in this document.				
What is needed	**Other components also installed on this computer (circle those that apply)**	**How to gather this information**	**When this information is used**	**Notes**
Hub monitoring server host name	Portal server Portal desktop client Warehouse Proxy Summarization and Pruning agent	Manage Tivoli Enterprise Monitoring Server	"Tivoli Enterprise Monitoring Server checklist" on page 27	
Remote monitoring server host name	Portal server Portal desktop client Warehouse Proxy Summarization and Pruning agent	Manage Tivoli Enterprise Monitoring Server	"Tivoli Enterprise Monitoring Server checklist" on page 27	
Remote monitoring server host name	Portal server Portal desktop client Warehouse Proxy Summarization and Pruning agent	Manage Tivoli Enterprise Monitoring Server	"Tivoli Enterprise Monitoring Server checklist" on page 27	
Remote monitoring server host name	Portal server Portal desktop client Warehouse Proxy Summarization and Pruning agent	Manage Tivoli Enterprise Monitoring Server	"Tivoli Enterprise Monitoring Server checklist" on page 27	
Remote monitoring server host name	Portal server Portal desktop client Warehouse Proxy Summarization and Pruning agent	Manage Tivoli Enterprise Monitoring Server	"Tivoli Enterprise Monitoring Server checklist" on page 27	
Remote monitoring server host name	Portal server Portal desktop client Warehouse Proxy Summarization and Pruning agent	Manage Tivoli Enterprise Monitoring Server	"Tivoli Enterprise Monitoring Server checklist" on page 27	
Portal server host name	Monitoring server Portal desktop client Warehouse Proxy Summarization and Pruning agent	Manage Tivoli Enterprise Monitoring Server	"Tivoli Enterprise Portal Server checklist" on page 31	

Table 8. Fix pack planning worksheet (continued)

IBM Tivoli Monitoring installation directory (CANDLEHOME environment variable): **Note:** This directory is referred to as *ITMinstall_dir* in this document.				
Fix pack installation directory (where you extract the fix pack files): **Note:** This directory is referred to as *patch_dir* in this document.				
What is needed	**Other components also installed on this computer (circle those that apply)**	**How to gather this information**	**When this information is used**	**Notes**
Portal desktop client locations	Monitoring server Portal server Warehouse Proxy Summarization and Pruning agent	Manage Tivoli Enterprise Monitoring Server	"Tivoli Enterprise Portal desktop client checklist" on page 33	
Warehouse Proxy agent location	Monitoring server Portal server Portal desktop client Summarization and Pruning agent	Manage Tivoli Enterprise Monitoring Server	"Tivoli Enterprise Monitoring Agent checklist - local installation" on page 34	
Warehouse Summarization and Pruning agent location	Monitoring server Portal server Portal desktop client Warehouse Proxy	Manage Tivoli Enterprise Monitoring Server	"Tivoli Enterprise Monitoring Agent checklist - local installation" on page 34	
Agent types to update (product codes)		**tacmd listSystems**	"Tivoli Enterprise Monitoring Server checklist" on page 27 "Tivoli Enterprise Monitoring Agent checklist - local installation" on page 34	

Use the following table to identify the number of each type of agent to be updated.

Table 9. Agent updates table

Agent type	Number to update
NT (Windows OS)	
UX (UNIX OS)	
LZ (Linux OS)	
UL (UNIX Log)	
A4 (i5/OS)	
UM (Universal Agent)	

Preserving user customizations

During installation of a fix pack, many product files are replaced with newer versions. Other files are merged with existing files to produce the updated version. Still other files are generated by the installation process using values you provide.

These general rules apply to how user customizations are preserved:

- User-defined constructs are kept. For example situations, policies, queries, and workspaces are always preserved automatically on upgrade.
- Values you can change through a supported product interface are preserved.
- Values that you have changed manually (for example, because of a technote or as directed by IBM software support) are probably preserved. Any value that you have changed manually that was restored to a default value during an upgrade is recoverable from the backups made during upgrade.

The configuration process works with two basic types of files:

- ***.ini** (initialization) files are used to collect the inputs from the installation process, the responses to installation questions captured as keyword-value pairs. These are laid down with default values and basic information about that component.
- ***.config** (configuration) files are generated by the values in the .ini files and the values entered during configuration.

Essentially, **ini** files are source files, while **config** files are output files. Although the input ini files are modified by the configuration tools and sometimes by hand, the configuration output files are rarely modified. In fact, by their very nature, configuration files are generated, and thus anything changed "by hand" in configuration files is lost during the reconfiguration of that component.

To recover a lost "by hand" customization after installing a new fix pack, do the following:

1. Compare the new version of the .config or .ini or .config file with the version saved in the *ITMhome_dir*\backups\<*date_and_time_of_upgrade*> directory.
2. Change the installer-supplied defaults to the hand-edited values found in the backup file, make changes as required to carry your hand-edited customizations forwards, and save the new file.

Files that are preserved on upgrade

For components running on **Windows** computers, you can modify these files or settings and expect the changes to be preserved on upgrade:

- **ENV** files: The current settings from ENV files are preserved by checking "key = value" and adding keys that did not exist in the new file from the old file and replacing the value from the old file in the new file. Keys with default values are preserved.
- **INI** files: The ini files are preserved as generally described above. If a change was made in from a provided configuration tool, the values is always preserved. If you were instructed by a technote or IBM support engineer to make a manual change, the value is most likely, but not always, preserved (depends on what you changed and why).
- **Bannerimage.html** in the CNB directory: if you add a customer image for your own banner, this is preserved.
- **OM_TEC.config** in the CMS\TECLIB directory.
- **cnp.bat** or **cnp_<***inst***>.bat** (where <*inst*> can be the name of an of an instance of the Tivoli Enterprise Portal to connect to): Any changes made to the -D flags on the Java calls of these files are preserved.
- **Applet.html**: Any changes made to the -D flags in file is preserved.

For components running on UNIX or Linux computers, you can modify these files or settings and expect the changes to be preserved on upgrade:

- **ENV** files: The current settings from ENV files are preserved by checking "key = value" and adding keys that did not exist in the new file from the old file and replacing the value from the old file in the new file. Keys with default values are preserved.
- **INI** files: The ini files are preserved as generally described above. If a change was made using a provided configuration tool, the values is always preserved. If you were instructed by a technote or IBM support engineer to make a manual change, the value is most likely, but not always, preserved (depends on what you changed and why).
- **Bannerimage.html** in the CNB directory: if you add a customer image for your own banner, this is preserved.
- **cnp.sh** or **cnp_ <***inst***>.sh** (where <*inst*> can be the name of an of an instance of the Tivoli Enterprise Portal to connect to): Any changes made to the -D flags on the Java calls of these files are preserved.
- **Applet.html**: Any changes made to the -D flags in file is preserved.

Files that are not preserved on upgrade

For components running on **Windows** computers, you cannot modify these files because they will be replaced or regenerated on upgrade:

- On the Tivoli Enterprise Portal Server, the **CNP.bat** and **applet.html** files are built based on the content of the CNPS, CNP, and CNB directories. Other than the above –D flag exclusion, everything in this file is regenerated .
- The buildpresentation.bat file is generated by during installation. Any updates to this file will be lost.
- These TEC event synchronization files:
  - In the TEC_CLASSES directory of the rulebase created during TEC event synchronization install: `omegamon.baroc`.
  - In the TEC_RULES directory of the rulebase created during TEC event synchronization install: `omegamon.rls`.

Before these files are replaced, backup copies are made automatically and placed in the same directories as the original files and have suffix .“bac” added to their names. You can open these backup files and migrate customer modifications manually.

For components running on **UNIX** or **Linux** computers, you cannot modify these files because they will be replaced or regenerated on upgrade:

- *ARCH*/cq[cj][cw]/* (where *ARCH* is a specific architecture, such as li6243) and one of following two-letter codes: cq, cj, or cw). These files (unless otherwise noted above) are overwritten during upgrade.
- /etc/initd/ITMagents* (the ITMagents boot restart files). These files are regenerated during the installation and configuration.

Special exceptions

Two UNIX configuration files exist that typically would not have their values persisted, but which in fact do persist values. These two files are as follows:

- <*ITMhome_dir*>/tables/<*TEMS_name*>/KBBENV
- <*ITMhome_dir*>/config/.ConfigData/<hostname>_ms_<*TEMS_name*>.config.

These files are generated from kbbenv.ini and ms.ini respectively. Changes made to these files are saved in the same way that changes made to the source ini files are saved.

Changes in the behavior of the autostart scripts

The behavior of the autostart scripts generated by installation of fix packs on UNIX platforms has evolved.

- In Fix Pack 003, the installation process produced an autostart script with only one entry using a generic `CandleAgent start all` command and users modified this file as needed.
- In Fix Pack 004, the installation process generated individual entries for each application in a particular installation, but the values captured in the file could not be overridden.
- In Fix Pack 005, the multiple entries remain and an override capability has been added.

The autostart script, named ITMAgents<*N*> or rc.itm<*N*> depending on the UNIX platform, generated by an installation or upgrade contains an entry for each application in a particular installation. The entries look similar to this

```
su - <USER> -c "ITM_Install_Home/bin/itmcmd agent start <product_code>"
```

Or

```
su - <USER> -c "ITM_Install_Home/bin/itmcmd agent –o <Instance> start <product_code>"
```

Where:

USER The ID that the application will be started as. By default, *USER* is the owner of the bin directory for the application. For the UNIX Log Alert agent, *USER* is the owner of the *ITM_Install_Home*/*PLAT*/ul/bin directory.

N Is an integer specific to each installation on a system.

ITM_Install_Home
: Is the full path to the IBM Tivoli Monitoring version 6.1 installation directory.

product_code
: Is the two-character code for this application. Refer to "Sample output for the kincinfo command on Windows" on page 38 for a list of the component codes.

instance
: Is the instance name required to start this application.

PLAT
: Is the platform directory where the application is installed.

The `kcirunas.cfg` file was added to allow overrides to this default processing. The `kcirunas.cfg` file is delivered in the root directory of the media, in the same location as install.sh. During installation, this file is copied to the *ITM_Install_Home*/config directory. This file is provided as a sample file with each section commented out. You do not have to modify this file if you want the autostart script to be generated with the default processing.

For local installation usage, you may modify the `kcirunas.cfg` file in the root directory of the media if you want to use the same set of values for multiple installations on similar systems from this image. You may also modify the `kcirunas.cfg` file in the *ITM_Install_Home*/config directory if you want to use a specific set of values for each individual installation from this image.

For remote deployment usage, you can modify the `kcirunas.cfg` file in the root directory of the media. You can also modify the `kcirunas.cfg` file in the Tivoli Enterprise Monitoring Server depot after populating the depot from this image. To locate the `kcirunas.cfg` in the monitoring server depot, run the following commands:

```
cd ITM_Install_Home
find tables –name kcirunas.cfg -print
```

The file `kcirunas.cfg` has the same syntax and structure as the *ITM_Install_Home*`/config/`*HOST*`_kdyrunas.cfg` (where *HOST* is the short hostname for this system) produced by remote configurations, such as remote deployment or Tivoli Enterprise Portal-based agent configuration. By default, each product code section is disabled by making the product code item a comment such as `<!productcode>`. To activate a section, do the following:

1. Remove the comment indicator (the exclamation point, !) so that the product code item looks like <product_code>.
2. Copy a product code section.
3. Customize the product code section and activate it, rather than create new sections from scratch.

Commented, or *de-activated*, sections are ignored. Uncommented, or *activated*, sections for applications that are not installed are ignored. For agents that do not require an instance value, specify only the <product_code>, <instance> and <User>. For agents that do require an <instance> value, specify the <product_code>, <instance>, <User> and <name>.

Notes:

1. Any changes made directly to the autostart script (`ITMAgents`*N* or `rc.itm`*N* depending on the platform) will not be preserved and will be overwritten the next time that you configure an application, or install or upgrade an application.

2. Any changes made to the `AutoRun.sh` script will not be preserved and will be overwritten the next time you apply higher maintenance.

Understanding the GA versions of the IBM Tivoli Monitoring version 6.1 agent CDs for Windows platforms

The General Availability (GA) versions of the IBM Tivoli Monitoring version 6.1 agent CDs for the Windows operating system must *NOT* be installed into an IBM Tivoli Monitoring version 6.1 Fix Pack 005 environment or be used to populate a Tivoli Enterprise Monitoring Server depot. The IBM Tivoli Monitoring version 6.1 agent CDs have been refreshed for use with Fix Pack 005.

You experience this problem only if you ordered and received your copy of the GA agents prior to April 1, 2006. In March 2006, all IBM Tivoli Monitoring version 6.1 GA agents were refreshed to correct the problem. All copies of GA agents ordered and received after April 1, 2006 are corrected.

There is a problem with the installer on the GA version of the IBM Tivoli Monitoring version 6.1 agent CDs for the Windows operating system. If the GA version of agent CDs for Windows is used, the following events occur:

- The agent framework component is replaced by an older version.
- The OS agent fails.
- You will be unable to administer the system remotely.

The IBM Tivoli Monitoring version 6.1 agent CDs for the Windows operating system have been refreshed with an updated agent installer.

If you have already installed a GA-level agent after Fix Pack 005 installation, there is a way to recover. Obtain the refreshed ITM Tivoli Monitoring version 6.1 GA agent and run the installer from the refreshed agent CD. This will allow the Tivoli Enterprise Monitoring Agent component to be restored to the correct level. The agent version is NOT updated. The agents remain at the GA level.

You need to replace your GA version of the IBM Tivoli Monitoring version 6.1 agent CD images for the Windows operating system with the refreshed agent CD images. In addition, non-OS agents must also be recreated in the agent depot. If the GA version of non-OS agents has been placed in the agent depot, the agent bundle must be removed before it can be added back to the depot using the refreshed IBM Tivoli Monitoring version 6.1 agent CDs.

See Appendix A in the *IBM Tivoli Monitoring Administrator's Guide* for more information about using the **tacmd removeBundles** and **tacmd addBundles** commands to remove agents from and add agents to the agent depot.

Identifying a refreshed version of IBM Tivoli Monitoring agent CD images

Identify the refreshed IBM Tivoli Monitoring version 6.1 agent CD images by examining the KGLWICMA.ver file in the VERFiles directory of the CD image. The KGLWICMA.ver file indicates a VRMF value of 06100301 or later under the [COMPONENT INFO] tag as shown in the following example:

```
[COMPONENT INFO]
Product Code=GL
Desc=Tivoli Enterprise Monitoring Agent Framework
```

```
ComponentID=KGLWICMA
PlatformCode=WI
DPlatformCode=Windows
VRMF=06100301
```

To identify a refreshed agent image in an agent depot, the same KGLWICMA.ver exists in the VERFILES directory of the depot as shown in the following example:

```
C:\IBM\ITM\cms\Depot\Packages\WINNT\pc\061000000\VERFILES
```

where *pc* is one of the products codes in the KINCINFO command output, found at "Sample output for the kincinfo command on Windows" on page 38.

Summary of this section

Every General Availability (GA) version of the IBM Tivoli Monitoring version 6.1 agent for Windows operating system CD and installation image must be replaced with the refreshed version. Every GA version of the IBM Tivoli Monitoring version 6.1 agent bundle for the Windows operating system installed in a depot must be replaced with the refreshed version before it can be deployed into an IBM Tivoli Monitoring version 6.1 Fix Pack 005 environment. You will encounter this scenario only when you install a GA-level application agent *AFTER* you have deployed the Fix Pack 001, Fix Pack 002, or Fix Pack 004 OS agent.

Notes:

1. After you update the GA version of the IBM Tivoli Monitoring version 6.1 agent bundle with the refreshed version, that agent bundle *cannot* be used to remotely uninstall the GA version of the agent from an endpoint system.
2. If you install the Fix Pack 005 version of the Windows OS agent on a computer that already contains a GA version agent, you must update that GA version agent with the refreshed version. If you install the Fix Pack 005 Windows OS agent on a computer, you must make sure that any other agents installed on that same computer are updated with that agent's refreshed version. All Windows application agents were refreshed with the updated version of the installation code when Fix Pack 001 was released.
3. If you install the Fix Pack 005 Windows OS agent after installing the GA version of the application agent, the agent framework is updated to the refreshed version. However, if you modify the GA version of the application agent installation by adding another agent from the same image, the KGLWICMA.ver file will no longer be accurate and it will appear as if the agent framework is at the unrefreshed GA version.
4. Do *not* use the **tacmd updateAgent** command to update a GA version of an IBM Tivoli Monitoring version 6.1 agent on Windows computers with a refreshed version. If you do, you can cause the installation of the refreshed agent to create a duplicate entry in the Add/Remove Programs list on the computer that you are updating. If this occurs, delete the duplicate entry by running a local uninstallation of the agent after you remove the refreshed version of the IBM Tivoli Monitoring version 6.1 agent.

   Instead, you can use the **tacmd updateAgent** command to update a GA version of the agent with the agent *fix pack* image (and not the full image).

   Note: Since Fix Pack 004, this note applies to non-OS agents only.

Chapter 3. Fix pack installation instructions

The following table outlines the steps required to install the fix pack in your environment.

Table 10. Overall installation steps for Fix Pack 005

Goal	Where to find information
Ensure your monitoring environment is prepared for fix pack installation.	"Before you install this fix pack checklist" on page 22
If your Tivoli Enterprise Monitoring Server, Tivoli Enterprise Portal Server, and Tivoli Enterprise Portal desktop client are running on the same system, update that single server.	"Single server quick installation checklist" on page 25
Update your hub Tivoli Enterprise Monitoring Server	"Tivoli Enterprise Monitoring Server checklist" on page 27
Update your remote Tivoli Enterprise Monitoring Servers	"Tivoli Enterprise Monitoring Server checklist" on page 27
Update your Tivoli Enterprise Portal Server	"Tivoli Enterprise Portal Server checklist" on page 31
Update your Tivoli Enterprise Monitoring desktop clients	"Tivoli Enterprise Portal desktop client checklist" on page 33
Update your local Tivoli Enterprise Monitoring Agents	"Tivoli Enterprise Monitoring Agent checklist - local installation" on page 34
Remotely update other Tivoli Enterprise Monitoring Agents	"Tivoli Enterprise Monitoring Agent checklist - remote deployment" on page 35
Update your local i5/OS OS agents, if applicable.	"Installing the fix pack for the i5/OS monitoring agent" on page 42
Update your event synchronization on your IBM Tivoli Enterprise Console event server, if appropriate.	"Installing the IBM Tivoli Enterprise Console event synchronization fix pack" on page 44

Notes:

1. Because of increases in the size of product components, support for Linux Intel platforms is split into two files. See Table 1 on page 2 for the fix pack file that you must use for upgrading the IBM Tivoli Monitoring components.
2. If your Warehouse Proxy agent or Summarization and Pruning agent are on computers other than the monitoring server or portal server, use the instructions in the "Tivoli Enterprise Monitoring Agent checklist - local installation" on page 34 to install the updates.
3. As you upgrade the various components of the system, the installer shows you defaults based on your previous settings, the choices you made the last time you configured the component. If nothing has changed, you can press **Enter** to advance through the installation. However, if this is the first time a component has been configured, the installer presents common default settings.
4. If you use Fix Pack 005 to upgrade a remote Tivoli Enterprise Monitoring Server before you upgrade the hub monitoring server and the remote monitoring server is a machine with multiple IP interfaces, it might be necessary to set the KDEB_INTERFACE to the IP address of the primary remote monitoring server interface. The main symptom of this problem is empty Tivoli Enterprise Portal workspaces for agents that are attached to this remote

© Copyright IBM Corp. 2007

monitoring server. To correct this problem, add the statement KDEB_INTERFACELIST=<*IP_Address_of_Primary_Interface*> to the KBBENV file for the remote monitoring server.

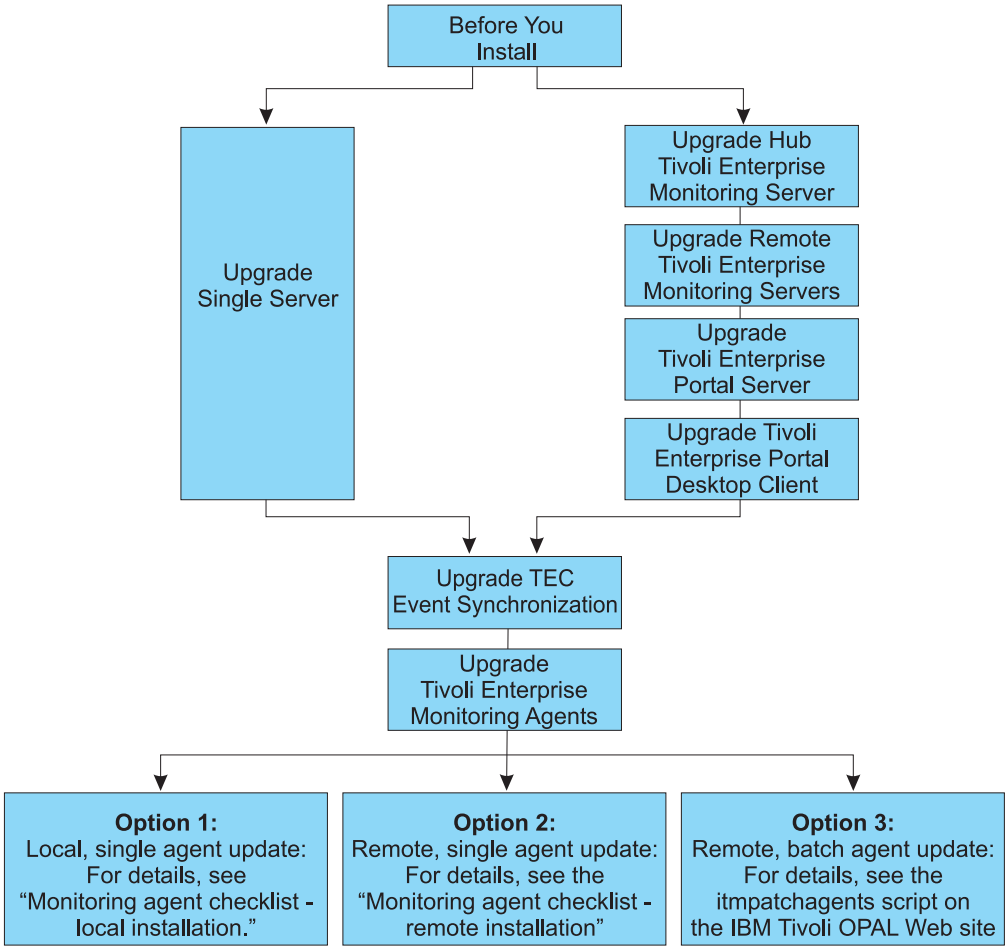
5. Fix Pack 005 makes changes to the WAREHOUSELOG table, adding a column named WPSYSTEM. This column represents the system name of the computer where the Warehouse Proxy Agent is installed. If the user ID used by the Warehouse Proxy Agent to connect to the warehouse database is not authorized to alter a table in the database, you may have to run the following command from the database administrator user ID. The command is the same for DB2, ORACLE, or Microsoft SQL databases:

   ```
   ALTER TABLE WAREHOUSELOG ADD WPSYSNAME CHAR(32);
   ```

   Run this command when fix pack installation is complete, before you restart the IBM Tivoli Monitoring components.

