Tivoli® IBM Tivoli Monitoring

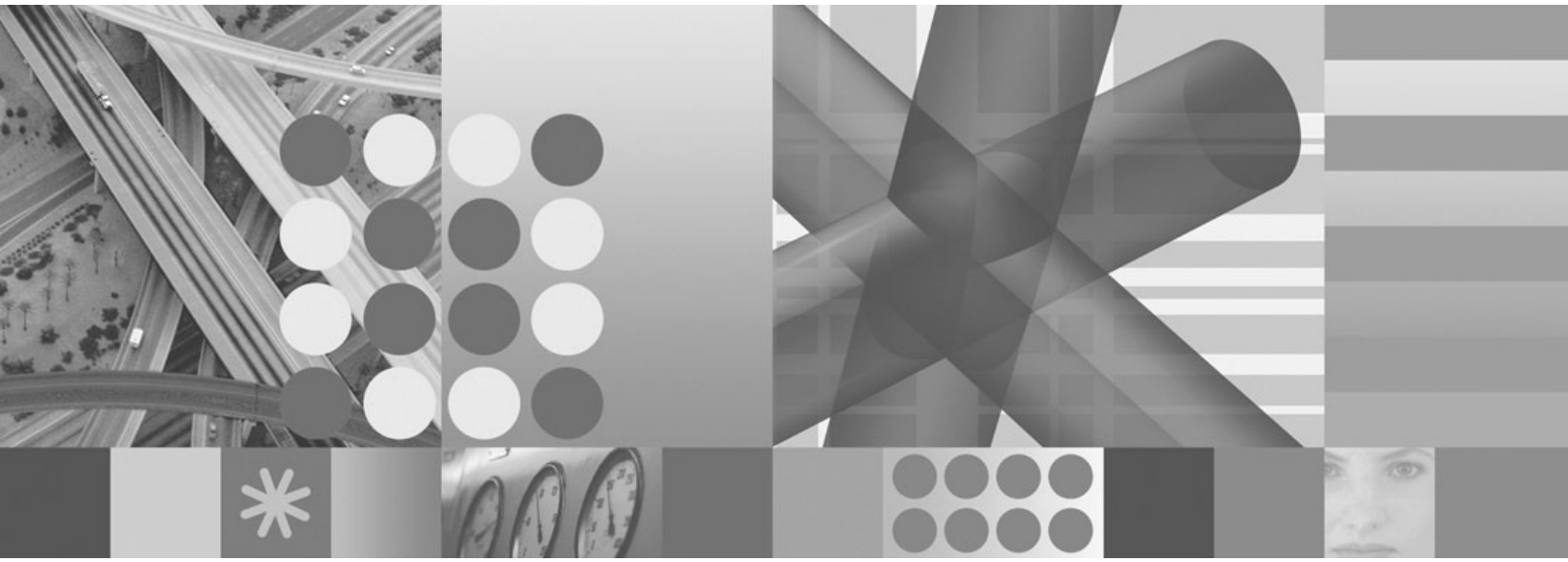
Version 6.1

Fix Pack 004 Readme and Documentation Addendum

GI11-8053-00

Tivoli® IBM Tivoli Monitoring

Version 6.1



Fix Pack 004 Readme and Documentation Addendum

GI11-8053-00

Note
Before using this information and the product it supports, read the information in Appendix C, "Notices," on page 83.

First edition (December 2006)

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.

Contents

Chapter 1. Fix Pack 004 overview

Fix Pack 004 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.

Note: Fix Pack 004 is an IBM Tivoli Monitoring V6.1 Enterprise level fix pack. Fix Pack 004 is not intended for IBM Tivoli Monitoring Express V6.1 installations.

You can download the IBM Tivoli Monitoring, Fix Pack 004 fix pack files from Passport Advantage® or from the IBM Software Support Web site. The files listed in Table 1 are available on the IBM Software Support Web site. See the *IBM Tivoli Monitoring Passport Advantage Readme First* for details on fix pack file names and downloading the files from Passport Advantage.