6. These checklists provide the order and procedures for installing the fix pack. Perform the tasks in the order shown.

Install your environment in the following order:



Locations of installation logs

If the installation of some component of the fix pack fails, that failure is typically documented in the installation logs. To find the installation logs for IBM Tivoli Monitoring components, look for the installation log files described in Table 11.

Table 11. Installation and startup log file names and locations

Activity	Windows	UNIX or Linux systems
During installation	*ITM_HOME*\InstallITM\Abort IBM Tivoli Monitoring *date_time*.log	$*ITM_HOME*/logs/candle_installation.log
While starting a component	• For the Tivoli Enterprise Portal: *ITM_HOME*\CNP\logs\kcjerror.log *ITM_HOME*\CNP\logs\kcjras1.log • For errors with distributed Tivoli Enterprise Monitoring Agents: *ITM_HOME*\TMAITM6\logs*hostname_pc_key*.log • For errors on the Tivoli Enterprise Portal Server, Tivoli Enterprise Monitoring Server, or warehouse proxy agent: *ITM_HOME*\logs*hostname_pc_key*.log where *hostname* is the hostname of the computer where the component is running, *pc* is the two-letter product code, and *key* is a hexadecimal identifier. Refer to the product code appendix in the *IBM Tivoli Monitoring: Installation and Setup Guide* for a list of product codes or to the output for the kincinfo info command found in "Sample output for the kincinfo command on Windows" on page 38.	$*ITM_HOME*/logs/*hostname_pc_key*.log

Before you install this fix pack checklist

Perform the following actions as appropriate before you install this fix pack.

Table 12. Checklist for actions to perform before you install this fix pack

✓	Installation step
	1. **US Customers Only:** If you have not done so already, adapt your system and the product set to **daylight savings time** changes. The switch to **daylight savings time** occurred 3 weeks earlier (March 11, 2007) this year in the United States than it did last year and also ends 1 week later on November 4, 2007. Refer to **URGENT Actions Required: Changes to Daylight Saving Time will affect IBM Tivoli Monitoring 6.1 and IBM Tivoli OMEGAMON 350/360 and their associated Operating Systems**, found at http://www-1.ibm.com/support/docview.wss?uid=swg21254621 for more information. In IBM Tivoli Monitoring version 6.1 Fix Pack 005, the JREs for some operating systems have been patched using the JTZU utility. • New Linux and UNIX users can begin using IBM Tivoli Monitoring version 6.1 with a JRE that is already corrected for Daylight Saving Time. They do not need to run the JTZU utility to update the IBM Tivoli Monitoring version 6.1 JREs. For information about the JTZU utility, see http://www-1.ibm.com/support/docview.wss?uid=swg21254621. • New Windows users, however, must run the JTZU utility to update the IBM Tivoli Monitoring version 6.1 JREs. Refer to the sections "Patching Java™" and "Java Update First Steps" in the flash for more information. • All customers upgrading to IBM Tivoli Monitoring version 6.1 Fix Pack 005 from an earlier IBM Tivoli Monitoring Fix Pack must run the JTZU utility to update the IBM Tivoli Monitoring version 6.1 JREs. Refer to the sections "Patching Java" and "Java Update First Steps" in the flash for more information. If you have already run the JTZU utility against your JRE, it is not necessary to run it again after applying this fix pack. However, if you choose to run JTZU again, it will report that the JRE has already been updated.

Table 12. Checklist for actions to perform before you install this fix pack (continued)

✓	Installation step

	2. Back up your Tivoli Enterprise Monitoring Servers (hub and remote) and your Tivoli Enterprise Portal Server. If you encounter issues during fix pack installation, performing these backups will ensure that you have the information that IBM Software Support requires to recover your previous version. Do the following:
	On Linux or UNIX:
	a. Close the Tivoli Enterprise Portal browser and desktop clients.
	b. Stop the Tivoli Enterprise Portal Server, the Tivoli Enterprise Monitoring Server, the Eclipse Help Server, and all the monitoring agents running on the system.
	c. If the Tivoli Enterprise Portal Server is installed, run the following command:
	`./itmcmd execute cq "runscript.sh migrate-export.sh"`
	d. Use the tar command to compress the contents of *ITM_Install_dir*, the directory where IBM Tivoli Monitoring is installed, using a command such as:
	`tar -cvf /tmp/ITM_Install_dir.backup.tar ITM_Install_dir`
	e. Add the following files to the tar file created in step 4 above:
	• On AIX:
	`/etc/rc.itm*`
	`tar -uvf /tmp/ITM_Install_dir.backup.tar /etc/rc.itm*`
	• On HP-UX:
	`/sbin/init.d/ITMAgents*`
	`tar -uvf /tmp/ITMinstall_dir.backup.tar /etc/init.d/ITMAgents*`
	• On other UNIX or Linux systems:
	`/etc/initd/ITMAgents*`
	`tar -uvf /tmp/ITM_Install_dir.backup.tar /etc/init.d/ITMAgents*`
	f. Use the appropriate database commands to back up the Tivoli Data Warehouse databases.
	On Windows:
	a. Close the Tivoli Enterprise Portal browser and desktop clients.
	b. Stop the Tivoli Enterprise Portal Server, the Tivoli Enterprise Monitoring Server, the Eclipse Help Server, and all the monitoring agents running on the system.
	c. Launch **Manage Tivoli Monitoring Services** (KinConfg.exe) and select the **Advanced** option to unconfigure all of IBM Tivoli Monitoring processes, except the Tivoli Enterprise Portal desktop client. When you are finished, every component except the Tivoli Enterprise Portal desktop shows **configured = No** by its component name.
	d. Use a compression command to compress the contents of the *ITM_Install_dir* directory.
	e. Use the appropriate database commands to back up the Tivoli Enterprise Portal Server and Tivoli Data Warehouse databases.
	f. Use the regedit facility to export the entire Windows registry to file C:\WinRegB4Install.reg.

	3. On systems running the Tivoli Enterprise Portal browser client, clear the browser cache to avoid exception messages. a. From the Windows **Start** button, select **Control Panel**. b. Double-click the **Java Plug-in** icon to display the Java Plug-In Control Panel. c. Select the **Cache** tab. d. Click the **Clear** button and click **Apply**. e. Close the Java Plug-In Control Panel.
	4. Ensure that the browser that is used to connect to the Tivoli Enterprise Portal is running with Java version 1.4.2. Versions higher than 1.4.2 are not currently supported.

Table 12. Checklist for actions to perform before you install this fix pack (continued)

✓	**Installation step**
	5. If you are running firewall or anti-virus software on your system, check that the use of ephemeral ports for loopback operations are not blocked because the IBM Tivoli Monitoring installation program processes bind-and-connect, intra-process TCP sessions during the fix pack installation process.
	6. For UNIX computers, close Manage Tivoli Enterprise Monitoring Services before you upgrade to Fix Pack 005.
	7. Before installing the fix pack on UNIX or Linux computers, set the environment variable CANDLEHOME to the IBM Tivoli Monitoring installation directory by running the following command: `export CANDLEHOME=`*`ITMinstall_dir`* Where *ITMinstall_dir* is the location where IBM Tivoli Monitoring is installed.

	8. If you are installing the fix pack on Linux or UNIX computers, and you installed the IBM Tivoli Monitoring components (both the base monitoring components like the monitoring server and any monitoring agents) as a non-root user, you must perform the following steps to ensure that the user who installs the fix pack has the appropriate permissions:
	Note: *ITMinstall_dir* is the installation location for IBM Tivoli Monitoring and *user_id* is the ID that was used to install the IBM Tivoli Monitoring components.
	a. Log in to the computer as *user_id*.
	b. Run the following command to change ownership of root owned files modified by SetPerm previously back to *user_id*:
	`su - root -c "`*`ITMinstall_dir`*`/bin/UnSetRoot `*`user_id`*`"`
	c. Install the fix pack on the computer, following the steps outlined in the checklists.
	d. Run the following command to reset the file permissions and file ownership as required:
	`su - root -c "`*`ITMinstall_dir`*`/bin/SetPerm -a"`

Single server quick installation checklist

The following checklist is to be used only if you have the following components installed on the same system:

- Tivoli Enterprise Monitoring Server
- Tivoli Enterprise Portal Server
- Tivoli Enterprise Portal desktop client

Note: Only hub monitoring servers support SOAP servers.

Table 13. Checklist for installing the fix pack on a local host computer

✓	Installation step
	1. Gather information about the monitoring components in your environment. See "Fix pack installation planning worksheets" on page 9.
	2. Based on the platform of your local host computer, download and extract the required fix pack files to a temporary location on your computer. You can use the following space to write down the location of your patch directory. **Patch directory:**

	3. Install the fix pack.
	On Windows computers, launch the installation wizard by double-clicking the setup.exe file in the \WINDOWS subdirectory in the patch directory that you specified inStep 2.
	On Linux and UNIX computers, run the following command from the command line:
	`cd patch_dir`
	`./install.sh`
	Notes:
	a. From the component list, select only the components that you have previously installed for upgrade. The installer program displays the correct list of installed components from previous product or fix pack installations. If you clear an item that was selected, you will be removing or uninstalling the component rather than choosing not to upgrade it.
	b. On Windows computers, you must leave all of the items selected in the **Setup Type** window that is displayed after you install the fix pack.
	c. When you are asked if you want to add application support for other products, add application support for the Tivoli Enterprise Portal Server, the browser client, and the desktop client.

Table 13. Checklist for installing the fix pack on a local host computer (continued)

✓	Installation step

	4. On Linux and UNIX computers, re-apply application support on your local monitoring server.
	a. Run the following command to start the monitoring server:
	`./itmcmd server start tems_name`
	b. Run the following command to activate the application support on the monitoring server:
	`./itmcmd support [-h install_dir] [-m] -t tems_name pc`
	
	where:
	-h (optional) Parameter to specify the installation directory if it is not the one in which this script is located. Adding this parameter is typically not necessary. Also use this option to take action on an installation directory other than this one.
	install_dir The home directory that you created for IBM Tivoli Monitoring.
	-m (optional) Option to skip the installation of the product-provided situations and policies.
	-t Use this required option to specify the monitoring server name.
	tems_name Specifies the name of the monitoring server you are configuring. This argument is required.
	Notes:
	1) The monitoring server must be specified within the structure of *install_dir*.
	2) Be very careful when you enter the *tems_name* on a UNIX or Linux system. If you enter the name incorrectly, you will create a new monitoring server instance instead of upgrading the existing one. To recover from this situation, refer to the appendix on uninstalling IBM Tivoli Monitoring components in the *IBM Tivoli Monitoring: Installation and Setup Guide*.
	pc The product code of the product that will connect to this monitoring server. You can specify one or more products for which to add application support. If you are specifying multiple products, you must separate the product codes with either a space or comma as illustrated above.
	To view the product code for the application support you just installed, run the following command:
	`./cinfo`
	
	For sample output of this command, see "Validating what you installed" on page 37.
	c. Run the following command to stop the monitoring server:
	`./itmcmd server stop tems_name`
	d. Run the following command to restart the monitoring server:
	`./itmcmd server start tems_name`

	5. If the installation of this component failed refer to the installation logs found in Table 11 on page 21 for a description of installation problems.
	6. If you are running IBM Tivoli Monitoring in a globalized environment, re-install the latest IBM Tivoli Monitoring language pack. For information about installing the language packs, see the "Installing the language packs" section of the "Installing IBM Tivoli Monitoring"" of the *IBM Tivoli Monitoring Installation and Setup Guide*. **Note:** This requirement also applies if you reconfigure any of the base components, such as the portal server.

Tivoli Enterprise Monitoring Server checklist

The following checklist provides the fix pack installation steps for the hub and remote monitoring servers.

Notes:

1. Only hub monitoring servers support SOAP servers.
2. When a query through SOAP is issued to a monitoring agent such as the UNIX log agent, that query sometimes fails with a message such as ″Unable to start request.″ This is a timing error that occurs when the Tivoli Monitoring Services environment is starting up. The SOAP caching of nodes is not complete when the first SOAP query is made.

   To recover from this situation, recycle the SOAP server and the hub and remote Tivoli Enterprise Monitoring Servers.
3. The process for updating the hub and remote monitoring servers is the same, although you must update the hub monitoring server first, as shown in the fix pack installation flow chart.
4. The process for updating distributed monitoring servers is shown in Table 14. The process for updating a monitoring server on z/OS is shown in Table 15 on page 30.

Table 14. Checklist for installing the fix pack on the monitoring server on distributed platforms

✓	**Installation step**
	1. Gather information about the monitoring components in your environment. See “Fix pack installation planning worksheets” on page 9.
	2. In environments with multiple remote monitoring servers. to avoid communication problems after the installation, stop the monitoring agents associated with the monitoring server your are upgrading. Then stop the monitoring server you are upgrading.

	3. Install the fix pack.
	On Windows computers, launch the installation wizard by double-clicking the setup.exe file in the \WINDOWS subdirectory in the patch directory that you specified previously.
	On Linux and UNIX computers, run the following command from the command line:
	`cd patch_dir`
	`./install.sh`
	Ensure that you select **Tivoli Enterprise Monitoring Server** from the component list.

Table 14. Checklist for installing the fix pack on the monitoring server on distributed platforms (continued)

✓	**Installation step**
	4. On Linux and UNIX computers, reconfigure the monitoring server. a. At the command line change to the /opt/IBM/ITM/bin directory (or the directory where you installed IBM Tivoli Monitoring). b. Run the following command: `./itmcmd config -S -t tems_name` where *tems_name* is the name of your monitoring server. **Notes:** a. Be very careful when you enter the *tems_name* on a UNIX or Linux system. If you enter the name incorrectly, you will create a new monitoring server instance instead of upgrading the existing one. To recover from this situation, refer to the appendix on uninstalling IBM Tivoli Monitoring components in the *IBM Tivoli Monitoring: Installation and Setup Guide*. b. The name of the configuration file for the Tivoli Enterprise Monitoring Server is case-sensitive on UNIX and Linux. If you fail to enter these case-sensitive commands correctly, you may find that the changes you made to the Tivoli Enterprise Monitoring Server configuration have not been picked up because a second configuration file has been generated and is not being used at monitoring server startup. To fix this problem: 1) Look in the folder `/opt/IBM/ITM/config` to determine if there are two config files with similar names that differ only in the case of some part of the file name (for example, /opt/IBM/ITM/config/winlnx1a_ms_WINLNX1A.config and /opt/IBM/ITM/config/WINLNX1A_ms_WINLNX1A.config). 2) Check the last modified timestamp of both files. Delete the older file and rename the new one as appropriate.

Table 14. Checklist for installing the fix pack on the monitoring server on distributed platforms (continued)

✓	Installation step

	5. On Linux and UNIX computers, re-apply application support on your monitoring server.
	a. Run the following command to start the monitoring server:
	`./itmcmd server start tems_name`
	b. Run the following command to activate the application support on the monitoring server:
	`./itmcmd support [-h install_dir] [-m] -t tems_name pc`
	
	where:
	-h (optional) Parameter to specify the installation directory if it is not the one in which this script is located. Typically, this parameter is not required. Also use this option to take action on an installation directory other than this one.
	install_dir The home directory that you created for IBM Tivoli Monitoring.
	-m (optional) Option to skip the installation of the product-provided situations and policies.
	-t Use this required option to specify the monitoring server name.
	tems_name Specifies the name of the monitoring server you are configuring. This argument is required.
	Notes:
	1) The monitoring server must be specified within the structure of *install_dir*.
	2) Be very careful when you enter the *tems_name* on a UNIX or Linux system. If you enter the name incorrectly, you will create a new monitoring server instance instead of upgrading the existing one. To recover from this situation, refer to the appendix on uninstalling IBM Tivoli Monitoring components in the *IBM Tivoli Monitoring: Installation and Setup Guide*.
	pc The product code of the product that will connect to this monitoring server. You can specify one or more products for which to add application support. If you are specifying multiple products, you must separate the product codes with either a space or comma. To view the product code for the application support you just installed, run the `cinfo` command (for sample output, see "Validating what you installed" on page 37). **pc** will be one of the following.
	• A4 - AS/400®
	• LZ - Linux OS agent
	• UL - UNIX Log agent
	• UM - Universal agent
	• UX - UNIX OS agent
	• NT - Windows OS agent
	• SY - Summarization and Pruning agent
	
	Attention: Do not reapply application support for any agent not listed here. Applying application support files agents that were not updated as part of this fix pack might cause loss of customizations for those agents.
	c. Run the following command to stop the monitoring server:
	`./itmcmd server stop tems_name`
	
	Note: Be very careful when you enter the *tems_name* on a UNIX or Linux system. If you enter the name incorrectly, you will create a new monitoring server instance instead of upgrading the existing one. To recover from this situation, refer to the appendix on uninstalling IBM Tivoli Monitoring components in the *IBM Tivoli Monitoring: Installation and Setup Guide*.
	d. Run the following command to restart the monitoring server:
	`./itmcmd server start tems_name`

Table 14. Checklist for installing the fix pack on the monitoring server on distributed platforms (continued)

✓	Installation step
	6. If you are running IBM Tivoli Monitoring in a globalized environment, re-install the latest IBM Tivoli Monitoring language pack. For information about installing the language packs, see the "Installing the language packs" section of the "Installing IBM Tivoli Monitoring"" of the *IBM Tivoli Monitoring Installation and Setup Guide*.
	7. If the installation of this component failed, refer to the installation logs found in Table 11 on page 21 for a description of installation problems.
	8. Install the fix pack on the remaining components: portal server, portal desktop client, and monitoring agents (local and remote). The hub Tivoli Enterprise Monitoring Server, the Tivoli Enterprise Portal Server associated with the hub, and all of the Tivoli Enterprise Portal desktop clients that connect to that Tivoli Enterprise Portal Server must be upgraded to the same fix pack level. **Note:** This requirement also applies if you reconfigure any of the base components, such as the portal server.

Table 15 shows the process for updating a Tivoli Enterprise Monitoring Server on z/OS systems.

Table 15. Checklist for installing the fix pack on the Tivoli Enterprise Monitoring Server on z/OS systems

✓	Installation step
	1. Gather information about the monitoring components in your environment. See "Fix pack installation planning worksheets" on page 9.
	2. Access the IBM Tivoli Monitoring Version 6 support page at http://www-306.ibm.com/software/sysmgmt/products/support/IBMTivoliMonitoringV6.html and select the link for Fix Pack 005. Select each of the levelset PTFs and install it using the typical z/OS SMP/E installation procedures.
	3. If you are running OMEGAMON XE version 4.1 or OMEGAMON XE for Messaging version 6.0 monitoring agents and have applied IBM Tivoli Monitoring version 6.1 Fix Pack 005, apply the relink PTFs that have been provided by the OMEGAMON products. Refer to the PSP information and ++HOLD information in the OMEGAMON XE relink PTFs for additional instruction. For additional OMEGAMON XE maintenance, refer to the Planning Upgrades section of the following Web site for OMEGAMON XE maintenance levels: http://www-306.ibm.com/software/sysmgmt/products/support/IBMTivoliMonitoringV6.html. Depending on how you configured your runtime environments (RTEs), you may need to reload your RTEs after applying maintenance. The RTE Load function is typically not required after applying maintenance for RTEs that share the SMP/E TARGET libraries. If your RTEs are not SMP/E-sharing RTEs, you will probably need to reload the RTEs after applying maintenance. Check the ++HOLD information associated with the PTFs for any additional installation or configuration requirements.
	4. Install the fix pack on the remaining components: portal server, portal desktop client, and monitoring agents (local and remote). The hub Tivoli Enterprise Monitoring Server, the Tivoli Enterprise Portal Server associated with the hub, and all of the Tivoli Enterprise Portal desktop clients that connect to that Tivoli Enterprise Portal Server must be upgraded to the same fix pack level. **Note:** This requirement also applies if you reconfigure any of the base components, such as the portal server.

For other monitoring server on z/OS issues, see "Tivoli Enterprise Monitoring Server" on page 60.

Tivoli Enterprise Portal Server checklist

The following checklist provides the fix pack installation steps for the portal server.

Table 16. Checklist for installing the fix pack on the portal server

✓	Installation step
	1. Gather information about the monitoring components in your environment. See “Fix pack installation planning worksheets” on page 9.
	2. Based on the platform of your local host computer, download and extract the required fix pack files to a temporary location on your computer. You can use the following space to write down the location of your patch directory. **Patch directory:**
	3. Before you install the fix pack on a Tivoli Enterprise Portal Server on a Windows computer, ensure that the Windows Script Host (WSH) is at least version 5.6. You can check the version by running the **cscript** command.

	4. Install the fix pack.
	On Windows computers, launch the installation wizard by double-clicking the setup.exe file in the \WINDOWS subdirectory in the patch directory that you specified above.
	On Linux and UNIX computers, run the following command from the command line:
	`cd patch_dir`
	`./install.sh`
	Ensure that you select **Tivoli Enterprise Portal Server** from the component list.
	Notes:
	a. On Windows computers, you must leave all of the items selected in the **Setup Type** window that is displayed during the installation process.
	b. When you are asked if you want to add application support for other products, add application support for the Tivoli Enterprise Portal Server.
	c. Confirm that the Tivoli Enterprise Portal Server is running after upgrade. If it is not, restart it.

	5. If you are running IBM Tivoli Monitoring in a globalized environment, re-install the base IBM Tivoli Monitoring language pack. For information about installing the language packs, see the "Installing the language packs" section of the “Installing IBM Tivoli Monitoring” chapter of the *IBM Tivoli Monitoring Installation and Setup Guide*. **Note:** This requirement also applies if you reconfigure any of the base components, such as the portal server.
	6. If the installation of this component failed refer to the installation logs found in Table 11 on page 21 for a description of installation problems.
	7. Stop and restart Tivoli Enterprise Portal Server.
	8. Install the fix pack on the remaining components: portal desktop client and monitoring agents (local and remote). You must upgrade the Tivoli Enterprise Portal Server and the Tivoli Enterprise Portal desktop and browser clients to the same fix pack level.