Table 1. Fix Pack 004 file names

Fix pack file name	Platform
6.1.0-TIV-ITM_TMV-Windows-FP0004.zip	Windows® platforms
6.1.0-TIV-ITM_TMV-AIX-FP0004.tar	UNIX® platforms - AIX®
6.1.0-TIV-ITM_TMV-HPUXPARISC-FP0004.tar	UNIX platforms - HP-UX Integrity, HP-UX native processors
6.1.0-TIV-ITM_TMV-Solaris-FP0004.tar	UNIX platforms - Solaris
6.1.0-TIV-ITM_TMV-LinuxIA64-LinuxX64-FP0004.tar	Linux® on Intel® Itanium® and AMD Opteron 64-bit processors
6.1.0-TIV-ITM_TMV-Linuxip-FP0004.tar	Linux on pSeries®
6.1.0-TIV-ITM_TMV-Linuxz-FP0004.tar	Linux on zSeries®
6.1.0-TIV-ITM_TMV-LinuxIA32-1-FP0004.tar	Linux Intel platforms (Part 1 of 2)
6.1.0-TIV-ITM_TMV-LinuxIA32-2-FP0004.tar	Linux Intel platforms (Part 2 of 2)

See Chapter 2, “Installation instructions,” on page 15 for detailed installation procedures.

Note: If you are running your monitoring server on a z/OS® system, be sure to check for the z/OS Fix Pack 004 PTF, available from IBM Software Support. For information about installing the monitoring server on z/OS, see the Program Directory that comes with that product.

What’s new in this fix pack

The following new functions have been added to IBM Tivoli Monitoring in this fix pack:

Note: The new functions listed below are available in all languages, although they are displayed in English only. Although the interfaces for these functions are English-only, the functions themselves work in all locales. The interfaces will be translated in the next release of IBM Tivoli Monitoring.

- Support for a fix pack upgrade installation through an image refresh that eliminates the need to install individual component fix packs.
- Installing the fix pack on all computers where you are running the Warehouse Proxy agent and the Summarization and Pruning agent provides enhancements to reduce the disk space requirements for the Tivoli Data Warehouse. Specifically, the Warehouse Proxy Agent now trims all trailing whitespace data for character data that it inserts into VARCHAR columns in the Tivoli Data Warehouse.
- A new command for installing support for the upgrade toolkit on Solaris computers. See "Installing the upgrade toolkit on Solaris computers" on page 46 for details.
- Enhancements to Topology view properties. Configuring the threshold number of objects in the topology view before it switches automatically to a table view is done in the Properties editor. The view also has a Style tab for formatting the view, objects, labels, and connector lines.
- Network interface list for z/OS. If your site runs more than one TCP/IP interface or network adapter on the same z/OS image, you can now specify network interfaces to be used by the monitoring server on z/OS and by a monitoring agent installed in a separate address space from the monitoring server. You specify the network interfaces in the Configuration Tool panels for IP communication protocol parameters for each component. The Configuration Tool then generates the KDEB_INTERFACE parameter in members KDSENV (for the monitoring server) and K*pp*ENV, where *pp* is the monitoring agent, of the RKANPARU library. See "Network interface list" on page 63 for details.
- Take-Action authorization and command execution through Netview. You can now configure a Tivoli Enterprise Monitoring Server or monitoring agent address space to redirect z/OS Take Action commands to NetView® through the Program to Program Interface (PPI). NetView uses the Tivoli Enterprise Portal user ID to check command authorization. If the user ID is authorized, the command is issued and the response is logged in the NetView Netlog. See "Take-Action command authorization and execution through NetView" on page 63 for details.

The following functions were added to IBM Tivoli Monitoring in a previous fix pack:

- Enhancements to the Tivoli Enterprise Console® event viewer. You can now launch the Situation event results workspace directly from the Tivoli Enterprise Console event viewer.
- Dynamic workspace linking. A new link type has been added to the workspace link feature that enables the link author to identify the target workspace by the host identifier. The dynamic link type adds more opportunities for workspace linking, such as to provide links to workspaces of other types of monitoring agents. For detailed information on using this new function, see the ″New in this release″ help topic in the Tivoli Enterprise Portal online help.
- Ability to create a topology view in the Tivoli Enterprise Portal. For monitoring products that support the topology view, you can add the view to a workspace to graphically show objects and their logical relationships to one another. For detailed information on using this new function, see the ″New in this release″ help topic in the Tivoli Enterprise Portal online help.
- TMS Infrastructure view. The Tivoli Enterprise™ Monitoring Server has a topology view called TMS (Tivoli Monitoring Services) Infrastructure view, which visually expresses the relationships and linking of monitoring agents and other components to the hub monitoring server.

Note: The TMS Infrastructure view has moved from the Managed System Status workspace to a new workspace, the Self Monitoring Topology workspace. For detailed information on using this new function, see the ″New in this release″ help topic in the Tivoli Enterprise Portal online help.

- Additional hyperlinks can be added to the Event Tools view (part of the event management enhancements). These links can be pointers to Web sites, as well as mechanisms for launching applications on the client computer. The links are defined in the eventtools.htm file, located in the *ITMinstall_dir*/cnb directory, where *ITMinstall_dir* is the directory where you installed IBM Tivoli Monitoring. To add new hyperlinks or to modify existing hyperlinks, open the eventtools.htm file in a text editor. Instructions for editing the hyperlinks are contained in this file as comments.
- Ability to link from a situation event in the embedded IBM Tivoli Enterprise Console event console to the Event Results workspace in the Tivoli Enterprise Portal. To use this new function, right-click a situation event from inside the IBM Tivoli Enterprise Console event console and click **ITM Situations → Situation Results**.
- Enhanced ease of adding new views within the Tivoli Enterprise Portal. See the online help in the Tivoli Enterprise Portal for information.
- Enhanced firewall functionality through the use of a gateway feature. For information about this function, see the ″Firewall Gateway Feature″ document in the IBM Tivoli Monitoring information center (located at http://publib.boulder.ibm.com/infocenter/tivihelp/v3r1/index.jsp?toc=/com.ibm.itm.doc/toc.xml).
- The Linux OS agent has added Linux File and Directory monitoring which includes file information attributes to refer to file information characteristics. The File Information workspace shows a list of files and directories on your file system. The default directory shown is the root (/) directory.
- The UNIX OS agent has added AIX Printer Queue Support monitoring, as well as the ability to monitor disk attributes (such as available free space) in megabytes and gigabytes (instead of kilobytes).
- Increased default security for the Tivoli Enterprise Portal on Windows computers.

  When you are installing the full media that contains the fixes in IBM Tivoli Monitoring V6.1 Fix Pack 003 and related agent fix packs, there is a new requirement to type a Tivoli Enterprise Portal Server sysadmin password. You are prompted for this new password during installation. For silent installations, you can set the SYSADMINPWSD=value in the response file. A Windows ID, sysadmin, is created.

  The password is required *only* for fresh installations on Windows (not on Linux). Any upgraded installations continue to function in the same way as the installation from which you are upgrading. Because the password is verified by the Windows operating system, you must create a password that conforms to any Windows password rules. The sysadmin ID must also conform to account policies on the computer where the software is installed.
- The IBM Tivoli Monitoring IBM Tivoli Enterprise Console event synchronization installation wizard has been updated to provide the option to automatically stop and restart your event server. In previous releases, you had to do this manually. For information about installing the event synchronization fix pack that enables this change, see “Installing the IBM Tivoli Enterprise Console event synchronization fix pack” on page 38.

  If you are installing the event synchronization for the first time (instead of updating an existing installation), use the installation instructions provided in

"Chapter 6: Installing the IBM Tivoli Enterprise Console event synchronization" in the *IBM Tivoli Monitoring Installation and Setup Guide*. This document is available in the IBM Tivoli Monitoring information center at http://publib.boulder.ibm.com/infocenter/tivihelp/v3r1/index.jsp?toc=/com.ibm.itm.doc/toc.xml.