If you are upgrading from IBM Tivoli Monitoring Version 6.1 Fix Pack 002 or earlier, you must migrate any custom workspaces containing Situation Event Console View(s) manually using this script and procedure:

1. Ensure that the Tivoli Enterprise Portal Server is running.
2. Ensure that the user running the command has write access to the current directory path because the script creates temporary files.
3. Run the following command:

Platform	Command
Windows	*ITM_HOME*\cnps\WSFixupEventConsole <*server*> <*username*> <*password*>
UNIX or Linux	*ITM_HOME*/bin/itmcmd execute cq "WSFixupEventConsole.sh <*server*> <*username*> <*password*>" **Note:** The double quotation marks are required to correctly invoke this script.

where:

<*server*>
: Is the hostname and port number of the Tivoli Enterprise Portal Server where you are running the script (for example, localhost:1920).

<*username*>
: Is the identifier of the user to authenticate on the Tivoli Enterprise Portal Server. The user must have both **Workspace Administration Mode** and **Workspace Author Mode** Workspace Administrator permissions enabled on the server.

<*password*>
: Is the password associated with the <*username*>.

Tivoli Enterprise Portal desktop client checklist

The following checklist provides the fix pack installation steps for the portal desktop client. Repeat this checklist for each desktop client in your environment.

Note: The installation procedures are the same as used for the GA level installation. For detailed installation procedures, see the "Installing IBM Tivoli Monitoring" chapter in the *IBM Tivoli Monitoring Installation and Setup Guide*.

Table 17. Checklist for installing the fix pack on the portal desktop client

✓	Installation step
	1. Gather information about the monitoring components in your environment. See "Fix pack installation planning worksheets" on page 9.
	2. Based on the platform of your local host computer, download and extract the required fix pack files to a temporary location on your computer. You can use the following space to write down the location of your patch directory. **Patch directory:**
	3. Close the Tivoli Enterprise Portal desktop client on the system where you are installing the fix pack.

	4. Install the fix pack.
	On Windows computers, launch the installation wizard by double-clicking the setup.exe file in the \WINDOWS subdirectory in the patch directory that you specified above.
	On Linux and UNIX computers, run the following command from the command line:
	`cd patch_dir`
	`./install.sh`
	Ensure that you select **Tivoli Enterprise Portal Desktop Client** from the component list.
	Notes:
	a. On Windows computers, you must leave all of the items selected in the **Setup Type** window that is displayed during the installation process.
	b. When you are asked if you want to add application support for other products, add application support for the desktop client.

	5. If you are running IBM Tivoli Monitoring in a globalized environment, re-install the base IBM Tivoli Monitoring language pack. For information about installing the language packs, see the "Installing the language packs" section of the "Installing IBM Tivoli Monitoring" chapter of the *IBM Tivoli Monitoring Installation and Setup Guide*. **Note:** This requirement also applies if you reconfigure any of the base components, such as the portal server.
	6. If the installation of this component failed refer to the installation logs found in Table 11 on page 21 for a description of installation problems.
	7. Install the fix pack on the monitoring agents (local and remote).

Tivoli Enterprise Monitoring Agent checklist - local installation

The following checklist provides the high-level local installation steps for OS monitoring agents that ship as part of base IBM Tivoli Monitoring. Other monitoring agents that ship as separate products are accompanied by readme files that contain additional information.

Notes:

1. The installation procedures are the same as used for the GA level installation. For detailed installation procedures, see the "Installing IBM Tivoli Monitoring" chapter in the *IBM Tivoli Monitoring Installation and Setup Guide*.
2. This checklist is for a local installation of the monitoring agents. You can also use the remote deployment function to deploy the monitoring agents across your monitoring environment. the remote deployment function, use the steps in the "Tivoli Enterprise Monitoring Agent checklist - remote deployment" on page 35.
3. For local installations, if you have the Universal Agent installed on a UNIX or Linux computer, you must upgrade the Universal Agent at the same time that you upgrade any other component to Fix Pack 005.

Table 18. Checklist for locally installing the fix pack on an agent

✓	Installation step
	1. Gather information about the monitoring components in your environment. See "Fix pack installation planning worksheets" on page 9.
	2. Based on the platform of your local host computer, download and extract the required fix pack files to a temporary location on your computer. You can use the following space to write down the location of your patch directory. **Patch directory:**

	3. Install the fix pack.
	On Windows computers, launch the installation wizard by double-clicking the setup.exe file in the \WINDOWS subdirectory in the patch directory that you specified above.
	On Linux and UNIX computers, run the following command from the command line:
	`cd patch_dir`
	`./install.sh`
	Ensure that you select the monitoring agents that you are upgrading from the component list.
	Note: On Windows computers, you must leave all of the items selected in the **Setup Type** window that is displayed after you install the fix pack.

	4. For OS agents, if you are running IBM Tivoli Monitoring in a globalized environment, re-install the base IBM Tivoli Monitoring language pack. For information about installing the language packs, see the "Installing the language packs" section of the "Installing IBM Tivoli Monitoring" chapter of the *IBM Tivoli Monitoring Installation and Setup Guide*. **Note:** This requirement also applies if you reconfigure any of the base components, such as the portal server.
	5. If the installation of this component failed refer to the installation logs found in Table 11 on page 21 for a description of installation problems.

Tivoli Enterprise Monitoring Agent checklist - remote deployment

The following checklist provides the remote installation steps for monitoring agents. Each agent is accompanied by a readme file that contains additional information. Be sure to check this readme file for any additional or unique installation steps.

Note: Consider increasing the **tacmd** timeout period to ensure that you can successfully deploy the fix pack. The default value is 30 minutes. Increase this period to at least 60 minutes (1 hour). The valid range for the timeout period is from 5 to 1440. Use the following steps to increase the timeout period:

On Linux and UNIX computers, edit the <*install_dir*>/bin/tacmd file and change the following environment variable:

```
TACMD_TIMEOUT=30
```

On Windows computers, edit the <*install_dir*>/bin/KUIENV file and change the following environment variable:

```
TACMD_TIMEOUT=30
```

For more information about setting the `TACMD_TIMEOUT` value, refer to the monitoring agent troubleshooting section of the *IBM Tivoli Monitoring: Problem Determination Guide.*.

Table 19. Checklist for remotely deploying the fix pack to an agent

✓	**Installation step**
	1. Add the agent updates to your agent monitoring server and hub monitoring server depot. On your agent monitoring server and hub monitoring server, run the following command from the fix pack directory to add the fix pack to the agent depot: *ITMinstall_dir*`/bin/tacmd addBundles -i` *patch_file* where *ITMinstall_dir* is the directory where you installed IBM Tivoli Monitoring and *patch_file* is the location of the fix pack. For additional information about the **tacmd addbundles** command, see the *IBM Tivoli Monitoring Installation and Setup Guide*.

Table 19. Checklist for remotely deploying the fix pack to an agent (continued)

✓	Installation step

	2. On the hub monitoring server, run the **tacmd updateAgent** command to remotely deploy the agent fix packs (which you previously added to the agent depot).
	`tacmd updateAgent -t pc -n node_name`
	
	where:
	pc Identifies the product to update, by product code. You have the following choices:
	• A4 - AS/400
	• LZ - Linux OS agent
	• UL - UNIX Log agent
	• UM - Universal agent
	• UX - UNIX OS agent
	• NT - Windows OS agent
	• SY - Summarization and Pruning agent
	node_name
	Identifies the node, the directory on the monitoring system where the OS agent is installed, to which you want to add the agent. The name of a node includes the computer where the OS agent is installed and the product code for the OS agent. For example, stone.ibm.com:LZ is the name of the node on computer stone.ibm.com, which has a Linux OS agent installed.
	The following example updates the Windows OS agent to the latest level available in the agent depot:
	`tacmd updateAgent -t NT -n Primary:WIN1:NT`
	The following example updates a Universal Agent running on a UNIX computer to a specific fix pack level:
	`tacmd updateAgent -t um -n unix1:KUX -v 061003010`
	Notes:
	a. If you have a large number of monitoring agents to which to deploy updates, consider using the itmpatchagents script, available as a sample from the IBM Tivoli Open Process Automation Library (http://www-18.lotus.com/wps/portal/topal). This script enables the automatic deployment of updates across your monitoring environment.
	b. The remote deployment of the Windows Operating System Agent now requires Java. If you use the `tacmd updateagent` command to update an agent on a remote Windows workstation or server, the deployment can fail because of this new Java requirement, with the following error messages:
	`KUICUA011I: Updating the NT agents.`
	
	`KUICUA015E: The updateAgent command did not complete because an error occurred.`
	`Refer to the following error returned from the server:`
	
	If you see this message, you have two options.
	• Review "Windows OS monitoring agent APARs" on page 88. If you do not need any of the fixes covered by these APARs, do not install the fixpack for the Windows OS agent.
	• Use this workaround to install the fix pack:
	1) Log on to the remote system and open a command window.
	2) From the command window, change directories to the *$ITM_HOME* directory (the default ish C:\IBM\ITM).
	3) Navigate to the tmaitm6\agentdepot\061005000\InIBMJRE directory.
	4) From that directory, install Java version 1.4.2 on the remote computer by launching **ibmjava142.exe** and accepting all the default values. You can choose a different installation drive, but do not change the directory structure for the installation.
	5) After Java is installed, you can use the `tacmd updateagent` command from the original deployment server to deploy and update the agent.

Table 19. Checklist for remotely deploying the fix pack to an agent (continued)

✓	Installation step
	3. For OS agents, if you are running IBM Tivoli Monitoring in a globalized environment, re-install the base IBM Tivoli Monitoring language pack. For information about installing the language packs, see the "Installing the language packs"s section of the "Installing IBM Tivoli Monitoring" chapter of the *IBM Tivoli Monitoring Installation and Setup Guide*. **Note:** This requirement also applies if you reconfigure any of the base components, such as the portal server.
	4. If the installation of this component failed refer to the installation logs found in Table 11 on page 21 for a description of installation problems.

For additional information about deployment issues, refer to the *IBM Tivoli Monitoring V6.1 Deployment Guide* found at this Web site: http://www.ibm.com/software/tivoli/opal/?NavCode=1TW10TM4J.

Validating what you installed

To validate that all components have been installed and are at the correct levels, open the Managing Tivoli Enterprise Monitoring Services status window, and compare your screen to the levels shown in Figure 2.

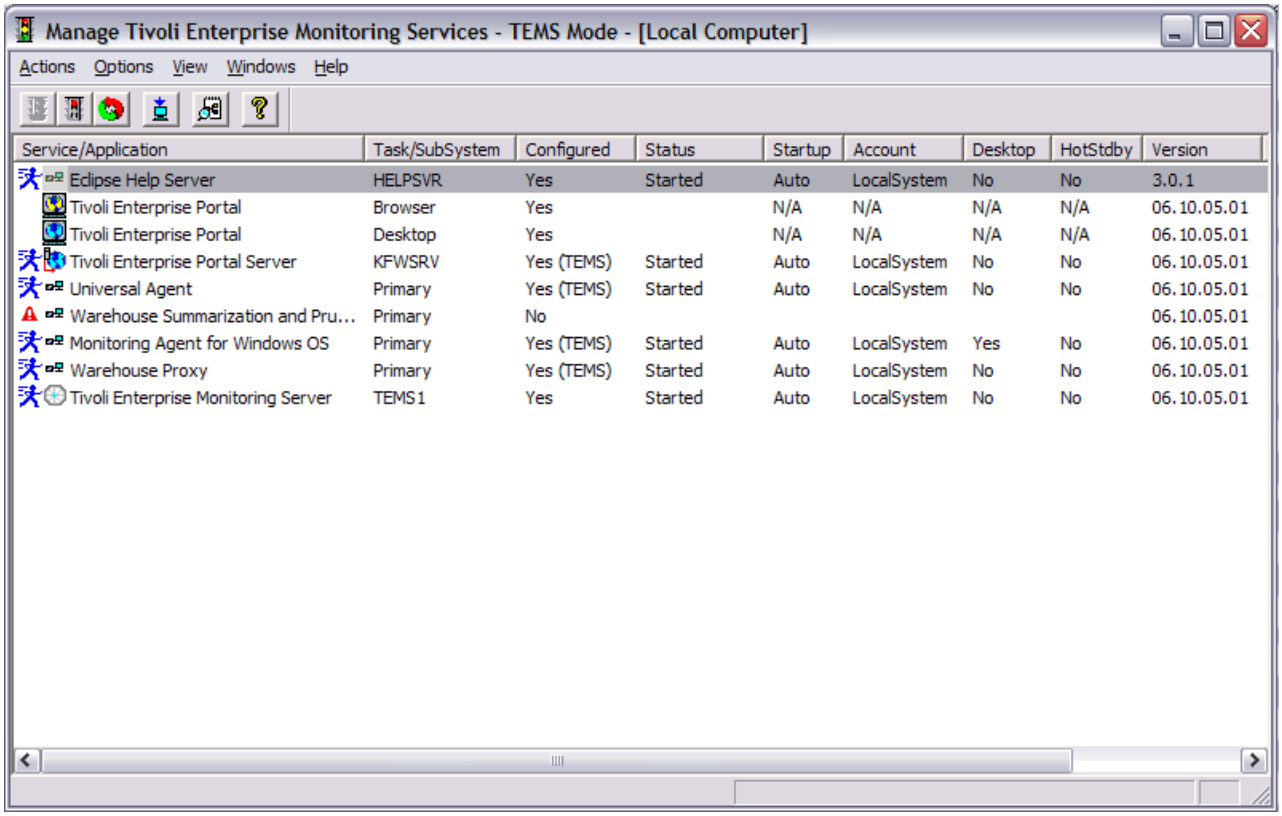


Figure 2. Levels for all components after applying Fix Pack 005

You can also validate your installation by running the `kincinfo` command on Windows or the `cinfo` command on Linux or UNIX.

Note: The `kincinfo` and `cinfo` command output examples in the sections that follow show that all components that can be updated. If you do not have all

of these components installed, then components not installed will not be displayed in the output of these commands.

Sample output for the kincinfo command on Windows

To run the `kincinfo`, open a command prompt window and enter the following command:

`kincinfo` *parameter*

where *parameter* is one of the following:

- `-d` displays a list of installed products, which can be parsed
- `-i` lists the inventory in English
- `-r` displays a list of running agents
- `-l` is the log switch

You must specify a parameter on this command. There is no default.

The following example shows the output of the `kincinfo -i` command:

```
kincinfo -i
********** Mon May 07 14:19:20 Eastern Daylight Time 2007 ********
User      : Administrator Group    : NA
Host Name : FVWIN18      Installer: Ver: 0NOVALUE00000
CandleHome: C:\IBM\ITM
************************************************************************
...Product Inventory

A4        i5/OS Support
          WINNT Version: 06.10.05.01 Build: 200702230014

A4        i5/OS Support
          WINNT Version: 06.10.05.01 Build: 200702230014

A4        i5/OS Support
          WINNT Version: 06.10.05.01 Build: 200702230014

A4        i5/OS Support
          WINNT Version: 06.10.05.01 Build: 200702230014

AX        Tivoli Enterprise Monitoring Agent Framework
          WINNT Version: 03.50.03.00 Build: 200510061051

CJ        Tivoli Enterprise Portal Desktop Client
          WINNT Version: 06.10.05.01 Build: 200705012123

CQ        Tivoli Enterprise Portal Server
          WINNT Version: 06.10.05.01 Build: 200705012135

CW        Tivoli Enterprise Portal Browser Client
          WINNT Version: 06.10.05.01 Build: 200705012123

GL        Tivoli Enterprise Monitoring Agent Framework
          WINNT Version: 06.10.05.01 Build: 200705012139

HD        Warehouse Proxy
          WINNT Version: 06.10.05.01 Build: 200705012139

IT        TEC GUI Integration
          WINNT Version: 06.10.05.01 Build: 200611010030

IT        TEC GUI Integration
          WINNT Version: 06.10.05.01 Build: 200611010031

IT        TEC GUI Integration
```

```
          WINNT Version: 06.10.05.01 Build: 200611010030

KF        IBM Eclipse Help Server
          WINNT Version: 06.10.05.01 Build: 200704171107

LZ        Linux OS Support
          WINNT Version: 06.10.05.01 Build: 200704301644

LZ        Linux OS Support
          WINNT Version: 06.10.05.01 Build: 200704301644

LZ        Linux OS Support
          WINNT Version: 06.10.05.01 Build: 200704301644

LZ        Linux OS Support
          WINNT Version: 06.10.05.01 Build: 200704301644

MS        Tivoli Enterprise Monitoring Server
          WINNT Version: 06.10.05.01 Build: 200705012139

NS        NLS Support
          WINNT Version: 03.50.03.00 Build: 200510061051

NT        Monitoring Agent for Windows OS
          WINNT Version: 06.10.05.01 Build: 200701160818

NT        Windows OS Support
          WINNT Version: 06.10.05.01 Build: 200701160818

NT        Windows OS Support
          WINNT Version: 06.10.05.01 Build: 200701160818

NT        Windows OS Support
          WINNT Version: 06.10.05.01 Build: 200701160818

NT        Windows OS Support
          WINNT Version: 06.10.05.01 Build: 200701160818

SY        Summarization and Pruning Agent
          WINNT Version: 06.10.05.01 Build: 200705012135

SY        Summarization and Pruning Agent
          WINNT Version: 06.10.05.01 Build: 200705012135

TM        IBM Tivoli Monitoring 5.x Endpoint Support
          WINNT Version: 06.10.05.01 Build: 200604051327

TM        IBM Tivoli Monitoring 5.x Endpoint Support
          WINNT Version: 06.10.05.01 Build: 200604051327

UI        Tivoli Enterprise Services User Interface
          WINNT Version: 06.10.05.01 Build: 200705012139

UL        UNIX Logs Support
          WINNT Version: 06.10.05.01 Build: 200701120847

UL        UNIX Logs Support
          WINNT Version: 06.10.05.01 Build: 200701120847

UL        UNIX Logs Support
          WINNT Version: 06.10.05.01 Build: 200701120847

UL        UNIX Logs Support
          WINNT Version: 06.10.05.01 Build: 200701120847

UM        Universal Agent
          WINNT Version: 06.10.05.01 Build: 200705012131
```

```
UM        Universal Agent Support
          WINNT Version: 06.10.05.01 Build: 200705012131

UM        Universal Agent Support
          WINNT Version: 06.10.05.01 Build: 200705012131

UM        Universal Agent Support
          WINNT Version: 06.10.05.01 Build: 200705012131

UM        Universal Agent Support
          WINNT Version: 06.10.05.01 Build: 200705012131

UX        UNIX OS Support
          WINNT Version: 06.10.05.01 Build: 200701161329

UX        UNIX OS Support
          WINNT Version: 06.10.05.01 Build: 200701161329

UX        UNIX OS Support
          WINNT Version: 06.10.05.01 Build: 200701161329

UX        UNIX OS Support
          WINNT Version: 06.10.05.01 Build: 200701161329

C:\ >
```

Sample output for the cinfo command on UNIX or Linux

To validate that all components have been installed, run the following command:

```
./cinfo
```

This command offers you four options on the CINFO menu shown in the example that follows. Choose the option that meets your needs.

```
*********** Mon May  7 14:35:50 EDT 2007 ******************
User      : root         Group: root sys dasadm1 db2grp1 db2fgrp1
Host name : cvtlin01     Installer Lvl:06.10.05.01
CandleHome: /usr/IBM/ITM
************************************************************

    -- CINFO Menu --
 1) Show products installed in this CandleHome
 2) Show which products are currently running
 3) Show configuration settings
 4) Show installed CD release versions
 X) Exit CINFO
1

*********** Mon May  7 14:35:53 EDT 2007 ******************
User      : root         Group: root sys dasadm1 db2grp1 db2fgrp1
Host name : cvtlin01     Installer Lvl:06.10.05.01
CandleHome: /usr/IBM/ITM
************************************************************
...Product inventory

a4      Monitoring Agent for i5/OS
         tms     Version: 06.10.05.01
         tpd     Version: 06.10.05.01
         tps     Version: 06.10.05.01
         tpw     Version: 06.10.05.01

ax      IBM Tivoli Monitoring Shared Libraries
         li6243  Version: 06.10.05.01

cj      Tivoli Enterprise Portal Desktop Client
         li6263  Version: 06.10.05.01
```

```
cq      Tivoli Enterprise Portal Server
         li6263  Version: 06.10.05.01

cw      Tivoli Enterprise Portal Browser Client
         li6263  Version: 06.10.05.01

hd      Warehouse Proxy
         li6243  Version: 06.10.05.01

it      TEC GUI Integration
         tpd     Version: 06.10.05.01
         tps     Version: 06.10.05.01
         tpw     Version: 06.10.05.01

jr      Tivoli Enterprise-supplied JRE
         li6243  Version: 400 Rel: 100

kf      IBM Eclipse Help Server
         li6243  Version: 06.10.05.01

lz      Monitoring Agent for Linux OS
         li6263  Version: 06.10.05.01
         tms     Version: 06.10.05.01
         tpd     Version: 06.10.05.01
         tps     Version: 06.10.05.01
         tpw     Version: 06.10.05.01

ms      Tivoli Enterprise Monitoring Server
         li6243  Version: 06.10.05.01

nt      Monitoring Agent for Windows OS
         tms     Version: 06.10.05.01
         tpd     Version: 06.10.05.01
         tps     Version: 06.10.05.01
         tpw     Version: 06.10.05.01

sh      Tivoli Enterprise Monitoring SOAP Server
         li6243  Version: 06.10.05.01

sy      Summarization and Pruning Agent
         li6243  Version: 06.10.05.01
         tms     Version: 06.10.05.01

tm      Monitoring Agent for IBM Tivoli Monitoring 5.x Endpoint
         tms     Version: 06.10.05.01
         tps     Version: 06.10.05.01

uf      Universal Agent Framework
         li6243  Version: 06.10.05.01

ui      Tivoli Enterprise Services User Interface
         li6243  Version: 06.10.05.01

ul      Monitoring Agent for UNIX Logs
         li6243  Version: 06.10.05.01
         tms     Version: 06.10.05.01
         tpd     Version: 06.10.05.01
         tps     Version: 06.10.05.01
         tpw     Version: 06.10.05.01

um      Universal Agent
         li6243  Version: 06.10.05.01
         tms     Version: 06.10.05.01
         tpd     Version: 06.10.05.01
         tps     Version: 06.10.05.01
         tpw     Version: 06.10.05.01
```

```
ux      Monitoring Agent for UNIX OS
         tms     Version: 06.10.05.01
         tpd     Version: 06.10.05.01
         tps     Version: 06.10.05.01
         tpw     Version: 06.10.05.01

    -- CINFO Menu --
 1) Show products installed in this CandleHome
 2) Show which products are currently running
 3) Show configuration settings
 4) Show installed CD release versions
 X) Exit CINFO
```

Installing the fix pack for the i5/OS monitoring agent

The procedure for installing the fix pack for the i5/OS monitoring agent differs from the other OS agents. Use the instructions in this section to install the i5/OS agent fix pack.

Note: Remember to install the application support files for the i5/OS agent on the monitoring server, portal server, and portal desktop client, as outlined in the installation checklists for those components.

Special instructions

Sign on as QSECOFR or with a profile with an equivalent special authority (SPCAUT) *ALLOBJ, *AUDIT, *IOSYSCFG, *JOBCTL, *SAVSYS, *SECADM, *SERVICE, *SPLCTL

Special notes on i5/OS monitoring agent product information:

- The OS400_Comm_FunctnChk_Workaround situation has been deleted for this fix pack because this workaround is no longer needed.
- The AuxStorPool_Percent_Used attribute name for the OS400_System_ASP_Warning situation has changed to System_ASP_Used to better indicate that this attribute provides metrics only for system ASP, and not all ASPs. Therefore, changing the situation formula from *IF *VALUE OS400_System_Status.AuxStorPool_Percent_Used *GE 90 to *IF *VALUE OS400_System_Status.System_ASP_Used *GE 90.

  After installation of the fix pack, the OS400_System_ASP_Warning situation might lose the condition formula. If this occurs, manually add the *IF *VALUE OS400_System_Status.System_ASP_Used *GE 90 condition to the situation and save the situation before starting it.
- The i5/OS monitoring agent log might display a message similar to the following if the QAUTOMON user does not have access to certain subsystem descriptions:

  ```
  Not authorized to subsystem description
  ```

  Perform the following steps if you receive the preceding message:

  1. Place the cursor on the message and press F1 to find the subsystem descriptions for which the QAUTOMON user does not have access.
  2. Use EDTOBJAUT *library/subsystem desc* to assign QAUTOMON *USE authority to the subsystem descriptions.

Special note on User Authority: If object authority to OMA objects was granted or changed, the authorities will be lost when the new fix pack is installed. The following steps will allow the authorities to be restored.

Before installing the agent fix pack:

Note that all user profiles that have been granted special authority to OMA objects. Example of finding special authority to one OMA object:

```
DSPOBJAUT OBJ(QAUTOMON/STROMA) OBJTYPE(*CMD) -
```

Repeat for other OMA objects that might have user profile authority granted.

Create a savefile for the security data to be saved. Example:

```
CRTSAVF FILE(yourlib/SECDTA)
```

Save the security data for the user profiles found. Example:

```
SAVSECDTA DEV(*SAVF) SAVF(yourlib/SECDTA)
```

After installing the agent fix pack:

Restore the saved user profiles. Example:

```
RSTUSRPRF DEV(*SAVF) USRPRF(user1 user2) SAVF(yourlib/SECDTA)
```

Use the RSTAUT command to restore authority to ALL objects that listed user profiles have had special authority granted. Example:

```
RSTAUT USRPRF(user1 user2)
```

Verify that the special authorities have been restored.

Installing the i5/OS agent fix pack checklist

Use the following steps to install the fix pack:

Table 20. Checklist for remotely deploying the fix pack to an agent

✓	Installation step
	1. Copy the agent binary a4520cma.sav to a computer with FTP access to the i5/OS agent system. That file is found in one of these locations: • **Windows CD image**: OS400\TMAITM6 directory • **UNIX or Linux CD image:** OS400/TMAITM6 directory
	2. On the i5/OS agent's system command line, create a CCCINST library, if this library does not already exist: `CRTLIB LIB(CCCINST)`
	3. Determine which version of the agent, if any, is currently installed using the **DSPSFWRSC** command. If products 0KA4430, 0KA4440, or 0KA4610 are listed then an agent is already installed. If 0KA4430, 0KA4440, or 0KA4610 is already installed, skip to Step 4. If no agent was previously installed, skip to Step 8.
	4. Enter `GO OMA` to display the Tivoli Monitoring: i5/OS Agent panel. Use option 4, Configuration, and record the CMS Server values and port numbers. Use F12 to exit without updating the existing configuration.
	5. Use **GO OMA** option 3 to end the agent and then use F3 to exit the OMA Menu. Make sure that no other users are displaying the Tivoli Monitoring: i5/OS Agent panel.

Table 20. Checklist for remotely deploying the fix pack to an agent (continued)

✓	Installation step

	6. Create a save file on the target i5/OS computer and save the existing agent if desired. Saving the current agent enables you to restore it if you later choose to remove the new version. This step is optional.
	`CRTSAVF  yourlib/PREFP03KA4`
	`SAVLICPGM LICPGM(0KA4yyy) DEV(*SAVF) SAVF(yourlib/PREFP03KA4)`
	
	where *yyy* can be 430, 440, or 610

	7. Use command **DLTLICPGM 0KA4430** if product 0KA4430 exists on the system, or use command **DLTLICPGM 0KA4440** if product 0KA4440 exits on the system. It is not required to delete product 0KA4610, although you may choose to do so using command **DLTLICPGM 0KA4610**.
	8. Create a save file on the target i5/OS for the fix pack: `CRTSAVF  CCCINST/A4520CMA  TEXT('ITM 6.1 Fix Pack 4')`

	9. FTP the agent save file to the target system. Use the following commands:
	`ftp <target computer>`
	`login <i5/OS user profile and password>`
	`bin`
	`put c:\temp\a4520cma.sav CCINST/A4520CMA.savf`
	`quit`

	10. Load the fix pack from the save file:
	a. If you are installing the product on a computer that has English upper and lower case as the primary language (language ID 2924), run the following command:
	`RSTLICPGM LICPGM(0KA4610) DEV(*SAVF) SAVF(CCCINST/A4520CMA)`
	b. If you are installing on a computer that does not have English ID 2924 as the primary language, then run the following two commands:
	`RSTLICPGM LICPGM(0KA4610) DEV(*SAVF) RSTOBJ(*PGM) SAVF(CCCINST/A4520CMA)`
	
	`RSTLICPGM LICPGM(0KA4610) DEV(*SAVF) RSTOBJ(*LNG) LNG(2924)  /`
	`SAVF(CCCINST/A4520CMA) LNGLIB(QKA4LNG)`

	11. Optionally delete the installation library, which is no longer needed: `DLTLIB CCCINST`
	12. Configure the agent and then start it. Use **GO OMA**, option 4 to configure the agent. Use the values you recorded in Step 5. Use **GO OMA**, option 2 to start the agent.

Installing the IBM Tivoli Enterprise Console event synchronization fix pack

The following sections provide information about installing the IBM Tivoli Enterprise Console event synchronization fix pack on your Tivoli Enterprise Console event server:

- "Fix pack prerequisites" on page 46
- "Notes about rule bases" on page 46

- "Important information for Windows users" on page 47
- "Installation instructions" on page 47
- "Verifying the installation of the event synchronization fix pack" on page 51
- "Uninstalling the IBM Tivoli Enterprise Console event synchronization" on page 51

Notes:

1. Before you can install this fix pack, you must have installed either the base IBM Tivoli Enterprise Console® event synchronization available with the GA level of IBM Tivoli Monitoring Version 6.1 or IBM Tivoli Monitoring and Tivoli Enterprise Console Event Synchronization Fix Pack 1, available with the GA level of IBM Tivoli Monitoring Version 6.1 FP 1 on your computer with a Tivoli Enterprise Console event server
2. To install IBM Tivoli Monitoring IBM Tivoli Enterprise Console event synchronization in a new environment, use the installer found on this CD with the naming setup<*operating_system*>.bin (.exe for Windows) and use the installation instructions provided in the "Installing the IBM Tivoli Enterprise Console event synchronization" chapter in the latest version of the *IBM Tivoli Monitoring Installation and Setup Guide*.
3. The setup files contained in the Fix Pack 005 media (setupAix.bin, setupWin32.exe, setupSolaris.bin, setupLinux.bin, setupLinux390.bin, setupHP11.bin) should be used for new installs only. If they are running on a system where Event Synchronization is already installed, the installer will detect a previous installation and will not continue.
4. If you have Tivoli Enterprise Console event synchronization installed on your computer already, first determine which version is installed (see Table 21 for assistance). If the version installed is 1.0.0.3 (Fix Pack 003), you are at the current level. There is no update for the Tivoli Enterprise Console event synchronization in Fix Pack 005. If the version installed is earlier than version 1.0.0.3, download the 6.1.0-TIV-ITM_TEC-FP0003.tar file (or 6.1.0-TIV-ITM_TEC-FP0003.zip for Windows) and extract the contents to a temporary location on your event server.
5. Before installing the fix pack on RedHat Enterprise Linux 4 on AMD64/EM64T, RedHat Enterprise Linux 4 on System p™, or SUSE Linux Enterprise Server 9 on AMD64/EM64T computers, ensure that you have installed the required libraries. See the footnotes in Table 4 on page 5 for details.
6. When fix pack installation on all components is complete, you must recycle the TEC server (installer will ask if you want to restart the TEC server or you can manually restart the TEC server) for the modification to run. To determine if this is required, review the vpd.properties file to verify the installed versions of all components.

Determining what level of event synchronization is installed

To verify what level of TEC event synchronization is installed on your computer, perform one of the following platform-specific actions shown in Table 21.

Table 21. Determining the level of TEC event synchronization installed by platform

Platform	Action
Windows	1. Open or list the vpd.properties file, located in the <*Operating_System_Drive*>\<*OS_Name*> directory (for example, C:\windows or c:\winnt). 2. Verify that the value associated with the `TecEvntSyncInstaller` string is `|1|0|3|0|1.0.0.3`, which indicates that Fix Pack 3 has been applied.

Table 21. Determining the level of TEC event synchronization installed by platform (continued)

Platform	Action
HP11	Run the following command from a user ID with root or administrator privileges: `swlist -v TecEvntSyncInstaller` Verify that the value associated with the `ismp_key` parameter has a value of `1.0.0.3`, which indicates that Fix Pack 3 has been applied.
AIX	1. Change directories to `/usr/lib/objrepos`. 2. Open or list the vpd.properties file. 3. Verify that the value associated with the `TecEvntSyncInstaller` string is `|1|0|3|0|1.0.0.3`, which indicates that Fix Pack 3 has been applied
Linux (SLES and Redhat)	1. Open or list the vpd.properties file is in the / or /root directory. 2. Verify that the value associated with the `TecEvntSyncInstaller` string is `|1|0|3|0|1.0.0.3`, which indicates that Fix Pack 3 has been applied.
Solaris	Run the following command from a user ID with root or administrator privileges: `pkginfo -l ISitmTecE` Verify that the displayed values for the parameter `Version` include a value of `1.0.3.0.DSP=1.0.0.3`, which indicates that Fix Pack 3 is applied.

Fix pack prerequisites

Before you can install this fix pack, you must have installed either the base event synchronization available with the GA level of IBM Tivoli Monitoring or IBM Tivoli Monitoring & Tivoli Enterprise Console Event Synchronization Fix Pack 1 on your event server.

Notes about rule bases

With this fix pack, the installation wizard provides the capability to back up the targeted rule base.

If you have multiple rule bases that are using IBM Tivoli Monitoring and Tivoli Enterprise Console Event Synchronization, you can run the fix pack installation to update each rule base. After you finish the first rule base, restart the fix pack installer and supply the targeted next rule base you want to update.

The rule bases targeted by the installer are upgraded and recompiled.

If the targeted rule base is the currently active rule base, it is reloaded. You must stop and restart the Tivoli Enterprise Console Server to make the reloaded version of the rule base the current rule base.

If the targeted rule base is not the currently active rule base, it is NOT reloaded. You must load the targeted rule base and then stop and restart the Tivoli Enterprise Console Server to make the targeted rule base current.

Note: Before you use any of the commands, you must source the Tivoli environment:

- For Windows environments, issue this command:
  `<Windows_system_directory>\system32\drivers\etc\Tivoli\setup_env.cmd`

  where *Windows_system_directory* can be c"\windows or c:\winnt.

- For UNIX or Linux environments, issue this command:

  ```
  . /etc/Tivoli/setup_env.sh
  ```

Use the **wrb -lscurrb** command from a bash command prompt (on Windows systems) or command prompt (on UNIX systems) to determine the current rule base.

Use the **wrb -loadrb <***rule base name***>** command from a bash command prompt (on Windows systems) or command prompt (on UNIX systems) to load a new rule base.

Use the **wstopesvr** command from a bash command prompt (on Windows systems) or command prompt (on UNIX systems) to stop the Tivoli Enterprise Console Server.

Use the **wstartesvr** command from a bash command prompt (on Windows systems) or command prompt (on UNIX systems) to start the Tivoli Enterprise Console Server.

Any user modifications to the targeted rule base's original omegamon.rls file must be manually migrated to the updated rule base's omegamon.rls file. Then the rule base must be compiled and loaded. After the rule base is loaded the Tivoli Enterprise Console Server must be stopped and restarted.

Note that this fix pack creates a backup copy of the original omegamon.rls file that is named omegamon.rls.bac in the <*rulebase_directory*>/TEC_RULES directory.

Important information for Windows users

For a Windows event server, any existing rule base that was created with a relative (not absolute) path cannot be found unless you move the fix pack installer to the drive where the rule base exists. To verify that your existing rule base uses an absolute path, run the following command from a bash environment on your server:

```
wrb -lsrb -path
```

If the returned path includes text similar to hostname:\<*rulebase_directory*>, with no drive letter (such as C:\), you must copy the fix pack executable (setupwin32fp3.exe) file from the download directory to the drive where the rule base exists and run the fix pack installation from that location.

Installation instructions

There are three options for installing the event synchronization fix pack:

- "Installing from a wizard" on page 48
- "Installing from the command line" on page 48
- "Installing from the command line using a silent installation" on page 50

Note: If you have IBM Tivoli Monitoring IBM Tivoli Enterprise Console event synchronization installed on your computer already, first determine which version is installed (see Table 21 on page 45 for assistance). If the version installed is 1.0.0.3 (Fix Pack 003), you are at the current level. There is no update for the IBM Tivoli Monitoring IBM Tivoli Enterprise Console event synchronization in Fix Pack 005. If the version installed is earlier than version 1.0.0.3, download the 6.1.0-TIV-ITM_TEC-FP0003.tar file (or

6.1.0-TIV-ITM_TEC-FP0003.zip for Windows) and extract the contents to a temporary location on your event server.

Before you start the installation, download the 6.1.0-TIV-ITM_TEC-FP0003.tar file and extract the contents to a temporary location on your event server.

Installing from a wizard

Use the following steps to install event synchronization from the installation wizard:

1. On the event server, launch the event synchronization installation:

   On Windows computers, double-click the setupwin32fp3.bin file in the temporary directory where you extracted the fix pack files.

   On Linux or UNIX computers, run the following command:

   ```
   setup<operating_system>fp3.bin
   ```

   where <*operating_system*> is the operating system you are installing on. For example, run the following command on an AIX computer:

   ```
   setupAixfp3.bin
   ```

2. Click **Next** on the Welcome window.
3. Select **I accept the terms in the license agreement** and click **Next**.
4. Complete the following fields and click **Next**:

Table 22. IBM Tivoli Enterprise Console event synchronization configuration fields

Field	Description
Rule base name	The name of the rule base to be updated with the fix pack information.
Backup rule base name	If you want the installation wizard to back up your rule base, provide a name for the back up version.
Backup rule base path	Type a path for the backup version of the rule base.

5. Click **Next**.
6. Click **Next** on the pre-installation summary panel.

   The installation begins.
7. When the installation and configuration steps are finished, you are given the option to automatically stop and restart the event server. If you want to have the wizard stop and restart your event server, select this option and click **OK**. Otherwise, click **OK** (you will have to manually stop and restart your event server).
8. Click **Finish** on the Summary Information window.

   Note: If any configuration errors occurred during installation and configuration, you are directed to a log file that contains additional troubleshooting information.

Installing from the command line

Use the following steps to install the event synchronization from the command line on your event server:

1. Run the following command to launch the installation:

   On Windows computers:

   ```
   setupwin32fp3.bin -console
   ```

On UNIX computers:

```
setup<operating_system>fp3.bin -console
```

where <*operating_system*> is the operating system you are installing on. For example, run the following command on an AIX computer:

```
setupAixfp3.bin -console
```

The following prompt is displayed:

```
Press 1 for Next, 3 to Cancel or 4 to Redisplay [1]
```

2. Type 1 to start the installation and press Enter.

   The following prompt is displayed:

   ```
   Software Licensing Agreement:
   Press Enter to display the license agreement on your screen. Please
   read the agreement carefully before installing the Program. After
   reading the agreement, you will be given the opportunity to accept it
   or decline it. If you choose to decline the agreement, installation
   will not be completed and you will not be able to use the Program.
   ```

3. Press Enter to display the software license agreement.
4. Type 1 and press Enter to accept the license.

   The following prompt is displayed:

   ```
   Press 1 for Next, 2 for Previous, 3 to Cancel, or 4 to Redisplay [1]
   ```

5. Type 1 and press Enter to continue.

   The following prompt is displayed:

   ```
   Rule base Name []
   ```

6. Type the name for the rule base and press Enter.

   The following prompt is displayed:

   ```
   If you want the installer to back up the rule base indicated above before
   modifying the rule base, please provide a backup rule base name.

   Backup rule base name []
   ```

7. Type the backup rule base name, if you want to use one, and press Enter. If you do not want to create a backup rule base, leave this option blank and press Enter.

   The following prompt is displayed:

   ```
   If you have provided a backup rule base name you must provide a backup rule
   base path. NOTE: We append the backup rule base name to the backup rule base
   path for clarity and easy look-up.

   Backup rule base path []
   ```

8. Type the path for the backup rule base and press Enter.

   Note: If you are creating a backup rule base, you *must* provide this path. If you are not creating a backup rule base, leave this option blank and press Enter.

   The following prompt is displayed:

   ```
   Press 1 for Next, 2 for Previous, 3 to Cancel, or 4 to Redisplay [1]
   ```

9. Type 1 and press Enter to continue.

   The following prompt is displayed:

   ```
   IBM Tivoli Monitoring
   Press 1 for Next, 2 for Previous, 3 to Cancel, or 4 to Redisplay [1]
   ```

10. Type 1 and press Enter to continue. The event synchronization is installed.

    The following prompt is displayed:

```
Installation and Configuration has completed.
Please stop and restart the Tivoli Enterprise Console Server.

Press 1 for Next, 2 for Previous, 3 to Cancel, or 4 to Redisplay [1]
```

11. Type 1 and press Enter to continue.

    The following prompt is displayed:

```
Installation and configuration has completed.
Please restart the Tivoli Enterprise Console server for the changes to take
effect.
Mark appropriately below to restart the Tivoli Enterprise Console server.
[ ] 1 - Restart the Tivoli Enterprise Console server to make changes effective

To select an item enter its number, or 0 when you are finished: [0]
```

12. Type 0 and press Enter to continue.

    The following prompt is displayed:

```
Press 3 to Finish, or 4 to Redisplay [1]
```

13. Type 3 to finish and press Enter.

You must stop and restart the event server for these changes to take effect.

Installing from the command line using a silent installation

Use the following steps to install the event synchronization using a silent installation from the command line on your event server. This installation method runs silently, so you will not see status messages during the actual installation.

1. Run the following command to generate the configuration file:

   On Windows computers:

```
setupwin32fp3.bin -options-template filename
```

   where *filename* is the name of the configuration file to create, for example, es_silentinstall.conf.

   On UNIX computers:

```
setup<operating_system>fp3.bin -options-template filename
```

   where <*operating_system*> is the operating system you are installing on. For example, run the following command on an AIX computer:

```
setupAixfp3.bin -options-template filename
```

2. Edit the output file to specify the **rulebasePanel.rbName** variable. Define the name of a rule base that has Tivoli Enterprise Console Event Synchronization installed. This is the rule base that will be updated.

   Notes:

   a. If you do not specify a rule base name, the installation will fail.
   b. Remove the pound signs (###) from the beginning of any value that you want to specify.
   c. Do not enclose any values in quotation marks (").
   d. If you do not specify any of the other values, the default values are used.
   e. If you specify values, ensure that the value you specify meets the minimum required values. Otherwise, the installation stops and an error is written to the log file.

3. Save the file.
4. Run the following command:

   On Windows computers:

```
setupwin32fp3.bin -options filename -silent
```

where *filename* is the name of your configuration file.

On UNIX computers:

```
setup<operating_system>fp3.bin -options filename -silent
```

where <*operating_system*> is the operating system you are installing on. For example, on AIX, run the following command:

```
setupAixfp3.bin -options filename -silent
```

You must stop and restart the event server for these changes to take effect. (Stopping and restarting the event server can be done by the silent installation wizard by marking the appropriate field).