See the latest refreshed version of the *IBM Tivoli Monitoring Installation and Setup Guide* for installation and configuration details on the following functions that were added to IBM Tivoli Monitoring in a previous fix pack:

- Support for the Tivoli Enterprise Portal Server on AIX version 5.3.
- Support for the Warehouse Proxy on AIX version 5.3.
- Support for accessing and displaying data from an Oracle database for your Tivoli Data Warehouse when you are running the Tivoli Enterprise Portal Server on a Linux computer.
- A new utility, secureMain, has been added to change the file permissions level for files on Linux and UNIX computers. After initial installation, many files have a 777 permission level. The secureMain script enables you to easily change these permissions.
- Support for the Warehouse Proxy on Linux operating systems.
- Support for multiple Warehouse Proxy agents in a single monitoring environment.
- A Discovery Library adapter (DLA) for use in a configuration management database (CMDB), such as IBM Tivoli Change and Configuration Management Database. The DLA scans the IBM Tivoli Monitoring environment and identifies the managed systems in the environment. You can then feed this information into IBM Tivoli Change and Configuration Management Database or another CMDB.

See the refreshed version of the *IBM Tivoli Monitoring Administrator's Guide* for configuration details on the following functions that were added to IBM Tivoli Monitoring in a previous fix pack:

- Enhancements to event management through the Tivoli Enterprise Portal. You can now add more detailed note information, as well as attach files, to individual events. A new user permission has been added to enable users to attach files. Also, the way that events are acknowledged has also been improved. For detailed information on using these new functions, also see the "New in this release" help topic in the Tivoli Enterprise Portal online help.
- For the Tivoli Enterprise Portal, the HTTP proxy server parameters have been removed from the Configure Tivoli Enterprise Portal Browser window, and the instructions in the *IBM Tivoli Monitoring Administrator's Guide* to Enable the HTTP Proxy Server for the browser client are no longer valid.
- For the Tivoli Enterprise Portal, when you have security enabled, you can now control the number of log in attempts before a user is locked out of the portal.

See the *IBM Tivoli Monitoring Command Reference Guide* for details on the following functions that were added to IBM Tivoli Monitoring in a previous fix pack:

- Support for importing and exporting workspaces from the Tivoli Enterprise Portal through the command-line interface. You can now easily use a set of commands to export a workspace from one system to another, reducing the amount of time you need to spend customizing your monitoring environment. For information about the commands that enable this function, see "Appendix E: Command reference".

- Support for creating managed system lists (a defined set of managed systems) through the command-line interface. You can create your own managed system lists for any grouping of managed systems and apply them to the following tasks:
  - The distribution of a situation
  - The distribution for policies correlated by business application group
  - Managed system assignments for queries
  - Managed system assignments for Navigator items in custom Navigator views

  For information about the new commands that enable this function, see "Appendix E: Command reference".

See the refreshed version of the *IBM Tivoli Monitoring i5/OS® Agent User's Guide* for details on added support for using the SSL communication protocol for communication between the i5/OS agent and the monitoring server that was added to IBM Tivoli Monitoring in a previous fix pack.

In addition a number of customer APARs are addressed in this fix pack. See Appendix B, "APARs addressed by this fix pack," on page 67 for details.

Supported operating systems

Fix Pack 004 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 has been added in this fix pack is marked with **bold** highlighting.

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

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 2003 SE (64 bit)				X		
Windows 2003 EE (64 bit)				X		
Windows 2003 Server on Itanium2				X		
Windows 2003 on VMWare ESX Server V2.5.2	X	X	**New**	X	X	X
Windows Vista (32 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.
2. The **OS monitoring agent** column indicates the platforms on which an operating system monitoring agent is supported. It 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).

Table 3 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

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[3]	X			X[4]	`	
HP-UX 11i v1 (B.11.11) and HP-UX 11i v2 (B.11.23) (32/64) on PA-RISC[5]				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	X			X		
z/OS 1.6	X			X		
z/OS 1.7	X			X		

Table 3. Supported UNIX, i5/OS, and z/OS operating systems (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. It 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 3, "Known problems and limitations," on page 51 for details on installing this framework.
3. The monitoring server 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 OS agents on this operating system. This 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, see 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 004 does not support remote deployment for HP-UX 11i v2 on Integrity computers.
   - You can not upgrade either the OS or Log Alert agents that you currently have running on a HP-UX 11i v2 (B.11.23) on Integrity (IA64) computer in PA-RISC mode to Fix Pack 004, where these agents run in native 64-bit mode by default. You must first uninstall the previous version of these agents and then install the Fix Pack 004 versions.
9. HP-UX 11i v2 (B.11.23) on Integrity (IA64) native 64-bit support is new for Fix Pack 004.

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

Table 4. Supported Linux operating systems

Operating system	Monitoring server	Portal server	Portal client[1]	OS monitoring agent[2]	Warehouse Proxy	Warehouse Summarization and Pruning agent
Red Flag 4.1 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
RedHat Enterprise and Desktop Linux 4 Intel	X	X	X	X	X	X
RedHat Enterprise Linux 4 on AMD64/EM64T[3]				X		
RedHat Enterprise Linux 4 on Itanium 64-bit				X		
RedHat Enterprise Linux 4 on iSeries™ and pSeries[4]				X		
RedHat Enterprise Linux 4 on z/Series 31-bit	X	X		X	X	X
RedHat Enterprise Linux 4 on zSeries 64-bit	**New**[7]	**New**[7, 9]		X	X	X
RedHat Enterprise Linux 4 for Intel on VMWare ESX Server V2.5.2	X	X	**New**	X	X	X
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[5]				X		
SUSE Linux Enterprise Server 9 on Itanium 64-bit[6]				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	**New**[7]	**New**[7, 9]		X	X	X
SUSE Linux Enterprise Server 10 Intel	**New**	**New**	**New**	**New**	**New**	**New**

Table 4. Supported Linux operating systems (continued)