When installation is complete, the results are written to the itm_tec_event_sync_install.log file. On UNIX computers, this log file is always created in the /tmp directory. For Windows computers, this file is creates 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%
```

Verifying the installation of the event synchronization fix pack

To verify that the IBM Tivoli Monitoring and Tivoli Enterprise Console Event Synchronization fix pack has been successfully installed, do one of the following, depending on the operating system of the computer where your event server is running.

- **HP-UX:** Run the following command:

  ```
  swlist -v TecEvntSyncInstaller
  ```

  Verify that the displayed values for the parameter ismp_key has a value of 1.0.0.3, which indicates that Fix Pack 004 is applied.
- **Windows:** Review the vpd.properties file, located in the C:/Windows or C:/Winnt subdirectory. Locate the TecEvntSyncInstaller string and review the text for the |1|0|3|0|1.0.0.3 string, which indicates that the fix pack is applied.
- **AIX:** Review the vpd.properties file, located in the /usr/lib/objrepos directory. Locate the TecEvntSyncInstaller string and review the text for the |1|0|3|0|1.0.0.3 string, which indicates that the fix pack is applied.
- **Linux:** Review the vpd.properties file, located in the / or /root directory. Verify that the TecEvntSyncInstaller string reflects the string |1|0|3|0|1.0.0.3, which indicates that Fix Pack 004 is applied.
- **Solaris:** Run the following command:

  ```
  pkginfo -l ISitmTecE
  ```

  Verify that the displayed values for the parameter Version include a value of 1.0.3.0.DSP=1.0.0.3, which indicates that Fix Pack 004 is applied.

Uninstalling the IBM Tivoli Enterprise Console event synchronization

Use the following steps to uninstall the event synchronization from your event server:

Notes:

1. You cannot uninstall just the event synchronization fix pack . If you use these steps, you will uninstall the entire event synchronization package from your event server.
2. Before you use any of the commands, you must source the Tivoli environment:
   - For Windows environments, issue this command:

     `<Windows_system_directory>\system32\drivers\etc\Tivoli\setup_env.cmd`

     where *Windows_system_directory* can be c"\windows or c:\winnt.
   - For UNIX or Linux environments, issue this command:

     `. /etc/Tivoli/setup_env.sh`

1. Run the following uninstallation program:
   - On Windows computers: *%BINDIR%*\TME\TEC\OM_TEC_uninst\uninstaller.exe
   - On UNIX computers: *$BINDIR*/TME/TEC/OM_TEC/_uninst/uninstaller.bin
2. Follow the prompts in the uninstallation program.

You can also run this uninstallation program in silent mode (by running the program from the command line with the **-silent** parameter) or in console mode (by using the **-console** parameter).

You must stop and restart the event server for these changes to take effect. (Stopping and restarting the event server can be done by the uninstallation wizard by marking the appropriate field).

If your event server is running on an HP-UX computer, ensure that the $BINDIR/TME/TEC/OM_TEC/_uninst and $BINDIR/TME/TEC/OM_TEC/_jvm directories are successfully removed by the uninstallation program. If they are not, manually delete these directories.

Note: InstallShield can create a second _uninst directory called _uninst2 (InstallShield can also continue this out to _uninstX - where X is 2, 3, 4, 5, ...). This second directory is created when InstallShield finds an existing _uninst directory and another process has access to it. If this occurs on your computer when uninstalling, you must use the uninstaller found in the latest directory. Using the uninstaller in the most recently created directory will correctly uninstall the product.

Chapter 4. After you install

This section contains information for you to consider or use when you have finished installing the fix pack.

Clearing the Tivoli Enterprise Portal browser cache

On systems running the Tivoli Enterprise Portal browser client, clear the browser cache to avoid exception messages.

1. From the Windows **Start** button, select **Control Panel**.
2. Double-click the **Java Plug-in** icon to display the Java Plug-In Control Panel.
3. Select the **Cache** tab.
4. Click the **Clear** button and click **Apply**.
5. Close the Java Plug-In Control Panel.

Determining what components were installed

IBM Tivoli Monitoring automatically installs components that have been upgraded in the current fix pack. When installation is complete, you can use the `cinfo` command (Linux or UNIX) or `kinclnfo` command (Windows) to determine which components have been installed. When you run these command, you might discover that support files that you did not select were also installed and that these support files are not available for uninstallation. This situation happens when the component that you upgraded requires that support files in other components be upgraded as well, even though you did not select them. This behavior ensures that components stay in synch, and is not a cause for alarm.

When you upgrade the Tivoli Enterprise Portal on Windows, the installer program might detect and place check marks by the previously installed features incorrectly. Some of the installed features are not checked, and other features that were not installed are checked. Ensure that the list of installed components matches what was previously installed.

Installing Global Services Kit (GSKit) if you use silent installation

When you install or upgrade the fix pack using a silent installation, the prompt for the root password is bypassed, and the GSKit is therefore not installed or upgraded. You must be install or upgrade GSKit manually after the silent installation has completed from a user ID with root or administrator authority.

You must install the GSKit from a user ID with root or administrator authority.

Securing your Linux or UNIX IBM Tivoli Monitoring installation

For installations on the Linux or UNIX environment, do the following.

Important: Be sure to run the secureMain utility on any installation, especially those installations that include the UNIX OS Agent, to prevent privilege escalation.

© Copyright IBM Corp. 2007

If you install or upgrade IBM Tivoli Monitoring on a Linux or UNIX computer, the file permissions for many files and directories are set to a very low level, 777. Use the secureMain utility to change these permissions.

Note: You do not need to be logged in as a root user to run this utility, but you are prompted for the root password when it is required.

The secureMain utility has the following syntax:

```
secureMain [-h install_dir] lock|unlock
```

where:

-h *install_dir*
The directory path for the IBM Tivoli Monitoring installation. If this parameter is not supplied, then the script attempts to determine the installation directory.

lock Tightens the directory tree permissions. The permissions are set to 750.

If certain products or components that require access by multiple user IDs are installed, a basic permission model of 755 is used. Some specific files and directories remain at 777 permissions.

unlock
Loosens the directory tree permissions.

Note that the **unlock** parameter does not restore permissions to exactly what they were before **secureMain lock** was run. The unlock parameter sets most files and directories back to 777 permissions but not all files and directories. Permissions on the common directories shared by applications, and on the server components (monitoring server, portal server, and portal client) are set to 777. Permissions on most application specific directories are not reset.

Installing the upgrade toolkit on Solaris computers

IBM Tivoli Monitoring, Version 6.1 provides an upgrade toolkit to facilitate your move from a Tivoli Distributed Monitoring environment to the IBM Tivoli Monitoring environment. For Fix Pack 005, the upgrade toolkit upgrades to the Fix Pack 005 version of the agents.

For Fix Pack 005, you must use the following command to install support for Solaris computers:

```
wpatch -c /cdrom -i OPMT_SOL manage_node -y
```

See *IBM Tivoli Monitoring: Upgrading from Tivoli Distributed Monitoring* for additional information on using the **wpatch** command to install the upgrade toolkit.

Installing Java Web Start

The Java Web Start application lets you launch the Tivoli Enterprise Portal desktop client application without having to explicitly install the IBM Tivoli Monitoring version 6.1 installer on each system where you want to run the desktop client. After installing Java Web Start, you no longer have to manually update each Tivoli Enterprise Portal desktop client installation when you install additional support or products to the Tivoli Enterprise Portal Server because each Java Web Start client automatically downloads any new jar files and resources. The files to enable this

application include a text file, a utility jar file, template JNLP file, and a digitally signed version of jsafe.zip (required if you are integrated with Tivoli Enterprise Console) and can be downloaded from the OPAL Web site: http://www-18.lotus.com/wps/portal/topal.

Installing upgrades to monitoring agents

In an effort to improve quality within the OMEGAMON portfolio, IBM has provided additional focus on verification of OMEGAMON XE products and components running with IBM Tivoli Monitoring version 6.1 Fix Pack 005. Refer to the Planning Upgrades section of the following Web site for OMEGAMON XE maintenance levels **http://www-306.ibm.com/software/sysmgmt/products/support/IBMTivoliMonitoringV6.html**.

A staged upgrade is supported but minimally, the hub Tivoli Enterprise Monitoring Server, the Tivoli Enterprise Portal Server associated with the hub, and all of the Tivoli Enterprise Portal desktop clients that connect to that Tivoli Enterprise Portal Server must be upgraded to the same fix pack level. Remote Tivoli Enterprise Monitoring Servers and OMEGAMON XE monitoring agents can be upgraded during subsequent maintenance windows.

If you are upgrading one or more OMEGAMON XE Version 3.1 monitoring agents to OMEGAMON XE 4.1, refer to the *IBM Tivoli Monitoring: Upgrade Road Map for OMEGAMON XE V4.1 Monitoring Agents* (GC32-1980-01). The upgrade roadmap can be downloaded from http://www-1.ibm.com/support/docview.wss?rs=650&context=SSTFXA&dc=DA400&uid=pub1gc32198001&loc=en_US&cs=UTF-8&lang=en&rss=ct650tivoli.

Understanding deployment options

For additional information about deployment issues, refer to the *IBM Tivoli Monitoring V6.1 Deployment Guide* found at this Web site: http://www.ibm.com/software/tivoli/opal/?NavCode=1TW10TM4J.

Exploiting new configuration options for z/OS components

New configuration options were available in Fix Pack 004 for z/OS components, including a network interface list and Take-Action command authorization and execution through IBM Tivoli NetView® on z/OS. For more information about these functions see http://www-1.ibm.com/support/docview.wss?rs=0&q1=netview+command+authorization+situations&uid=swg27009342&loc=en_US&cs=utf-8&cc=us&lang=en.

Chapter 5. Known problems and limitations

The following sections identify problems that might occur during the use of this fix pack. Where available, workaround solutions are provided for the problems. These types of workarounds are found in this chapter:

- "General installation component issues"
- "Remote deployment issues" on page 58
- "Tivoli Enterprise Monitoring Agents" on page 60
- "Tivoli Enterprise Monitoring Server" on page 60, both on distributed platforms and z/OS
- "Tivoli Enterprise Portal desktop and browser clients" on page 66
- "Tivoli Enterprise Portal Server" on page 67
- "Historical data collection issues" on page 72, including issues affecting the summarization and pruning agent and the warehouse proxy
- "Universal agent issues" on page 74
- "Globalization" on page 75
- "Online help" on page 76

General installation component issues

These known problems and limitations are related to the installation component.

- If you upgrade Java, the installation program performs the upgrades and then ends without displaying any confirmation message. You must restart the component on which you installed the Java upgrade for the upgrade to take effect.
- Do not install and run IBM Tivoli Monitoring version 6.1 components (for example, the Tivoli Enterprise Monitoring Server or monitoring agents) using the same names as other IBM Tivoli Monitoring components. This caution applies to releases IBM Tivoli Monitoring version 350/360 and version 6.1 both to the Tivoli Enterprise Monitoring Server and monitoring agent components.

  Specifically, if agents are created in one environment with the same name as agents created in a different environment, problems are likely to occur, especially if those environments come together at some point, such as when IBM Tivoli Monitoring Version 6.1 production components and IBM Tivoli Monitoring non-production components are installed and running on the same computers.

  For example, all test components installed on computers designated for test must be installed with different names from the names given to production components. Problems can occur if both a test and production version of the same agent were running on the same computer.

  Or in this example, if the test agent is reconfigured to point to a production Tivoli Enterprise Monitoring Server while the production agent was also running, problems with the monitoring server might occur. For example, a UNIX server named host01 is running a test agent named host01:KUX and a production agent also named host01:KUX. Each agent is configured to connect to its test or production Tivoli Enterprise Monitoring Server, RTEMS_TEST01 and RTEMS_PROD01 respectively. Test agent host01:KUX is mistakenly reconfigured to connect to a production Tivoli Enterprise Monitoring Server named RTEMS_PROD02 while the production agent host01:KUX is still running. This results in a situation where Tivoli Enterprise Monitoring Server issues can occur

© Copyright IBM Corp. 2007

because there is more than one agent with the same name, each reporting through a different production monitoring server.

The types of Tivoli Enterprise Monitoring Server and Tivoli Enterprise Portal Server problems that can occur include the following:

- Corruption of the hub Tivoli Enterprise Monitoring Server nodelist or nodestatus table.
- Looping in the Hub Tivoli Enterprise Monitoring Server, consuming CPU processing time.
- Tivoli Enterprise Portal Server failures during nodelist or nodestatus processing.

These issues are not easily detected and prevented by the IBM Tivoli Monitoring Version 350/360 and Version 6.1 products. Refer to Technote 1253875 at http://www-1.ibm.com/support/docview.wss?uid=swg21253875 for more information.

- Names for monitoring servers must be between 2 and 32 characters in length. For more information about naming conventions, refer to the *IBM Tivoli Monitoring: Installation and Setup Guide*.
- You must install the GSKit from a user ID with root or administrator authority. If you are running the installer program interactively as non-root, the installer will prompt you for the root password. When you install using a silent installation, the prompt for the root password is bypassed, and GSKit must be installed manually when after the silent installation has completed from a user ID with root or administrator authority.
- If you are performing a silent installation of application support on a zLinux system and you specify `ComponentSelectionPanel.tepdSelected="true"` in the response.txt file without having the desktop client installed, the install program exits with an error that indicates the entire operation failed when actually only the desktop client portion failed.

  To recover from this situation, rerun the silent installation and specify `ComponentSelectionPanel.tepdSelected="false"`.
- Fix pack installation fails on AIX V5.3 computers at maintenance level 8.0.0.3.

  Update the AIX xlC.aix50.rte component to 8.0.0.4. See the following Web site for installation instructions: http://www-1.ibm.com/support/docview.wss?uid=swg1IY84212

Remote deployment issues

These known problems and limitations are related to remote deployment.

- The **tacmd createNode** command might time out and generate the following Java exception in the trace_cn.log file:

```
<Exception><![CDATA[java.lang.StringIndexOutOfBoundsException: String index out
     of range: 1
     at java.lang.String.charAt(String.java(Compiled Code))
     at com.ibm.tivoli.remoteaccess.UNIXProtocol.getPerms(Unknown Source)
     at com.ibm.tivoli.remoteaccess.UNIXProtocol.putFile(Unknown Source)
     at com.ibm.tivoli.itm.install.remote.CreateNodeImage.distributeFiles
          (CreateNodeImage.java:2615)
     at com.ibm.tivoli.itm.install.remote.CreateNodeImage.install
          (CreateNodeImage.java:831)
     at com.ibm.tivoli.itm.install.remote.CreateNodeClient.main
          (CreateNodeClient.java:1607)
]]>
```

This is a StringIndexOutOfBounds exception, which is caused by a lack of memory available. The solution is to free system memory and try again.

- The following problems occur for 32-bit Windows computers:
  - Missing entry in Add and Remove Programs after you run the UpgradeAgent or CreateNode commands with the target system as either a Windows 2003 based Server or Windows 2000 Terminal Server.
  - Missing entry in Add and Remove Programs after deploying or upgrading the Windows monitoring agent.
  - The Windows monitoring agent is removed after removing another agent from your computer. Additionally, all directories are cleared and registry entries are deleted.

  Perform one of the following to add the Universal Agent to the target computer to create the Add and Remove Programs entry:
  - Deploy a Universal Agent on the target computer.
  - Physically take the installation CD to the remote computer and install the Universal Agent on the target computer.

  For the remote computer, you can choose to remove the Universal Agent after you have installed it to create the Add and Remove Programs entry.

  If an entry in Add and Remove Programs does not exist and other monitoring agents are deployed to the target computer and then removed, the Windows monitoring agent can disappear after a second agent is removed from the remote computer.
- For 64-bit Windows computers, the installation stops indicating that there are missing .cab files.

  Locally install all of your monitoring agents. Due to a current restriction on 64-bit Windows computers, remote deployment cannot be used to update monitoring agents that are installed from a single CD. For example, the Universal Agent and the Windows agent both reside on the same CD and there are four agents on the Database CD. In order to upgrade any agent on these CDs, you must do one of the following:
  - Physically take the CD to a remote computer and install it.
  - Copy the CD to the remote computer and install it.
  - Use a network drive that the remote computer can access for the installation.

  Uninstall the previous version of the agent before installing the new version. You must upgrade all of the agents on the CD at the same time from the local installation. If you need to install an agent from the CD at a later time, you must install the agent from the exact same location as you used for the original installation. Consider using a local copy of the CD or a network copy from the target computer and that it remain until all agents from that CD are removed. If you use a network copy, the mapped drive must remain at the same location for all installation of components from the mapped CD image.
- When attempting to install an application agent using Add Managed System from the Tivoli Enterprise Portal to a Windows OS computer, you might receive the following error message:

  ```
  The managed system configuration failed for the following reason:
  KFWITM290E An unexpected error occurred.  The current task was cancelled.
  ```

  Perform the following procedure to verify that the application agent installation was successful:

  1. Click **OK** on the error message window.
  2. Select the **Navigator update pending** button if it appears at the bottom of the Tivoli Enterprise Portal navigator.

3. Verify that the new agent entry appears within the Tivoli Enterprise Portal navigator.
4. Select the agent and browse through its workspaces to determine if it is communicating successfully and reporting data.

If the application agent was successfully installed, you can ignore the error message.

If the application agent was not successfully installed, use the `tacmd addSystem` command to install the agent.

Tivoli Enterprise Monitoring Agents

These known problems and limitations are related to Tivoli Enterprise Monitoring Agents.

- For all OMEGAMON XE agents on z/OS that support sysplex-level tables, you are encouraged to specify history collection for all managed system in a sysplex, but collection actually takes place only on the current sysplex proxy-managed system. UADVISORS distributed to other systems will have no data to write (unless they become the sysplex proxy). The sysplex proxy functionality will move to another eligible Tivoli Enterprise Monitoring Server in this sysplex if the current sysplex proxy monitoring server is stopped or fails.

  Therefore, distribute the sysplex-level tables to all eligible managed systems, but only the current sysplex proxy system will record data.

Tivoli Enterprise Monitoring Server

These known problems and limitations are related to Tivoli Enterprise Monitoring Servers, both on distributed platforms and on z/OS systems.

Tivoli Enterprise Monitoring Server on distributed platforms issues

- If you hand modify any values (change them without using the GUI or command line) in any *.config file (for example, HOSTNAME_ms_TEMSNAME.config or KBBENV) for any component, you will likely lose those values when the component is reconfigured.
- The monitoring server can use a large number of file descriptors, especially in a large environment. On UNIX and Linux systems, the maximum number of file descriptors available to a process is controlled by user limit parameters. To display the user limits, run the following command:

  ```
  ulimit -a
  ```

  The `nofiles` parameter is the number of file descriptors available to a process. For the monitoring server process (kdsmain), the `nofiles` parameter should be set larger than the maximum number of agents that will be connecting to the monitoring server. If the monitoring server is unable to get file descriptors when needed, unexpected behavior can occur, including program failures. Consider increasing the value to 1000 file descriptors or more.

  There are other user limit parameters that control how much data, stack, and memory are available to a process. For large environments, consider increasing these memory-related user limit parameters for the monitoring server (kdsmain) process.

Configuring the user limit parameters usually requires root access, and involves changing system startup files which are operating system specific. Consult the operating system manuals for information on how to configure the user limit parameters.

- When you install Fix Pack 5 on the Tivoli Enterprise Monitoring Server on Windows, the installation can hang and the Manage Tivoli Monitoring Services status windows indicates that that the monitoring server is in the ″Start Pending″ state. If you check the ITM_HOME\CNP\logs\kcjerror.log and kcjras1.log files, you will find this error:

```
+45FFF5A0.0027
+45FFF5A0.0027 ************
+45FFF5A0.0027 ************ WARNING: UNABLE TO MAKE AN INTRA-PROCESS TCP
+45FFF5A0.0027 ************          CONNECTION USING THE LOOPBACK INTFC
+45FFF5A0.0027 ************          IF YOU ARE RUNNING FIREWALL SOFTWARE
+45FFF5A0.0027 ************          IT MAY REQUIRE A CONFIGURATION CHANGE
+45FFF5A0.0027 ************
+45FFF5A0.0027
+45FFF5A0.0027
+45FFF5A0.0027
```

  The IBM Tivoli Monitoring installation program processes bind-and-connect, intra-process TCP sessions using ephemeral ports on the loopback interface. This interface does not function correctly if firewall or anti-virus software prevents such activities.

  To correct this problem modify your firewall or anti-virus software to permit the use of ephemeral ports for loopback operations.

- Changes made in Fix Pack 003 for the Tivoli Enterprise Monitoring Server component caused problems for some users such that situations were not being started at the remote agents connected to a remote monitoring server. Fixes are available for the monitoring server on z/OS and on distributed platforms.
  - **On z/OS**: OA18854 has been created to PE PTF UA28536. The fix for this is to rebuild the Object Access List file at the remote monitoring server. To do this the client can delete: &rvhilev.RKDSDOBJ file, then open the Configuration Tool, and rebuild the RTE where the monitoring server is defined and submit this JCL. This job will rebuild only files that are not allocated.
  - **On Distributed Platforms:** To support this fix in the distributed environment, do the following.

    On Windows:

    1. Stop all remote monitoring servers.
    2. In the <*IBMhome_dir*>\cms directory, locate the following two files: QA1DOBJA.DB and QA1DOBJA.IDX.
    3. Back up these files.
    4. Copy the refreshed version of these files (QA1DOBJA.DB.WINDOWS and QA1DOBJA.IDX.WINDOWS, available from http://www-1.ibm.com/support/docview.wss?uid=swg21250181) into the <*IBMhome_dir*>\cms directory.
    5. Rename the file QA1DOBJA.DB.WINDOWS to QA1DOBJA.DB.
    6. Rename the file QA1DOBJA.IDX.WINDOWS to QA1DOBJA.IDX.
    7. Restart the remote monitoring servers.

    On UNIX or Linux:

    1. Stop all remote monitoring servers.
    2. In the <*IBMhome_dir*>\tables\<*hub_name*> directory locate the following two files: QA1DOBJA.DB and QA1DOBJA.IDX.

3. Back up these files.
4. Copy the refreshed version of these files (QA1DOBJA.DB.UNIX and QA1DOBJA.IDX.UNIX, available from http://www-1.ibm.com/support/docview.wss?uid=swg21250181 has been created to address it.) into the *<IBMhome_dir>*\tables*<hub_name>* directory.
5. Rename the file QA1DOBJA.DB.UNIX to QA1DOBJA.DB.
6. Rename the file QA1DOBJA.IDX.UNIX to QA1DOBJA.IDX.
7. Restart the remote monitoring server.

For more information, see Technote 1250181 at http://www-1.ibm.com/support/docview.wss?uid=swg21250181 .

- Some products might have two .sql files when using Manage Tivoli Enterprise Monitoring Services to add application support to a Tivoli Enterprise Monitoring Server on a different computer.
  - Use k*pc*.sql, where *pc* is the two-character product code, if this is the first time that you are adding application support to that product.
  - Use k*pc*_upg.sql, where *pc* is the two-character product code, if you are upgrading a product where you previously added application support.

  The k*pc*.sql can contain delete statements that remove user customizations; therefore, you do not want to use it you have previously added application support and want to keep that configuration.
- In some instances where the hub Tivoli Enterprise Monitoring Server running on Linux on zSeries with Fix Pack 005, startup messages indicate that the monitoring server has timed out before it was able to start. However, the message may be generated in error. The monitoring server may have indeed started correctly with every service initialized. The message is misleading. Check the status of the monitoring server and if it is has started, ignore the error message.
- Be aware that the names used to configure the IP.UDP protocol on the Tivoli Enterprise Monitoring Server across platforms are inconsistent. On Linux or UNIX, IP.UDP is referred to as IP. In Windows and z/OS, it is named IP.UDP. However, IP.UDP and IP are the same protocol.

Tivoli Enterprise Monitoring Server on z/OS issues

- 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.

  To address this issue, 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), increase the value of the MINUMUM parameter and restart the address space. Refer to Technote 1257489 at http://www-1.ibm.com/support/docview.wss?uid=swg21257489 for more information.

- In some instances, when the hub Tivoli Enterprise Monitoring Server on z/OS is shut down with the typical /p command while agents and remote monitoring servers are still connected, the ITMS: Engine component abends with this message:

  ```
  ABEND S0C4 U0000 AT 91D8694C (KDSMAIN.VDM1SCP+270)
  ```

  To recover from this error, restart the hub monitoring server.
- In some instances, a remote Tivoli Enterprise Monitoring Server on z/OS is slow to acknowledge that it has been shut down (using either the /p or the /c command), even though monitoring agents running on the remote monitoring server acknowledge the shut down immediately.

  Before assuming that the shutdown of a remote monitoring server on z/OS failed, check the status again after 15 minutes.
- In an environment with multiple monitoring agents on z/OS running, the Tivoli Enterprise Monitoring Server on z/OS can fail to terminate after a /p shutdown command has been issued. The RKLVLOG may indicate ongoing activity, but the monitoring agent started tasks does not end in a reasonable amount of time.
- When creating the jobs for batch mode installation the Runtime Environment <*myruntime*> (RTE <*myruntime*>), the following warning message is displayed:

  ```
  WRN: KD5310CB D2 VERSION ERROR
  KD5310CB - You have selected to configure
  OMEGAMON XE for DB2 on z/OS V310 in this RTE=<myruntime>.
  The OMEGAMON XE for DB2 (D2) product version
  configured in this RTE is D2600.
  OMEGAMON XE for DB2 on z/OS V310 requires V310 or
  higher.  Please upgrade and reconfigure the D2
  first.  Then, proceed with the
  OMEGAMON XE for DB2 on z/OS V310 configuration.
  ```

  This warning can be ignored.
- The Tivoli Enterprise Monitoring Server or Tivoli Enterprise Monitoring Agent on z/OS RKPDLOG log indicates that the persistent datastore has no more writable datasets. This problem occurs when the persistent datastore maintenance jobs are not being run. Possible reasons for the maintenance jobs to fail are:
  - A bad JOB card in the RKANSAMU(KPDJOBC) member.
  - Failure to copy the maintenance procedures to the system procedure libraries.
  - Environment security profiles do not allow the jobs to execute.
  - The job being run on a system other then the one it was submitted on.
  - Batch initiators not running for the specified JOB class.
  - Automation purges or holds the jobs based on site requirements.

  This failure causes the datasets to become invalid or full over a period of time. This condition then contributes to multiple errors when the persistent datastore starts returning error codes to the persistent datastore clients.
- The RKPDLOG log on the hub Tivoli Enterprise Monitoring Server on z/OS may contain this message:

  ```
  14:15:00.18 (0000-EFB498CB:khdattr.c,615,"scanAttrlibDirectory") return status
     from  QPM1_ReadDir is <5>
  ```

  This message is being sent in error and does not mean that errors are occurring in the Tivoli Data Warehouse operation. You can ignore it.

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

Target document: *Configuring Tivoli Enterprise Monitoring Server on z/OS*

After installation of application support, product-provided situations are not displayed 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, *&rvhilev.&rte.&vsamfsv.RKSSSITF*, where *&rvhilev* is the VSAM runtime high-level qualifier, *&rte* is the RTE name, and *&vsamvsf* is the monitoring server EIB VSAM low-level qualifier." Refer to the TEMS started task to see a complete list of VSAM EIB files.

If the data sets are out of space:

1. Use IDCAMS to copy the data to a flat file.
2. Delete the existing file.
3. Modify the ICAT *PP*#1*xxxx* job to increase the size (where *PP* is the two-letter product code for the product [**DS** for a standalone Tivoli Enterprise Monitoring Server] and *xxxx* is the RTE JCL suffix) as follows:
   a. Invoke the Configuration Tool by executing this TSO command:
      `EX '&shilev.INSTLIB'`

      where *&shilev* is the installation high-level qualifier.
   b. On the Configuration Tool MAIN MENU, enter **3 (Configure Products)** and select the product you are want to configure (ITM Tivoli Monitoring Services or an OMEGAMON XE monitoring agent) on the PRODUCT SELECTION MENU.
   c. On the RUNTIME ENVIRONMENTS (RTES) menu, type **B** for (Build libraries) next to the runtime environment in which the monitoring server is configured, and press **Enter**. The PP#1xxxx job that allocates the runtime libraries is displayed.
   d. Edit the `CYL()` parameter in the job to increase the VSAM allocation to whatever value your DASD can accommodate
4. Submit the PP#1xxxx job.
5. Use IDCAMS to copy data from the flat file to the new VSAM.
6. Reinstall the application support for the product or products whose situations are missing or not starting correctly.

For instructions on installing application support for a monitoring agent installed on z/OS, refer to the configuration guide for your monitoring agent.

For instructions on installing application support for monitoring agents installed on a distributed system (Windows, UNIX, Linux) see the *IBM Tivoli Monitoring: Installation and Setup Guide*.

Access lists for remote monitoring servers can be inconsistent with lists maintained in the historical configuration user interface

Target document: *IBM Tivoli Monitoring: Problem Determination guide* and *Configuring Tivoli Enterprise Monitoring Server on z/OS*

In some instances, the historical configuration user interface fails to reflect that historical data was been started on the remote monitoring server on z/OS. The result it that the access lists for remote monitoring servers can be inconsistent with the lists maintained in the historical configuration user interface.

You can determine if you have this problem if error messages are displayed in the RKLVLOG, indicating that a monitoring agent on z/OS is unable to load probes for database tables or that UADVISOR situations have been started for products that are not configured to run on the remote Tivoli Enterprise Monitoring Server on z/OS. These messages do not affect normal operation of the remote monitoring server. To address this situation, you must stop collection at the remote monitoring server and restart it. But, because the interface is not aware of this collection activity, it cannot be stopped by clicking the **Stop Collection** button, which is greyed out and unavailable. Therefore you must first configure the attribute groups for historical collection.

Complete the following steps:

1. In the Tivoli Enterprise Portal, click **History Configuration Collection** icon that is located on the toolbar. You can also click **Edit→ History Configuration**.
2. In the History Collection Configuration window, select the product (agent type) for which you want to change the configurations.

   Note: The attribute groups that you can change display in a list box. When you select a product, you are configuring collection or pruning, or both, for all attribute groups for that product.
3. Select one or more attribute groups.
4. In the Configuration Controls section, complete the following steps:
   a. In the **Collection Interval** section, select the desired interval.
   b. In the **Collection Location** section, select where you want the data to be located.
      - TEMS - Tivoli Enterprise Monitoring Server
      - TEMA - Tivoli Enterprise Monitoring Agent

      Note: Collect data at the agent to minimize performance impact on the monitoring server from historical data management tasks.
   c. In the **Warehouse Interval** section, select the interval for the data you wish to collect. Set to **Off** if you do not want data warehousing, which disables the Summarization and Pruning sections.
   d. In the **Summarization** section, select the time periods for data summarization.

      Note: When you select a particular time period, by default, any time periods below the one you select is automatically selected too. For example, if you select to keep yearly summarized data, quarterly, monthly, weekly, daily, and hourly are selected too. You have the option to disable the time periods you do not want.
   e. In the **Pruning** section, select how you want to prune your data.

1) Select the time period for the table to be pruned, Yearly, Quarterly, Monthly, and so on.
2) Type the number of time periods in the next field.
3) Select the pruning time period you wish. For example, if you want to prune hourly data when it becomes 30 days old, select **Hourly**, keep **30** and choose **Days** as the time period from the drop-down list.

5. Click **Configure groups** to apply the configuration selections to the attribute group or groups. Click **Unconfigure groups** to clear the new settings.

   Note: You have to stop collection, by selecting Stop Collection, before you can change the configuration for an attribute group.

6. Click **Start Collection** to start the collection process on the configured group. If you have more than one Tivoli Enterprise Monitoring Server for an attribute group:
   a. When you click **Start Collection**, the **Select TEMS** window is displayed with a list of the available servers so you can choose a server from which to start collection.
   b. You can click the **Collection** column in the Attribute Groups table to see a list of started Tivoli Enterprise Monitoring Servers.
7. After this action, the **Stop Collection** button is available and you can stop collection for this remote monitoring server.

Tivoli Enterprise Portal desktop and browser clients

These known problems and limitations are related to the Tivoli Enterprise Portal desktop and browser clients.

- You cannot delete a situation by clicking the **Delete** icon on the Situation Editor toolbar when you perform a **Create >New** or **Create >Another** function.

  To delete the situation, right-click on the situation name and select **Delete** or, with the situation selected, select **Delete** from the tool bar.

- A policy does not function and returns a status code of 1145. Status code 1145 means that the Tivoli Enterprise Monitoring Server cannot find the situation's definition.

  When a policy workflow runs a situation-based activity, the definition of the associated situation is required and the policy will not function if the situation definition is not found. The definition can be missing because the situation was deleted by mistake. Restore the situation if it was deleted.

  Additionally, the situation definition is available to a policy only if the situation and policy have both been distributed to the same Tivoli Enterprise Monitoring Server. A policy and situation are not always directly distributed to a Tivoli Enterprise Monitoring Server, but are distributed to agents. The situation is distributed to the Tivoli Enterprise Monitoring Server if the agent to which the situation is distributed is connected to that Tivoli Enterprise Monitoring Server. Ensure that the situation has the same distribution as the policy.

- In some instances when upgrading custom workspaces from OMEGAMON 350 to IBM Tivoli Monitoring V6.1 Fix Pack 005, depending on how the workspace was saved in OMEGAMON 350, the original default workspace might not be displayed for some users. The default workspace is still available under the list of workspaces returned under Enterprise Workspace.

  You can access the original default workspace and reset it as the default by doing the following steps:

  1. In the Enterprise Workspace, select the original default workspace.

2. Click **Properties** in the toolbar.
3. Under **Workspace Options**, select **Assign as default for this Navigator item**.
4. Click **Apply** and **OK**.
5. Close the portal. When you are asked if you want to save the changes you have made, click **Yes**.
6. When you reopen the portal, the default workspace is correctly displayed.

Tivoli Enterprise Portal Server

These known problems and limitations are related to the Tivoli Enterprise Portal Server.

- In large environments, two symptoms might be observed when a Tivoli Enterprise Portal Server on AIX is started:
  - The system stops while initializing KfwServices. This happens when the KFW_STARTJVM environment variable setting in the `cq.ini` file is **N**. Other similar symptoms are possible.
  - The system goes into a loop when initializing KfwServices. This happens when the setting for the KFW_STARTJVM environment variable is **Y** .

  KfwServices on the portal server is linked with the default memory model. The default data and stack size of 256 MB in the default memory model causes this problem.

  In smaller environments, this problem might not occur at startup, but at some later point, as more virtual storage is required, the same situation can be observed.

  To determine if your portal server is likely to encounter this problem, enter `topas` from the command line on the portal server AIX system where the portal server is running. If the output of this command shows that KfwServices has a `PgSp` value of **180-250** MB, you should take steps to prevent this failure. In smaller environments, even if the value for this parameter is near 180, this is an indicator that the problem might occur when the system processes large queries.

  Apply this workaround to systems that use the DB2 small memory model to prevent these types of failures. This workaround requires that you modify the KfwServices load header, the potral server configuration and the DB2 configuration. If the changes are not made in both applications at the same time, the portal server log will show DB2 SQL errors of `SQLSTATE=55032`.

  For information about this workaround,, see Technote 1258694 at http://www-1.ibm.com/support/docview.wss?uid=swg21258694.

  Note: The directory names in the instructions that follow are typical, but use the directory locations appropriate to your system.

  1. Make these changes to the portal server configuration files.
     a. Stop the portal server using these commands:

        ```
        cd /opt/IBM/ITM/bin
         ./itmcmd agent stop cq
        ```

     b. Issue the following commands to reset the `maxdata` value:

        ```
        cp KfwServices KfwServices.orig
        /usr/ccs/bin/ldedit -bmaxdata:0x80000000 KfwServices
        ```

     c. To verify that the `maxdata` value has been reset, issue the following command:

        ```
        dump -ov KfwServices
        ```

This command causes the maxdata value in KfwServices to be displayed, as shown in this sample output:

```
maxSTACK     maxDATA     SNbss       magic       modtype
0x00000000  0x80000000  0x0003      0x010b        1L
```

d. Change directories as indicated:

```
cd /opt/IBM/ITM/config
```

e. Use any AIX text editor to add the following line at the end of the cq.ini file:

```
EXTSHM=ON
```

Save the edited cq.ini file.

2. Make these changes to the DB2 configuration files from the DB2 installation user ID (the default is db2inst1),
   a. Stop the DB2 server if not already stopped, using these commands:

```
cd /db2inst1/sqllib/adm
db2stop
```

   b. Issue the following commands:

```
export EXTSHM=ON
db2set DB2ENVLIST=EXTSHM
db2set -all
```

   c. Use any AIX text editor to add the following lines at the end of the file /db2inst1/sqllib/userprofile::

```
EXTSHM=ON
export EXTSHM
```

Save the edit userprofile file.

3. Restart DB2 using these commands:

```
cd /db2inst1/sqllib/adm
db2start
```

4. Restart the portal server using these commands:

```
cd /opt/IBM/ITM/bin
./itmcmd agent start cq
```

- After upgrading to IBM Tivoli Monitoring Version 6.1 Fix Pack 005 from Fix Pack 002 or earlier, you might find that your operators are no longer able to see the severity of situations in Situation Event Consoles. This issue can be addressed by running the workspace migration utility to upgrade those workspaces on the system where Tivoli Enterprise Portal Server is installed. For information about running this utility, see "Tivoli Enterprise Portal Server checklist" on page 31.
- You cannot use tacmd configurePortalServer command to determine available data sources for the Tivoli Enterprise Portal Server. The problem does not affect historical collection

  To determine available data sources for the portal server, log on to the Tivoli Enterprise Portal, open the query editor, and start the process to create a new query. This action causes the query editor to display information about the data sources defined to it. The query editor displays the names of the data sources and their description, but does not show the user ID and connection limit as the tacmd configurePortalServer command does. For additional information about issuing tacmd commands, refer to the *IBM Tivoli Monitoring: Command Reference*.
- If the password for the user ID used to create the Tivoli Enterprise Portal Server database on the Linux silent installation contains special characters such as the "*" (asterisk) or the "!" (exclamation point), the Tivoli Enterprise Portal Server database creation will fail.

- The *IBM Tivoli Monitoring Problem Determination Guide* provides the incorrect command and file name to change the timeout settings for Linux and UNIX computers.

  The default timeout for the Tivoli Enterprise Portal Server is 600 seconds. Use the following procedure to change the timeout setting to KFW_SQL1_ASYNC_NOTIFY_MAX_WAIT in the Tivoli Enterprise Portal Server environment configuration file if the Tivoli Enterprise Portal Server is timing out while waiting for a deployment action to complete:

  1. For Windows computers, open the *ITMHOME*cnps kfwenv configuration file.

     For Linux and UNIX computers, open the *ITMHOME*config cq.ini configuration file.
  2. Add KFW_SQL1_ASYNC_NOTIFY_MAX_WAIT=1000 to the end of the configuration file.
  3. Save the file and restart the Tivoli Enterprise Portal Server.
- You might see numerous errors in the Tivoli Enterprise Portal Server logs and the Tivoli Enterprise Portal Server might not shut down correctly when you send thousands of events more than the Tivoli Enterprise Portal Server was designed to handle.

  Use correct system design and load balancing in order to evenly distribute the load to the Tivoli Enterprise Portal Server.
- When your Tivoli Enterprise Portal Server is running on HP and you view custom workspaces after upgrading from OMEGAMON 350 to the current fixpack, the ″Status″ column in the Situation Event Console does not reflect the state assigned to the situation which is firing.

  From the toolbar, drag and drop a new Situation Event Console view icon into the existing workspace in the custom view to replace the Situation Event Console view that is not reflecting the correct states. You must then redefine the workspace links if you choose to use them.
- If you install the Tivoli Enterprise Portal Server on a Microsoft SQL Server 2000 computer with the SQL authentication method set to ″mixed mode,″ you might receive internal security authentication rule errors stating that all SQL servers must use ″Windows only″ authentication. Use the following procedure to install the portal server with the Microsoft SQL Server 2000 in Windows Authentication only mode. A script for performing this action should be available from your IBM service representative.

  1. Temporarily configure the Microsoft SQL Server 2000 computer to use mixed mode authentication (for example, SQL Server and Windows authentication).
  2. Use the *IBM Tivoli Monitoring Installation and Setup Guide* to install the Tivoli Enterprise Portal Server.
  3. Stop the portal server through the Manage Tivoli Enterprise Monitoring Services utility.
  4. Reconfigure the Microsoft SQL Server to use Windows authentication only.
  5. Open the Control Panel and double-click **Administrative Tools**.
  6. Double-click on **Data Sources (ODBC)**.
  7. Select the **System DSN** tab.
  8. Select the ″teps″ data source and click **Configure**.
  9. Click **Next** until you receive the window that prompts you to designate how you want the Microsoft SQL Server to verify the authenticity of the login ID.
  10. Select **With Windows NT® authentication using the network login ID**.

11. Click **Next** until the **Finish** button is displayed, and then click **Finish**.
12. Click **OK** and close the ODBC Data Sources control panel.
13. Open a Command Prompt window.
14. Enter the following command:

    ```
    osql –E
    ```

    Note: If the osql.exe application is not in your path, run the same command from the Microsoft SQL Server bin directory.
15. At the prompt, enter the following commands:

    ```
    > use teps
    > go
    ```
16. At the prompt, enter the following commands:

    ```
    > sp_changeobjectowner 'teps.KFWSEEDLEVEL', 'dbo'
    > go
    ```
17. Repeat the command in step 16, replacing KFWSEEDLEVEL for each of the following table names:
    - KFWATTAC
    - KFWDBVER
    - KFWEDGE
    - KFWFOUNDODI
    - KFWHISTBEHAVIOR
    - KFWHISTDATA
    - KFWHISTSTAT
    - KFWJRNLLOGIN
    - KFWLAUNCH
    - KFWLOGIN
    - KFWMOBJ
    - KFWMOBJASSIGNED
    - KFWMOBJPROP
    - KFWNOTES
    - KFWPARMA
    - KFWPRESDEF
    - KFWPRESENTATION
    - KFWQUERY
    - KFWRANGES
    - KFWSEEDLEVEL
    - KFWSOUND
    - KFWTMPL
    - KFWTMPLSIT
    - KFWTMPLSTA
    - KFWTOPO
    - KFWTSIT
    - KFWUAXREF
    - KFWUSER
    - KFWUSERTOPO
    - KFWWORKPLACE
    - KFWWORKSPACE

- KFWWORKSPACELINK

18. Exit the osql.exe application by typing "quit" and close the command prompt window.
19. The manual configuration steps are complete. Start the portal server and connect a client.

- The command line interfaces to import and export workspaces have the following limitations:
  - Custom queries are not exported or imported by the **tacmd exportWorkspaces** and **tacmd importWorkspaces** commands. When you export a workspace that utilizes custom queries and import that workspace into a different server, the workspace will not work correctly unless you manually recreate the custom query on the server onto which you imported the workspace.
  - Custom situations are not exported or imported by the **tacmd exportWorkspaces** and **tacmd importWorkspaces** commands. Situation definitions, both predefined and custom, are stored on the Tivoli Enterprise Monitoring Server. When you export a workspace that uses custom situations and import that workspace into a Tivoli Enterprise Portal Server that connects to a different monitoring server than the portal server that you exported the workspace from, you must also export the situations from the original monitoring server to the new monitoring server. You can use the **tacmd viewSit** and **tacmd createSit** commands to export and import situations from one monitoring server to another; refer to the *IBM Tivoli Monitoring User's Guide* for more information about the **tacmd viewSit** and **tacmd createSit** commands.
  - When you export a workspace from one portal server to another (for example from a test environment to a production environment), that workspace is not available from the logical view in the new portal server unless you have the exact same navigator items in the view. You cannot create these items manually but you must instead migrate them from one environment to another. To ensure that you have the *exact* same items, use the following process for setting up your environment and migrating the workspaces:
    1. Create the logical view on the portal server in the test environment.
    2. Run the migrate-export utility to migrate the portal server information to an SQL file. For information on this migration utility, see the "Tivoli Enterprise Portal Migration" chapter in the *IBM Tivoli Monitoring Administrator's Guide*, located at http://publib.boulder.ibm.com/infocenter/tivihelp/v3r1/index.jsp?toc=/com.ibm.itm.doc/toc.xml.
    3. Move the SQL file created by the migrate-export utility to the portal server in the production environment.
    4. Run the migrate-import utility to replicate the logical view on the production portal server.
    5. On the portal server in the test environment, create your workspaces and customize as desired.
    6. Use the **tacmd exportWorkspace** command to export the workspaces from the test environment.
    7. Use the **tacmd importWorkspace** command to import the workspaces in the production environment.

    Note: You must use the preceding process to create the navigator items in the new environment. You cannot manually create the navigator items.

- When you configure the Tivoli Enterprise Portal Server on z/Linux by using the `./itmcmd config -A cq"` command, the file /opt/IBM/ITM/ls3263/cw/applet.html is updated to include the portal server functions. Each time this command is issued, new entries for kcf.jar, kqi_resources.jar, kmc.jar, kmq_resources.jar are appended to the CACHE_ARCHIVE section of the applet.html file. This happens even if the jar files being added are the same version as previous ones.

  This does not affect the operation of the Tivoli Enterprise Portal Server and can be ignored.

Historical data collection issues

These known problems and limitations are related to historical data collection, the Summarization and Pruning Agent, and the Warehouse Proxy Agent.

- A request for historical data results in a SQL 3000 error. You have asked for historical data, but history does not start for this history group.

  Go back to the history configuration panel and start the history group associated with this data. After the collection is started, you will no longer experience the SQL 3000 error.

- For monitoring agents on z/OS that use Tivoli Data Warehouse and capture configuration data in GENHIST files, there are instances when a persistent datastore delete request can corrupt a dataset.

  This database corruption problem prevents Tivoli Data Warehouse from retrieving configuration data, so that the warehouse cannot determine what data has and has not already been exported from the persistent datastore. When this problem occurs, there is typically a RKPDOUT sysout in the started task. Messages similar to the following may be displayed:

  ```
  TiChainHeader::Delete(nnnnn, nnnnn): Error: Unable to find next entry
    that points to deleted level 1 index entry
  TiChainHeader::Delete:  Formatted print of current object follows.
  ```

  A secondary issue is that the persistent datastore starts tracing details about the environment. This can use up a lot of spool space. This issue can be observed if you determine that the RKPDOUT sysout is increasing in size significantly, and the overhead of the started task also increases.

  This problem affects the Tivoli Enterprise Monitoring Server on z/OS and all OMEGAMON XE z/OS agents.

  To recover from this situation, if the persistent datastore terminates, a restart of the agent or monitoring server on z/OS is required. If the dataset is corrupted, run the following command:

  ```
  /F stcname,KPDCMD RECOVER FILE DSN:datasetname
  ```

  where *stcname* is the name of the started task where the persistent datastore dataset is corrupted and *datasetname* is the name of the dataset with an issue. The dataset names that are candidates for corruption are those that have a low level qualifier of RGENHIS1, RGENHIS2, and RGENHIS3.

  Note that the current active dataset will not be eligible for this operation. However, issuing the following command can switch the datasets so that the active one becomes inactive:

  ```
  /F stcname,KPDCMD SWITCH GROUP=GENHIST
  ```

  When this operation is complete, you can issue the RECOVER command for the dataset that was active at the time of the SWITCH command was executed. The tracing can be stopped by issuing the following command:

```
/F stcname,KPDCMD DEBUG OFF
```

- The Tivoli Enterprise Portal Server might record messages similar to these below. These messages can be ignored.