Operating system	Monitoring server	Portal server	Portal client[1]	OS monitoring agent[2]	Warehouse Proxy	Warehouse Summarization and Pruning agent
SUSE Linux Enterprise Server 10 on AMD64/EM64T[8]				**New**		
SUSE Linux Enterprise Server 10 on Itanium 64-bit[6, 8]				**New**		
SUSE Linux Enterprise Server 10 for iSeries and pSeries[8]				**New**		
SUSE Linux Enterprise Server 10 for z/Series 64-bit[8]	**New**[7]			**New**	**New**	**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.
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. For RedHat Enterprise Linux 4 on AMD64/EM64T, you must install the following libraries:
   libstdc++.so.5
   libstdc++.so.5(CXXABI_1.2)
   libstdc++.so.5(GLIBCPP_3.2)
   libstdc++-3.4.3-9.EL4
   libgcc-3.4.4-2.i386.rpm
   libstdc++-3.4.4-2.i386.rpm
   compat-libstdc++-33-3.2.3-47.3.i386.rpm
   compat-libstdc++-296-2.96-132.7.2.i386.rpm
4. For RedHat Enterprise Linux 4 on System p™, you must install the following libraries. These libraries are available on the RedHat Enterprise Linux operating system installation media.
   libgcc-3.4.5-2.ppc64.rpm
   libstdc++-3.4.5-2.ppc64.rpm
   compat-libstdc++-33-3.2.3-47.3.ppc64.rpm
   compat-libstdc++-33-3.2.3-47.1.ppc.rpm
5. For SUSE Linux Enterprise Server 9 on AMD64/EM64T, you must install the compat-libstdc++-lsb-4.0.2_20050901-0.4.x86_64.rpm library. This library is available in the SUSE Linux Enterprise Server 9 for AMD64 and Intel EM64T Service Pack 3.
6. You cannot use the remote deployment function for the OS agent on this operating system. This 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.
   ```
7. This component supports the operating system in 64-bit tolerance mode.
8. See Technote 1247529 for minor known problems and workarounds for SUSE Linux Enterprise Server 10 on 64-bit operating systems.
9. 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.

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 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, V8.2 with Fix Pack 3 or higher fix packs, and V9.1 and fix packs.	
Linux	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.	
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 is **New**.		

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 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 MS SQL 2005	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

Table 6. Supported databases for the Tivoli Data Warehouse (continued)

Tivoli Data Warehouse database ("WAREHOUS")		
IBM DB2[1]	**MS SQL**	**Oracle[2]**
• "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 is **New**. 2. See the Oracle company support Web site (www.oracle.com) for information about installing and configuring Oracle on Solaris V10.		

Memory and disk requirements

The following tables show estimated memory and disk storage for IBM Tivoli Monitoring components on distributed systems, OS agents, and UNIX Log Agent.

IBM Tivoli Monitoring components on distributed systems

The following table shows estimated memory and disk storage for IBM Tivoli Monitoring components on distributed systems.

Table 7. Estimated memory and disk storage for IBM Tivoli Monitoring components on distributed systems

Component	Process memory requirements[1]		Disk storage requirements[4]
	Small environment[2]	Large environment[3]	
Hub monitoring server	70 MB	100 MB	650 MB[5]
Remote monitoring server	100 MB	300 MB	250 MB[5]
Portal server	100 MB[6]	300 MB[6]	800 MB
Portal client (browser or desktop)	150 MB	300 MB	150 MB
Tivoli Data Warehouse	2 - 4 GB depending on database configuration parameters	4 - 8 GB depending on database configuration parameters	See the *IBM Tivoli Monitoring Installation and Setup Guide* for details on estimating the size of your database.
Warehouse Proxy agent	50 MB	100 MB	150 MB
Summarization and Pruning agent	150 MB	300 MB	150 MB

Table 7. Estimated memory and disk storage for IBM Tivoli Monitoring components on distributed systems (continued)

Component	Process memory requirements[1]		Disk storage requirements[4]
	Small environment[2]	Large environment[3]	

Notes:

1. The memory and disk sizings shown in this table are the amounts required for the individual component beyond the needs of the operating system and any concurrently running applications.
2. A small environment is considered to be a monitoring environment with 500 to 1000 agents, with 100 to 200 monitored agents per remote monitoring server.
3. A large environment is considered to be a monitoring environment with 3000 or more monitored agents, with 500 to 1000 monitored agents per remote monitoring server.
4. The disk storage estimates apply to any size monitoring environment and are considered high estimates. The size of log files affect the amount of storage required.
5. The storage requirements for the hub and remote monitoring servers do not include storage for the agent depot, which can require an additional 1 GB or more.
6. The memory requirement for the portal server does not include database processes for the portal server database, which require up to 400® MB of additional memory, depending on configuration settings.

Add the sizings for individual components to calculate a total for more than one component installed on the same computer.

For example, if the hub monitoring server and portal server are installed on the same computer in a small monitoring environment, the initial requirement is 170 MB of memory and 900 MB of disk space beyond the needs of the operating system and other applications. If you add 400 MB of memory for the portal server database and 1 GB of storage for the agent depot, the total requirement for IBM Tivoli Monitoring components comes to 570 MB of memory and 1.9 GB of storage.

IBM Tivoli Monitoring OS agents and UNIX Log Agent

The following table shows estimated memory and disk storage for IBM Tivoli Monitoring OS agents and UNIX Log Agent. See the OS agent and UNIX Log Agent User's Guides located in the IBM Tivoli Monitoring information center for details on disk capacity planning for historical data.

Table 8. Estimated memory and disk storage for IBM Tivoli Monitoring OS agents and UNIX Log Agent

Agent	Process memory requirements	Disk storage requirements
i5/OS Agent		100 MB disk space for the monitoring agent
Linux OS Agent	256 MB RAM at a minimum although 512 MB or higher for better performance	100 MB of disk space for the monitoring agent
UNIX Log Agent	128 MB RAM at a minimum, 512 MB or higher for better performance	30 MB of disk space (100 MB for Linux)
UNIX OS Agent	256 MB RAM at a minimum although 512 MB or higher for better performance	164 MB of disk space for the monitoring agent
Windows OS Agent	• 32 MB RAM • 150 MB virtual memory, plus 5 MB for each agent installed	• 70 MB disk space for the monitoring agent • 5 MB to 600 MB disk space for historical data collection

Chapter 2. Installation instructions

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

Table 9. Overall installation steps for Fix Pack 004

Goal	Where to find information
Ensure your monitoring environment is prepared for fix pack installation.	"Before you install the fix pack"
Gather the information you need to perform the installation.	"Fix pack installation planning worksheets" on page 19
Update your monitoring server.	"Monitoring server checklist" on page 25
Update your portal server.	"Portal server checklist" on page 28
Update your portal desktop clients.	"Portal desktop client checklist" on page 30
Update your remote monitoring servers.	"Monitoring server checklist" on page 25
Update your local monitoring agents.	"Monitoring agent checklist - local installation" on page 32
Remotely update other monitoring agents.	"Monitoring agent checklist - remote installation" on page 33
Update your local i5/OS OS agents, if applicable.	"Installing the fix pack for the i5/OS monitoring agent" on page 35
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 38

Before you install the fix pack

Notes:

1. Security is required for the Tivoli Enterprise Portal on Windows computers. You will be required to type a Tivoli Enterprise Portal Server sysadmin password during installation. See the section on functions that were added to IBM Tivoli Monitoring in a previous fix pack in "What's new in this fix pack" on page 1 for additional information.
2. The fix pack might include modifications to product-provided situations. These changes are not merged automatically. While the changes are included, the updates fail and error messages are displayed when you install the application support. The changes made to each agent's situations are listed in the agent component readme. You can edit your situations, using the change descriptions provided in the agent component readmes, to merge the changes. For more information on editing a situation, see the "Customizing a situation" section of Chapter 10, "Situations for event-based monitoring" in the *IBM Tivoli Monitoring User's Guide*.
3. Language support is available only on the platforms that were supported for IBM Tivoli Monitoring V6.1 GA.

Perform the following before you install this fix pack:

- For UNIX computers, you must close Manage Tivoli Enterprise Monitoring Services before you upgrade to Fix Pack 004.

- The Eclipse Help server is not available on AIX computers. If you do not install the Eclipse Help server, the **IBM Eclipse Help System** link is broken for monitoring agents helps that have the **Searching Agent Help** topic. You must use the following steps to install the Eclipse Help server *before* you install your monitoring agents.
  1. Use the following Web site to download the Eclipse Help server: http://publib.boulder.ibm.com/infocenter/tivihelp/v15r1/topic/com.ibm.itm.doc/Eclipse30Unix.tar.
  2. Untar the tar file in the *itm_installdir* directory.
  3. Run the IC_start.sh file to start the Eclipse Help server. The IC_start.sh file is located in the *itm_installdir* helpsvr directory where you extracted the Eclipse30Unix.tar file.
- 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 004.
- 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 9 for details.
- *Note that you must upgrade the Tivoli Enterprise Portal Server and the Tivoli Enterprise Portal desktop and browser clients to the same fix pack level*. Also consider upgrading all base monitoring components, per hub, to the same fix pack level. For example, upgrade 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. The hub monitoring server and monitoring agents do not need to be at the latest fix pack level - you can continue to use an older hub monitoring server and monitoring agents in your upgraded environment, although you might consider upgrading as soon as possible to take advantage of new functions and fixes that are available.
- Any prerequisite fix packs or other software must be installed for the fix pack you are going to install.
- Note regarding re-adding application support for agents: During the installation of this fix pack, or during future agent upgrades, you might be presented with a list of agents for which to add application support to the monitoring server. Use caution when you select those agents for which to add support, as any customizations you've made to situations can be lost during this process. During the installation of this fix pack, add application support for *only* the OS agents and the UNIX Log agent. This prevents the loss of customizations to other agents. During future agent upgrades and new agent installations for this monitoring server, add application support for only those agents that you are upgrading or adding.
- 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.
- 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.

1. Log into the computer as *user_id*.
2. Run the following command to change ownership of any root owned files to *user_id*:

   ```
   su - root -c "ITMinstall_dir/bin/UnSetRoot user_id"
   ```

3. Install the fix pack on the computer, following the steps outlined in the checklists.
4. Run the following command to reset the file permissions and file ownership as required:

   ```
   su - root -c "ITMinstall_dir/bin/SetPerm -a"
   ```

- 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 without any parameters.
- 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.
- If you are running IBM Tivoli Monitoring in a globalized environment, for best results, after you apply a fix pack and reconfigure any components, re-install the base IBM Tivoli Monitoring language packs and any agent language packs.

  Note: This requirement also applies if you reconfigure any of the base components, such as the portal server.
- If you are installing Fix Pack 004 in an IBM Tivoli Monitoring environment that is running with a Japanese language pack and you do not want to reinstall the Japanese language pack (as described above) or you have reconfigured the portal server (for example, after adding agent application support files), you must perform the following steps prior to installing the fix pack or after reconfiguring:
  - Perform the following procedure for a portal server on Windows or Linux. If you do not, the browser client and all associated messages are displayed in English, instead of Japanese.
    1. Stop the portal server.
    2. Make a copy of the applet.html file (in the *<itm_install>*/*<platform>*/cw directory on Linux or the *<itm_install>*/CNB directory on Windows.
    3. Install the portal server fix pack.
    4. Edit both the pre-upgrade and post-upgrade versions of the applet.html file.
    5. In the pre-upgrade version, locate the lines regarding the *xxx*_ja.jar files. For example:

       ```
       -----
       document.writeln( '<!-- JARLIST: kjrall.jar, cnp.jar, ae.jar -->' );
       document.writeln( '<PARAM NAME = CACHE_ARCHIVE VALUE="cnp_vbjorball.jar,
       kjrall.jar,   util.jar, cnp.jar, chart.jar, ae.jar, cnp_jviewsall.jar,
       terminal.jar, browser.jar, icu4jm32.jar, deploy.jar, lp_ja.jar, kit_ja.jar,">' );
       ```