```
(DATE, TIME-{EBC}cthistorypublisherevaluator_i.cpp,986,"CTHistoryPublisher_i::HistoryManager::_buildProductList")
  Application 'KCF' in TEMS SYSTEM catalog but history configuration file 'C:\IBM\ITM\CNPS\SQLLIB\kcf.his' not found.
(DATE, TIME-{EBC}cthistorypublisherevaluator_i.cpp,986,"CTHistoryPublisher_i::HistoryManager::_buildProductList")
  Application 'KFA' in TEMS SYSTEM catalog but history configuration file 'C:\IBM\ITM\CNPS\SQLLIB\kfa.his' not found.
(DATE, TIME-{EBC}cthistorypublisherevaluator_i.cpp,986,"CTHistoryPublisher_i::HistoryManager::_buildProductList")
  Application 'KFW' in TEMS SYSTEM catalog but history configuration file 'C:\IBM\ITM\CNPS\SQLLIB\kfw.his' not found.
(DATE, TIME-{EBC}cthistorypublisherevaluator_i.cpp,986,"CTHistoryPublisher_i::HistoryManager::_buildProductList")
  Application 'KMC' in TEMS SYSTEM catalog but history configuration file 'C:\IBM\ITM\CNPS\SQLLIB\kmc.his' not found.
(DATE, TIME-{EBC}cthistorypublisherevaluator_i.cpp,986,"CTHistoryPublisher_i::HistoryManager::_buildProductList")
  Application 'KMQ' in TEMS SYSTEM catalog but history configuration file 'C:\IBM\ITM\CNPS\SQLLIB\kmq.his' not found.
(DATE, TIME-{EBC}cthistorypublisherevaluator_i.cpp,986,"CTHistoryPublisher_i::HistoryManager::_buildProductList")
  Application 'KMS' in TEMS SYSTEM catalog but history configuration file 'C:\IBM\ITM\CNPS\SQLLIB\kms.his' not found.
(DATE, TIME-{EBC}cthistorypublisherevaluator_i.cpp,986,"CTHistoryPublisher_i::HistoryManager::_buildProductList")
  Application 'KQI' in TEMS SYSTEM catalog but history configuration file 'C:\IBM\ITM\CNPS\SQLLIB\kqi.his' not found.
(DATE, TIME-{EBC}cthistorypublisherevaluator_i.cpp,986,"CTHistoryPublisher_i::HistoryManager::_buildProductList")
  Application 'KQM' in TEMS SYSTEM catalog but history configuration file 'C:\IBM\ITM\CNPS\SQLLIB\kqm.his' not found.
(DATE, TIME-{EBC}cthistorypublisherevaluator_i.cpp,986,"CTHistoryPublisher_i::HistoryManager::_buildProductList")
  Application 'KSY' in TEMS SYSTEM catalog but history configuration file 'C:\IBM\ITM\CNPS\SQLLIB\ksy.his' not found.
(DATE, TIME, 20:53:09-{EBC}cthistorypublisherevaluator_i.cpp,986,"CTHistoryPublisher_i::HistoryManager::_buildProductList")
  Application 'OMSMS' in TEMS SYSTEM catalog but history configuration file 'C:\IBM\ITM\CNPS\SQLLIB\omssqlms' not found.
(DATE, TIME-{EBC}cthistorypublisherevaluator_i.cpp,986,"CTHistoryPublisher_i::HistoryManager::_buildProductList")
  Application 'PDSSTATS' in TEMS SYSTEM catalog but history configuration file 'C:\IBM\ITM\CNPS\SQLLIB\pdssqlst' not found.
(DATE, TIME-{EBC}cthistorypublisherevaluator_i.cpp,986,"CTHistoryPublisher_i::HistoryManager::_buildProductList")
  Application 'SYSTEM' in TEMS SYSTEM catalog but history configuration file 'C:\IBM\ITM\CNPS\SQLLIB\syssqlte' not found.
```

  These messages can be ignored.

- If your workspace views display historical data across multiple pages, data is displayed only on the first page (and not displayed on subsequent pages).

Summarization and pruning Agent

These known problems and limitations are related to the Summarization and Pruning Agent.

- Sometimes when the Summarization and Pruning Agent has been correctly configured using the Managing Tivoli Enterprise Management Services interface and seems to be running, it actually is not. No data is ever aggregated into the various *_H, *_D, *_W, *_M, *_Q, *_Y tables in the WAREHOUS database, and no *sy_java*.log file is created.
- If the hub Tivoli Enterprise Monitoring Services on Windows, UNIX, or Linux run the following command on the monitoring server:

  ```
  itmcmd support -t <TEMS> sy
  ```

  Then recycle the monitoring server using this command:

  ```
  itmcmd server stop/start <TEMS> sy
  ```

  If the hub monitoring server is on z/OS, if the Tivoli Enterprise Portal Server is running is on Windows, then right-click on the portal server and select **Advanced->Add TEMS application support**. Select **Remote** and select **Summarization and Pruning Agent Support**. For more information, see Technote 1230920 at http://www-1.ibm.com/support/docview.wss?uid=swg21230920
- For the Warehouse Summarization and Pruning agent, if you are using Microsoft SQL server, install the MS SQL 2005 JDBC driver. The Warehouse Summarization and Pruning agent might fail to run at the scheduled time on Windows computers because of a limitation of the number of tables it can retrieve. The MS SQL 2005 JDBC driver addresses this limitation. You can download the JDBC driver from the Microsoft Web site, http://msdn.microsoft.com/data/jdbc/default.aspx.

- On Windows 2000 computers, the Summarization and Pruning agent does not work after you upgrade from OMEGAMON to IBM Tivoli Monitoring.

  A reboot is required to reset your home directory for the Summarization and Pruning agent.

Warehouse Proxy Agent

These known problems and limitations are related to the Warehouse Proxy Agent.

- When configuring one or more warehouse proxy agents, connect all of them to the hub Tivoli Enterprise Monitoring Server, not to a remote monitoring server. Connecting a warehouse proxy to a remote monitoring server results in incorrect connections. For example, if the local location broker facility in the remote monitoring server included a previously existing network address of a previously existing warehouse proxy agent, the monitoring agents connected to that remote monitoring server might try to send the data to this obsolete warehouse proxy.

  To address this problem, end the connection of the warehouse proxy agent to the remote monitoring server and reconfigure the warehouse proxy so it connects to the hub monitoring server.

- Sometimes the export operation for the warehouse proxy fails to start if the Tivoli Enterprise Monitoring Server on z/OS history collection starts before the warehouse proxy is configured and started.

  In this scenario, the Tivoli Monitoring Services environment is configured to collect history data at the monitoring agent for all default attribute groups using all default setting, including a warehouse interval of 1 hour, but the warehouse proxy has not been configured or started. Because history collection is enabled, when the warehouse interval is reached even without the warehouse proxy configured and started, messages similar to these can be found in the monitoring agent RKLVLOG when the monitoring agents tries to export history data:

  ```
  2006.128 14:44:55.00 (0000-EE3B57EB:khdxdacl.cpp,613,"resolveServerAddress")
     Warehouse proxy not registered
  2006.128 14:44:55.00 (0001-EE3B57EB:khdxdacl.cpp,458,"routeExportRequest")
    Export for object <CICSplex_Enqueue_Pool_Details> failed , Status = 73
  ```

  There is one entry like this for each object for which you are recording history. This is typical behavior.

  If you now configure and start the warehouse proxy, you expect the export operations to start working and these error messages to stop, but in some instances, this does not happen. Exports are attempted at the default collection interval (15 minutes), not the interval you may have specified. The environment fails to acknowledge that the warehouse proxy has been started and configured.

  In some cases even when history collection is stopped at the Tivoli Enterprise Portal, the environment continues attempting to export data to the warehouse proxy, causing the monitoring agent RKLVLOG to grow very fast during that time because export errors are being continually written.

  To address this problem, restart the affected components in the Tivoli Monitoring Services environments.

Universal agent issues

These known problems and limitations are related to the universal agent.

- Some instances of the Universal Agent do not start or appear as if they have not been upgraded after installing the fix pack.

All instances of the Universal Agent have been upgraded after you run the installation. You must manually restart those Universal Agent instances that do not automatically restart or appear as if they have not been upgraded.

- After upgrading to Fix Pack 005 on a UNIX or Linux computer, some of your Universal Agent instances that were installed remotely do not restart and you receive the following error:

  ```
  Starting agent...
  *** glibc detected *** double free or corruption (!prev): 0x08248e38 ***
  Unable to start agent. Please, check log file.
  ```

  Upgrade the Universal Agent to Fix Pack 005 and manually restart any Universal Agent instances that did not restart.
- On SUSE Linux Enterprise Server 10 computers, you cannot start the Universal Agent through the CandleManage GUI.
- After upgrading the Universal Agent with the fix pack, the correct version is not displayed. The agents have been upgraded as expected, however.

Globalization

These known problems and limitations are related to IBM Tivoi Monitoring components in a globalized environment.

- In non-English environments, the agent help is not displayed in the help panel.

  For Windows computers, run C:\IBM\ITM\CNB\classes\candle\helpmerg.bat from the command line.

  For UNIX computers, run $CANDLEHOME/bin/CandleExecute cq helpmerg.sh from the command line.
- The i5/OS operator messages displayed in the Tivoli Enterprise Portal in Japanese are not displayed correctly. This problem occurs after you have installed the fix pack and applied the language pack. The installation program changes the value for the CCSID variable in the QAUTOMON file.

  To fix this problem, you can do the following.

  1. Open a profile of the user QAUTOMON using this command:

     ```
     WRKUSRPRF USRPRF(QAUTOMON)
     ```
  2. Change the character code set ID (CCSID) of the profile to an appropriate Japanese CCSID (ex. 5035).
  3. Restart the i5/OS monitoring agent.
- For SUSE Linux Enterprise Server 10 computers, the Tivoli Enterprise Portal displays corrupted text resources in the Japanese locale.

  Download Kochi fonts contained in the kochi-substitute-20030809.tar package from the following Web site: http://sourceforge.jp/projects/efont/files/.
- Help or Expert Advice pages might not load in a Simplified Chinese language environment when using the browser client for the portal. This is related to a Java problem, which you can correct by setting the **-Dibm.stream.nio=true** Java Runtime parameter.

  On Windows computers, perform the following steps to set this parameter:

  1. On the Control Panel, double-click the icon for the Java plug-in.
  2. On the **Advanced** tab, type the following in the **Java Runtime Parameters** text box: `-Dibm.stream.nio=true`
  3. Click **Apply**.

  On Linux computers, perform the following steps to set this parameter:

  1. From a command line, change to the jre/bin directory:

     ```
     cd ../../jre/bin directory
     ```

2. Run the following command:

   ```
   ./JavaPluginControlPanel
   ```

3. On the **Advanced** tab, type the following in the **Java Runtime Parameters** text box: `-Dibm.stream.nio=true`
4. Click **Apply**.

- In some upgraded environments (for example in environments using a double-byte character set), you might need to re-install your Java for the Tivoli Enterprise Portal browser client, despite already having Java installed. This is because the portal server fix pack upgraded the level of Java available.

Online help

These known problems and limitations are related to online help.

- When the Tivoli Enterprise Portal online help is opened from the Tivoli Enterprise Portal help menu, in Internet Explorer the text entry fields in the **Index** and **Search** tabs are disabled; in Firefox the Index has no text entry field and the **Search results** field is filled with text. When the online help index and search text entry fields are disabled, it means your browser is unable to read the Java applets required to enable these fields. Use the following steps to resolve this problem:
  1. If the help is open, close the browser window.
  2. On the computer where the Tivoli Enterprise Portal Server is installed, locate the contents.htm file:

     Windows computers:

     <*install_dir*>\cnb\classes\candle\fw\resources\help\lang\

     UNIX computers:

     <*install_dir*>/cnb/classes/candle/fw/resources/help/lang
  3. Rename contents.htm to contents.bak.
  4. Rename contents_dhtml.htm to contents.htm.

  If the <*install_dir*>\cnb\classes\candle\fw\resources\help\lang\ directory does not have a contents_dhtml.htm file, edit contents.htm as follows:

  1. Close any open browser windows.
  2. Open contents.htm in a text editor.
  3. On line 15, change the var nWebhelpNavPaneMode parameter to 1 for DHTML: var nWebhelpNavPaneMode = 1
  4. Save the contents.htm file.

  The next time you start the help system from the portal Help menu, the **Index** and **Search text** entry fields will be enabled.
- The hover help is missing for the Time attribute in the **Local Time** and **Global Time** attribute groups. These are the descriptions:
  - **Time** in the **Local Time** attribute group: The time of the data sampling, corrected for local time zone and daylight saving time, formatted as HHMMSS. For example, 170700 is 5:07 PM.
  - **Time** n the **Global Time** attribute group: The time at the hub Tivoli Enterprise Monitoring Server when the data was sampled, formatted as HHMMSS. For example, 153000 is 3:30 PM.

Chapter 6. APARs addressed by this fix pack

The following APARs are addressed by this fix pack. For a list of APARs fixed in previous fix packs, refer to *IBM Tivoli Monitoring: Fix Pack 004 Readme and Documentation Addendum*.

Documentation APARs

The following APARs are addressed in Chapter 5, "Known problems and limitations," on page 57 in the Fix Pack 005 readme:

APAR Number	Symptom
IY91827	The Linux network input errors and output errors are incorrect for situation Linux_Network_IO_Errors_High.
IY91966	Users of the fix pack documentation wanted sample output from the `cinfo` and `kincinfo` commands. For sample output of these commands, see "Validating what you installed" on page 37.

IY92687	On all versions of IBM Tivoli Monitoring Version 6.1 since Fix Pack 3, lack of support for the SOAP server on remote distributed Tivoli Enterprise Monitoring Servers prevents `tacmd` commands from being issued when us specify a remote monitoring server as the "Server Name."These two commands are known to be affected:
	1. When you run the `tacmd createNode` command without logging into the console of the monitoring server, you may see the following error message:
	`The path for DEPOTHOME C:\IBM\ITM\CMS was not found.`
	`The specified path to the depot is incorrect or does not exist.`
	`If the variable DEPOTHOME was specified within the KBBENV file then change the value of this variable to correct path to the depot.`
	`If DEPOTHOME was not specified within KBBENV file, call IBM Support.`
	`If the variable DEPOTHOME was specified within the KBBENV file, change the value of DEPOTHOME to correct path to the depot. If DEPOTHOME was not specified within KBBENV file, call IBM Support.`
	2. If you then try to log on to the remote monitoring server by issuing a `tacmd login` command to a remote monitoring server where SOAP is disabled, you may see a message similar to the following:
	`KUIC00003E: Cannot connect to a server at addresses:`
	`https://server.mynetwork.com:3661, https://server.mynetwork.com:63765 ,`
	`http://server.mynetwork.com:1920,`
	`http://server.mynetwork.com:63764`
	`Make sure the server on server.mynetwork.com is available and configured for the specified protocols and ports.`
	To work around this problem, log in to **Managing Tivoli Monitoring Services** on the remote monitoring server and issue this command:
	`tacmd login -s <hub_tems_hostname>`
	
	Where <*hub_tems_hostname*> is the target monitoring server where you are trying to deploy agents or updates. You can then deploy agents or updates from the depot on the remote monitoring server.

© Copyright IBM Corp. 2007

APAR Number	Symptom

IY92894	The example of the `tacmd removebundles` command in Appendix A of the *IBM Tivoli Monitoring: Administrator's Guide* (SC32-9408-00) and on page 207 of the *IBM Tivoli Monitoring: Installation and Setup Guide* (GC32-9407-00), page 207 is incorrect.
	
	This sample command documented in these guides is intended to removed UX bundles from the agent depot:
	`tacmd removeBundles -i /mnt/bundles -t ux -p aix513 -v 060100000`
	
	Instead, this command removes all of the deployment bundles in the **/mnt/bundles** directory from the local deployment depot, where **ux** is the the bundle product type, **aix513** is the bundle platform, and **060100000** is the bundle version.
	
	Therefore, when this command is issued as documented, the following error message is returned:
	`KUICRB019E: The directory /mnt/bundles contains no bundles matching the product(s), platform(s), and/or version(s) specified. There are no bundles to remove.`
	
	The reason for this message is that, when specifying the **-i** option, the required pathname is that of the bundles contained Agent Depot /tables/<server?>/ depot directory, not that of the tar files, as the documentation implies. To remove the required Bundles from Agent Deploy's Depot, specify the pathname of the /depot directory in the removebundles command, as shown in the following example:
	`tacmd removebundles -i c:\IBM\ITM\cms\Depot\Packages\WINNT\KNT\061000000`
	
	Where -i = $CANDLEHOME\cms\depot\PACKAGES\<*ARCH*>\<*KOMPONENT*>\<*VERSION*>.

IY93194	On a Tivoli Enterprise Monitoring Server on UNIX, if you add to or create a file manually in the $CANDLEHOME/tables directory, the file will be seen as a monitoring server instance name and an attempt made to start a monitoring server with that name, which would fail. Normal configuration tasks require that you edit files placed in this directory by the installer program. The problem results when you add files to this directory or create new files in this directory. The autostart operation can be avoided by not manually placing or creating files in the $CANDLEHOME/tables directory.

Installation component APARs

The following APARs are addressed in Fix Pack 005:

APAR number	Symptom
IY89533	IBM Tivoli Monitoring Version 6.1 was creating /opt/IBM/ITM/tmaitm6/links with 777 permission.
IY89867	The Summarization and Pruning Agent fails to start on AIX version 5.3 after Fix Pack 3 is applied.
IY91097	Installation of IBM Tivoli Monitoring version 6.1 on UNIX platformsps can fail when a version GSKit version 7 already exists on the target system.
IY92495	On UNIX or Linux systems, the itmpatch tool returns a message stating a prereq is missing even though the prereq is installed.
IY93274	Values set by the **Edit Variables** action in KinConfg.exe were lost when users upgraded from anything to Fix Pack 4.

APAR number	Symptom
IY93472	The INITTAB does not start the database agents on a system reboot. When database agents are being deployed to the remote systems using the `tacmd` command or directly from the Tivoli Enterprise Portal client, the instance name and user information provided were not being processed correctly, causing an invalid entry to be generated similar to this: `su - USER -c "CANDLEHOME/bin/CandleAgent -o start ud"` Where *USER* is the owner of the application bin directory. This problem caused the UNIX OS monitoring agent to not be restarted on system reboot. See "Changes in the behavior of the autostart scripts" on page 14 for additional information.
IY93626	Customized startup accounts for the Tivoli Enterprise Monitoring Server on Windows are lost when upgrading from Fix Pack 3 to Fix Pack 4.
IY94205	UNIX agents did not restart when an AIX computer was restarted. After you performed a fresh installation or upgrade of the UNIX OS monitoring or UNIX Log Agent using IBM Tivoli Monitoring version 6.2 with Fix Pack 004, the agent did not start up automatically when you recycled the AIX computer. The execute permission on the `/etc/rc.itm*` files was not set correctly, preventing the files from running during system startup. See "Changes in the behavior of the autostart scripts" on page 14 for additional information.
IY95535	The summarization and pruning agent and database connection fail after installation of the fixpack. The problem occurred because apath customization in the hd.ini file was lost during upgrade, causing the Summarization and Pruning agent to no longer be able to connect to the database.
IY95966	OMEGAMON XE for CICS® files were not being included in the UNIX build because the packaging system was lower casing all *.class files.
IY95979	The path to GSKit is hard coded into the KUIENV file. This means that other paths cannot be used, preventing local security policies from being recognized when a fix pack is installed.
IY95980	Five Tivoli Enterprise Portal Server tables (KFWATTAC, KFWHISTBEHAVIOR, KFWNOTES, KFWTSIT,and KFWWORKSPACELINK) are missing from the list of tables when the DB2DATASOURCE.BAT command is used [usually to apply a changed password].
IY96040	Agents are restarted with an incorrect ID after the Fix Pack 004 upgrades. When the installation is owned by a specific user, and that user is not the user who will be running the agents, the auto start scripts are generated with the ID of the installation owner instead of the ID of the user running the agents. These scripts are regenerated every time a new installation or configuration is performed, preventing users from overriding the user ID to be used when restarting the agents after a reboot. See "Changes in the behavior of the autostart scripts" on page 14 for additional information.
IY96733	When upgrading to Fix pack 005 BETA, for the Tivoli Enterprise Portal Server on a UNIX or Linux platform, the osnames file is overwritten causing the customized Managed Systems tree in the Tivoli Enterprise Portal to lose its customizations.
IY96737	When you install Fix Pack 005 on the Tivoli Enterprise Portal on Windows browser client, duplicate jar file entries are added to the applet.html file.
IY97206	During upgrade to Fix Pack 005, product codes KDP, KMC, KOS, KIP and KHL had their support files deleted by running the obsolete.bat. This file should have only been run during upgrade from releases prior to IBM Tivoli Monitoring version 6.1.

Tivoli Enterprise Monitoring Agent APARs

The following APARs are addressed in Fix Pack 005:

APAR number	Symptom
IY88519	The # character is not being placed in front of secondary IP addresses in the CT_CMSLIST keyvalue string after any agent configuration.
IY92830 OA19675	There is a memory leak in the Tivoli Enterprise Monitoring Agent historical data collection code.
IY95114 OA19815	After installing Fix Pack 004, the hub and remotes Tivoli Enterprise Monitoring Servers lose their connections. The IP.PIPE handler was found to be vulnerable to host TCP/IP packet drop on the loopback interrupt socket.
IY95204	Applying application support to Tivoli Enterprise Portal Server on AIX 5.2 fails.
IY95363	The connection and traffic monitor modules in the Linux OS agent are timing out and hanging when a socket monitor query returned a ″not ready″ message.
IY97983	The UNIX OS agent in the DMZ running with the firewall gateway feature configured failed to connect to the hub Tivoli Enterprise Monitoring Server in a different network with undocumented error code 78.
IY97984	When DBCS characters are contained in system command, the system command isn't executed even if the situation goes to open status. Using a forward slash (\) in place of the backward slash (/) for path designations gets around this problem
IY97989 OA19398	The ITMS: Engine abends with S0C4 U0000 AT 989B8452 (KDE1LNKP.DEBHBN@+2BA) immediately after startup. Additionally, a KLVER011 ABNORMAL TERMINATION AVERTED: CODE(0C4000) error is produced in the RKLVLOG. Recycling the task clears the problem.
IY97993 OA20875	Non-unique Universally Unique IDs (UUIDs) result in RPC timeouts. The code to generate Universally Unique IDs (UUIDs) guarantees each UUID generated within a process is unique. Many IBM Tivoli Monitoring processes (agents) on a single machine can easily lead to a duplicate UUID. The presence of duplicate UUIDs will result in `who_are_you` callbacks not executing, which will result in an RPC timeout. RAS1 log will show the SAR state summary with an extended duration (over 300 seconds) and only 1 packet received.

Tivoli Enterprise Monitoring Server APARs

The following APARs are addressed in Fix Pack 005:

APAR Number	Symptom
IY87167	After installing the fix pack, the tacmd createnode commend failed with the error log displaying the following message: `1326 stdout = stderr = Logon failure: unknown user name or bad password.`
IY88076 OA20851	On a Tivoli Enterprise Monitoring Server on z/OS, adding application support for monitoring agents fails with error ″SQL1_CREATEREQUEST STATUS=8.″
IY89183 OA20854	Routines in Tivoli Enterprise Basic Services socket/transport layer (KDE) issue errors messages with undocumented error codes. The code has been modified and added to the socket/transport (KDE) layer to issue a platform specific errno along with descriptive text for that error.
IY89335 OA19650	Error message KFWITM220E is received when browsing the agent workspaces in hotstandby.
IY89710	On UNIX and Linux Tivoli Enterprise Monitoring Servers, the `tacmd listsystems` command returns a misleading message after the monitoring server is restarted.

APAR Number	Symptom
IY90327	When the Windows OS agent is remotely deployed using the `tacmd createNode` command, the agent deploys successfully, but there is no entry created in Add/Remove Programs, so the agent cannot be uninstalled using Add/Remove programs.
IY90711	You cannot use `tacmd editsystemlist` command on managed system list that contains the dash character.
IY90863	For IBM Tivoli Monitoring Version 6.1 Tivoli Enterprise Monitoring Servers, System Command activities are not issuing a command for each row of situation data even though the **Continue on Failure** property is selected. Instead, the activity behaves as if the **Continue on Failure** checkbox were unselected, and the activity terminates as soon as any row returns a non-zero result.
IY90974	For a Windows system with 4GB of physical memory, the TEMS RAS1 Service log reports physical memory of 2048MB.
IY91059 OA20857	A Tivoli Enterprise Monitoring Server runs out of memory and fails. This happens when the monitoring server is processing a SOAP request returning a large number of rows.
IY91363	A system command executed on a Japanese Windows computer that includes a backslash is redirected to an incorrect file path. This problem occurs when DBCS characters and the backslash(\) are contained in the system command. Using the forward slash (/) instead of the backslash (\) redirects the file to the correct path.
IY91973 OA20877	When trace level (UNIT:kfaibloc all) is set, the Tivoli Enterprise Monitoring Server might fail.
IY92023	The Tivoli Enterprise Monitoring Server on AIX may fail during a heavy remote deployment of agents.
IY92047 OA20858	The SNMP emitter activities in a workflow did not result in the expected alert or trouble ticket because the policy was not forwarding the desired situation attributes to the emitter.
IY92106	The KDSMAIN component in the hub Tivoli Enterprise Monitoring Server does a core dump when you select the "Windows Systems" line item from the Tivoli Enterprise Portal Server. The happened because of insufficient stack size for the SQL compiler recursion for the defined predicate limit.
IY92318	Some existing workspaces are not valid and cause the import/export feature to fail, and message KUICEW013E is logged when running the `tacmd exportworkspaces` command. New function enables you to specify certain workspaces, application types, and workspace users to EXLUDE from the export operation, so that you can easily export all workspaces except the offending workspaces.
IY92420 OA20860	The Tivoli Enterprise Monitoring Server fails in process KPX.
IY92682 OA20861	The HOSTINFO attribute was exposed by the Tivoli Enterprise Portal Server and hidden by the Tivoli Enterprise Monitoring Server.
IY92698	In IBM Tivoli Monitoring version 6.1, the Tivoli Enterprise Monitoring Server goes into STOP PENDING state due to failure when tracing Tivoli Enterprise Console EEIF code.
IY92784	When installing the Linux OS Agent on Linux SUSE 9, this command: `tacmd createnode -h <hostname> -u <user> -w <password -i <install_path> -d <install_dir>` fails with message KUICCN028E The silent response file for agent KLZ could not be found in the <*install_path*>.

APAR Number	Symptom
IY92942 OA19315	A policy contains a system command activity, the target of which is an agent that is connected to a different Tivoli Enterprise Monitoring Server to that on which the policy itself is running. To send the command to the agent, the policy must determine the address of the monitoring server to which the agent is connected and establish a connection with it. This defect causes the location broker look-up to fail so that a connection between the two monitoring servers cannot be established. Consequently, the system command cannot be issued and the activity terminates with an error.
IY93238	TEC Events are not translated using attribute table mapping even if attribute table event mapping file is supplied.
IY93294 OA19535	Direct broker lookups (performed by the hub Tivoli Enterprise Monitoring Server for remote monitoring server addresses) are always made with a NULL partition ID. If the remote monitoring server registers in a broker partition (that is, if the remote monitoring server has variable KDC_PARTITION configured to the desired remote monitoring server partition name), then the hub monitoring server fails to distribute requests to that remote monitoring server because the address lookup for that remote server fails.
IY93582 OA19742	On a remote Tivoli Enterprise Monitoring Server on z/OS, IP.SPIPE loops when a NOT_READY status is presented on a read_gsk call.
IY93646	Agents do no reconnect after a Tivoli Enterprise Monitoring Server communications failure.
IY93674	Encryption keys are not created or handled correctly at IBM Tivoli Monitoring Version 6.1 Fix Pack 4 upgrade or fresh install.
IY93701	Changes made in Fix Pack 003 for the Tivoli Enterprise Monitoring Sever component caused problems for some users such that situations were not being started at the remote agents connected to a remote monitoring server. This problem has been addressed in the current fix pack. If you experience this problem, Technote 1250181 found at http://www-1.ibm.com/support/docview.wss?uid=swg21250181 has been created to address it.
IY94094 OA19732	The Energy Policy Act of 2005 changed the rules for Daylight Savings Time in the United States. Refer to this web page for details: See this bullet in Chapter 1 (1 on page 22) for more information.
IY94184	Take Action commands were not working for the i5/OS OS monitoring agent after applying Fix Pack 4 when they had worked in Fix Packs 2 and 3. **Note:** The i5/OS monitoring agent has been rebuilt as well. You will want to install the updated monitoring agent.
IY94283 OA20862	Misleading errors messages in the agent trace log file.
IY94561 OA19860 OA20869	The remote Tivoli Enterprise Monitoring Server fails in startup to bind to the LLB after Fix Pack 004 was applied. The message ″Pipe in teardown status″ was received for the LLB pipe, accompanied by many ENDPOINTNOTBOUND messages.
IY95103 OA20870	A request to stop historical data collection on the hub Tivoli Enterprise Monitoring Server fails consistently when history collection is distributed between the hub and remote monitoring servers. Requests to stop collection on a remote monitoring server succeed.
IY95108 OA19815	After installing IBM Tivoli Monitoring version 6.1 Fix Pack 4, the hub and remote Tivoli Enterprise Monitoring Servers lose connection.
IY95208 OA20873	Historical data collection stops at the agent level.

APAR Number	Symptom
IY95372 OA20874	A problem with the agent switching mechanism caused large number of IBM Tivoli Monitoring agents to be shown in the Managed System Status workspace as offline, even though they were still actively connected to the remote Tivoli Enterprise Monitoring Server.
IY95379	After installing IBM Tivoli Monitoring Version 6.1 with Fix Pack 4 or later, customized situations are lost. The installer runs the table migrate utility but the situation customizations are not applied to the new Tivoli Enterprise Monitoring Server tables.
IY95539 OA20886	Situations created against universal agent applications fail to distribute properly and fire.
IY96672 OA20875	Non-unique Universally Unique IDs (UUIDs) result in RPC timeouts. The code to generate Universally Unique IDs (UUIDs) guarantees each UUID generated within a process is unique. Many IBM Tivoli Monitoring processes (agents) on a single machine can easily lead to a duplicate UUID. The presence of duplicate UUIDs will result in `who_are_you` callbacks not executing, which will result in an RPC timeout. RAS1 log will show the SAR state summary with an extended duration (over 300 seconds) and only 1 packet received.
IY96698	On UNIX platforms, the CTIRA_THRESHOLDS option does not work. Required files were omitted during packaging.
IY96853 OA20876	The hub Tivoli Enterprise Monitoring Server fails when TEC event forwarding is enabled if incorrect attribute properties are encountered. The event forwarder attempts to format each attribute value in the results buffer. If the precision of the attribute is invalid, a buffer overrun resulted while the server attempted to format the attribute value.
IY96870 OA20879	On a hub or hot standby Tivoli Enterprise Monitoring Server or Linux or AIX, you might be unable to stop the monitoring server after it is switched from backup to primary in a hot standby configuration. The `itmcmd server stop` hangs.
IY97038	The managed systems lists are not populating correctly.
IY97072	During the deployment of an update to an the UNIX Log Agent on an endpoint, you might experience a general failure of the Tivoli Enterprise Monitoring Server issuing that update. Additionally the following message may appear as a side effect of the condition arising during an updateAgent command: `KDY1031E The agent installation command amsaix4tmfp05b4/tmaitm6/agentdepot/rc.txt returned a the return code NOTFOUND` This message is returned because of an internal logic failure occurring on the monitoring server when the failure condition arises.
IY97985 OA19378	There is a 126-byte operating system limitations on **Take Action** commands issued from a Tivoli Enterprise Monitoring Server on z/OS. The condition is reported obscurely in a non-descript message in the RKLVLOG.d
IY97986 OA19398	The ITMS: Engine abends with S0C4 U0000 AT 989B8452 (KDE1LNKP.DEBHBN@+2BA) immediately after startup. Additionally, a KLVER011 ABNORMAL TERMINATION AVERTED: CODE(0C4000) error is produced in the RKLVLOG. Recycling the task clears the problem.
IY97990 OA19604	During Tivoli Enterprise Monitoring Server startup while doing database synchronization from a remote monitoring server to the Hub monitoring server, the message 1120 TYPERR was being observed in conjunction with access list updates taking place at the remote monitoring server.
IY97992 OA19622	The Tivoli Enterprise Monitoring Server on z/OS produces a KO41039 error in request RUNONDEMANDREQUEST. STATUS= 1102. REASON= 55.

APAR Number	Symptom
IY97999 OA20752	On the Tivoli Enterprise Monitoring Server on z/OS during persistent datastore switch operation, an environmental U1213 abend occurs when the log file fills and a SWITCH is transacted. The EXTRACT maintenance option is chosen and extract processing occurs immediately after a switch. When the extract process takes the file offline during a live request for data from another task, SAS-C framework abends the task. If no such read request for data is live when the file is taken offline, no abend will occur and the data will become available after the extract is complete.
IY97964	The ViewDepot fails intermittently on a Solaris remote Tivoli Enterprise Monitoring Server. The following messages are logged in the RAS log. `(4626988C.001D-1A:kdydepot.cpp,209,"readDepot") fopen error for file:/data/ITMC7/tables/REMOTETEMS_GTHANG/depot/PACKAGES/sol296/kux/061005000/kuxsol296.dsc`
OA19305	Abend0C4 occurs in KLVST200 when values greater than 31 are specified for the LIMIT parameter.
OA19487	The Tivoli Enterprise Monitoring Agent on z/OS abends if data collection is started and the persistent data stores are not available
OA19738	Various storage abends in the IBM Tivoli OMEGGAMON XE for Mainframe Networks monitoring agent address space occurred, including ABEND40D-10, ABEND80A and finally ABEND878-10 which causes the monitoring agent ASID to end.
OA20635	The Tivoli address space startup hangs immediately in ITMS: Engine initialization. The failure occurs after application of UA33185 to a Tivoli Enterprise Monitoring Server or monitoring agent on z/OS, most frequently in legacy OMEGAMON II® address spaces.

Tivoli Enterprise Portal APARs

The following APARs are addressed in Fix Pack 005:

APAR Number	Symptom
IY92844	When the Tivoli Enterprise Portal client discovered that a Tivoli Enterprise Monitoring Server that is down, sometimes the pipeline monitor goes into a rapid succession of entries and failures and you see hundreds of message similar to this on in very rapid succession in the log: `request pipeline test yielded a request exception at: <date/time>` . This causes high CPU usage in the Tivoli Enterprise Portal and Tivoli Enterprise Monitoring Server.
IY93385	The Tivoli Enterprise Portal client displays invalid managed systems information in the situation editor/distribution tab/managed system window. When there are references in the nodelist table to non-existant managed systems, the portal server returns those nodes to the client for display in the managed system display.
IY93444	You cannot view query definitions if they use certain attribute types with values.
IY94215	On the Tivoli Enterprise Portal client, a workspace containing a graphic view may hang while processing status changes.
IY94219	After Fix Pack 4, the event flyover in Tivoli Enterprise Portal client appears and disappears in a cycle, making it difficult for the user to read or interact with the data displayed in the popup. Prior to Fix Pack 4, the event flyover was displayed constantly when the user hovered over Enterprise navigator item.
IY94332	Custom situations should not have a severity entry. Currently when a custom sit is created, a severity of UNKNOWN is put in the TSITDESC field. If the Tivoli Enterprise Portal client is using TEC event forwarding, then a severity of UNKNOWN was being sent when it should have used the situation's name to determine the severity.
IY94422	An event console instance within a workspace may not dynamically set its filter criteria. The filter item was being unconditionally persisted when it should have been persisted only if a drag-and-drop operation was used to set it.

APAR Number	Symptom
IY94426	When you use the graphical view in the Situation Editor to view the situation formula, the situation result displays UNKNOWN in the final block.
IY94863	The Tivoli Enterprise Portal client hangs if the workspace contains a graphic view and a filtered situation event console.
IY94919	When a Tivoli Enterprise Monitoring Server and a z.OS monitoring agent reside in the same z/OS address space, the affinity for that monitoring agent will be OR'ed with the affinity of the z/OS agent. Unfortunately the ManagedSystemListHelper class expects the affinity for a Managed System List to be an exact match. It tests for a match against a monitoring server-only affinity and fails the test, so it is filtered out.
IY95669	The Tivoli Enterprise Portal client (both the desktop client and the browser client) hangs when acknowledging or closing multiple (more than 20) events at a time.

Tivoli Enterprise Portal Server APARs

The following APARs are addressed in Fix Pack 005:

APAR Number	Symptom
IY85626	When a Tivoli Enterprise Portal user tries to view the agent operations log, the operation fails with error messages.
IY87961	In the Workflow Editor, the SNMP Event emitter activity cannot be included in a policy having a "Wait until a situation is True" activity that is based on a situation using Universal Message Console attributes.
IY91209	The Tivoli Enterprise Portal client incorrectly enabled the **Restore Original Workspace** option when in administrator mode.
IY91456	The workspace properties dialog fails to update correctly. The TEPS was not updating the DEFAULT_WORKSPACE and WORKSPACE_LINK_TARGET_ONLY properties in DB2 table to reflect settings from the client.
IY91846	Over time, the Tivoli Enterprise Portal Sever has a memory or thread leak.
IY92042	Situations referencing the ManagedSystem.Reason attribute can be created in Candle® Management Workstation but cannot be accessed in Tivoli Enterprise Portal situation editor.
IY92269	The Managed System Status situations do not always reset in the Tivoli Enterprise Portal navigator or event console when the situations are restarted.
IY93135	In IBM Tivoli Monitoring version 6.2 with Fix Pack 004, the Tivoli Enterprise Portal Server on all platforms fails after importing a situation that was previously deleted. On Linux or UNIX, you see a core dump. On Windows, you see a CORBA::UNKNOWN exception.
IY93443	High CPU overhead and long response times are seen when interacting with the history configuration user interface.
IY94090	You cannot view the status of situations for managed systems using the Tivoli Enterprise Portal client and the **Manage Situations** view when the monitoring agents are connected to a remote Tivoli Enterprise Monitoring Server.
IY94531	When following a link from one of the sysplex reports from the Tivoli Enterprise Portal, the target workspace displays data for all plexes. It should only show data for the plex the link came from.
IY95210	In IBM Tivoli Monitoring Version 6.1 with Fix Pack 4 or 5, user-created situations based on attributes whose data type is SCALE were not being triggered as intended. For example, if you created a situation that should be triggered when the value of a scaled attribute reached 25 and the situation attribute was defined as SCALE:2, then even though the internal form is correct (2500), the situation might not triggered.

APAR Number	Symptom
IY95236	If a large number (200 or more) node updates need to be processed in the same interval, an incorrect SQL string might be generated. This has two results: the node status tree is not kept up to date properly and the SQL is tried every 10 seconds. The Tivoli Enterprise Portal Server appears to freeze.
IY95863	Migrate-Export fails to export large tables. A NoMoreData exception is caught in KfwSQLClient.exe, and the process exits. There's no obvious reason for the exception.
IY97382	The Tivoli Enterprise Portal Server might result in a crash and core dump when multiple users aggressively navigate to workspaces in similar parts of a Tivoli Enterprise Portal navigator, resulting in memory corruption. This problem will appear as either a hang or as visual corruption of the navigator on Windows.
IY97664	The Tivoli Enterprise Portal Server repeatedly issues a SELECT statement against the INODESTS table that contains a syntax error. The parse failure results in a memory leak and eventually all available storage is consumed resulting in a Tivoli Enterprise Monitoring Server crash.

Tivoli Data Warehouse APARs

The following APARs are addressed in Fix Pack 005:

APAR Number	Symptom
IY92548	The Tivoli Data Warehouse proxy agent uses 100% of its CPU if the database is stopped.
IY93058	Historical data is not inserted into Tivoli Data Warehouse tables when the Warehouse Proxy Agent is installed on a machine with a locale environment variable that changes the format of a decimal and replaces a period by a coma (such as Germany or France).
IY93509	The Warehouse Proxy Agent is not registered anymore and data cannot be inserted in the warehouse database.
IY93667	SQL Error ORA-12899 "value too large for column" is generated for the ″ITMUSER,″ ″WAREHOUSEMARKER, and .″ORIGINNODE″ columns when the Summarization and Pruning Agent is run against IBM Tivoli Monitoring Agents and ITCAM agents. The maximum values is 64.
IY95649	The Warehouse Proxy agent fails when the user attempts to insert data into the Tivoli Data Warehouse with the error ″[IBM][CLI Driver] CLI0109E or the Warehouse proxy terminates abnormally.

i5/OS OS monitoring agent APARs and defects

The following APARs are addressed in Fix Pack 005:

APAR Number	Symptom
IY90139	Situations created on OS400 Security Audit journal attributes stop triggering when the journal receiver becomes full and new journal receiver is attached to the journal. This also happens when a new journal receiver attached using CHGJRN command. This is also true for the situations created on Accounting journal attributes.
IY91992	When configuring the i5/OS OS monitoring agent V5R4M0, pressing **Enter** to save all parameters causes this error to be displayed: `Application error. MCH3601 unmonitored by KFPCOM at statement 0000000006.`

Linux OS monitoring agent APARs

The following APARs are addressed in Fix Pack 005:

APAR Number	Symptom
IY91006	The Processor Configuration Information worksapce in the Linux OS agent running on z/OS does not display any data.
IY92337	When defining Linux OS situations in the Situation Editor with attribute value, the value, even if it is valid, will turn red and prevent the situation from being saved.

Universal Agent APARs

The following APARs are addressed in Fix Pack 005:

APAR Number	Symptom
IY89541	When using the Socket data provider , a universal agent application experiencing frequent change between online and offline status may omit data rows from Tivoli Enterprise Portal universal agent workspace (report). The universal agent trace log will contain recurrence of a message that reads `*** dp_data failed. DCH synchronization required`.
IY91963	REXX™ SOCKET calls from ISPF running z/OS (1.7) to Universal Agent 6.10.03 do not always post data in the Tivoli Enterprise Portal Server but does create an entry with all fields blank. The first record is not getting translated from EBCDIC to ASCII.
IY92509	When the network is disconnected between the universal agent and the Tivoli Enterprise Monitoring Server, the universal agents write error messages continuously and consuming high CPU and Disk I/O.
IY94220	With the universal agent, only one managed system occurs in the Managed Systems List, and only one log file is monitored.
IY94579	When the Universal Agent is started or restarted from the Tivoli Enterprise Portal, the label is incorrect.
IY95185	When declaring a //SOURCE ODBC in a Universal Agent metafile that defines a user or password containing special character '@', the universal agent will receive a a SQL connection error due to invalid UserName of Password. As a result the SQL query will fail to execute.
IY95360	When a user adds the `KUMP_SNMP_MONITOR_TRAP=Y` statement to the um.ini file, the universal agent fails after 1-2 minutes.
IY95724	The universal agent fails when the SNMP data provider receives a SNMP version 3 trap.

UNIX Log Agent APARs

The following APARs are addressed in Fix Pack 005:

APAR Number	Symptom
IY92338	The description for syslog on Tivoli Enterprise Portal is truncated.

UNIX OS monitoring agent APARs

The following APARs are addressed in Fix Pack 005:

APAR Number	Symptom
IY87476	The UNIX OS monitoring agents aggregate values are different from the values that the system graphs are returning. IBM Tivoli Monitoring is calculating the value instead of having agent dialogs report it, indicating that the ″idle″ column in the ″ALL″ line from the mpstat command shomehow uses the ″%ec″ (processor % entitlement) as part of its calculation.
IY89018	The IBM Tivoli Monitoring Version 6.1 UNIX OS monitoring agent does not display the correct number of CPUs when CPUs are re-assigned “on the fly.”
IY91092	The Tivoli Enterprise Portal Server does not display disk performance data on HP-UX systems that have more than 1000 disks.
IY93478	The UNIX OS monitoring agent on AIX reports an incorrect Process CPU percent (CPU%) value.

Windows OS monitoring agent APARs

The following APARs are addressed in Fix Pack 005:

APAR Number	Symptom
IY88066	In the IBM Tivoli Monitoring Version 6.1 Windows OS Agent, situations do not filter out the _Total data row, causing false events triggered by the _Total row.
IY91280	When monitoring a process using the Windows OS agent, the Processor Time (%) of the process is over 100%. This value represents the sum of all the user's processors instead of an average.

Appendix. 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:

IBM World Trade Asia Corporation
Licensing
2-31 Roppongi 3-chome, Minato-ku
Tokyo 106, 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.

© Copyright IBM Corp. 2007

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.

Trademarks

IBM, the IBM logo, AIX, AS/400, Candle, CICS, DB2, i5/OS, iSeries, NetView, OMEGAMON, OMEGAMON II, OS/400, Passport Advantage, pSeries, REXX, System p, Tivoli, the Tivoli logo, Tivoli Enterprise, Tivoli Enterprise Console, z/OS, and zSeries are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both.

Java and all Java-based trademarks and logos are trademarks or registered trademarks of Sun Microsystems, Inc. in the United States, other countries, or both.

Intel and Itanium are trademarks of Intel Corporation in the United States, other countries, or both.

Linux is a trademark of Linus Torvalds in the United States, other countries, or both.

Microsoft, Windows, and Windows NT are registered trademarks of Microsoft Corporation in the United States, other countries, or both.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Other company, product, and service names may be trademarks or service marks of others.

Printed in USA

SC23-5960-00