```
document.writeln( '<PARAM NAME = CACHE_VERSION VALUE="6.5.0.7, 7.610.6173.a,
2.2.8.9,  7.610.6173.a, 2.2.2.6, 7.610.6173.a, 5.2.5.B, 3.0.4.4, 6.0.1.5, 1.0.0.0,
7.4.A.C, 0.0.1.2, 0.0.1.2,">' );
-----
```

6. Add these .jar file names to the post-upgrade version of the applet.html file.
7. Add any version numbers associated with the .jar files.
8. Save and close the applet.html files.
9. Restart the portal server.

– Perform the following procedure for a portal desktop client running on Linux:

1. Search for any *_ja.jar files in the *ITM_installDir*/*platform*/cj/lib directory. Make a list of these files.
2. Edit the *ITM_installDir*/*platform*/cj/original/cnp.sh_template file.
3. Locate the CLASSPATH entry in this file and add any *_ja.jar files identified in Step1.

   For example:

   ```
   CLASSPATH=|CANDLEHOME|/JRE/|BINARCH|:.......:${KCJ_LIB}/lp_ja.jar:${KCJ_LIB}\
   /kit_ja.jar
   ```

4. Reconfigure the portal desktop client by running the following command:

   ```
   ./itmcmd config -A cj
   ```

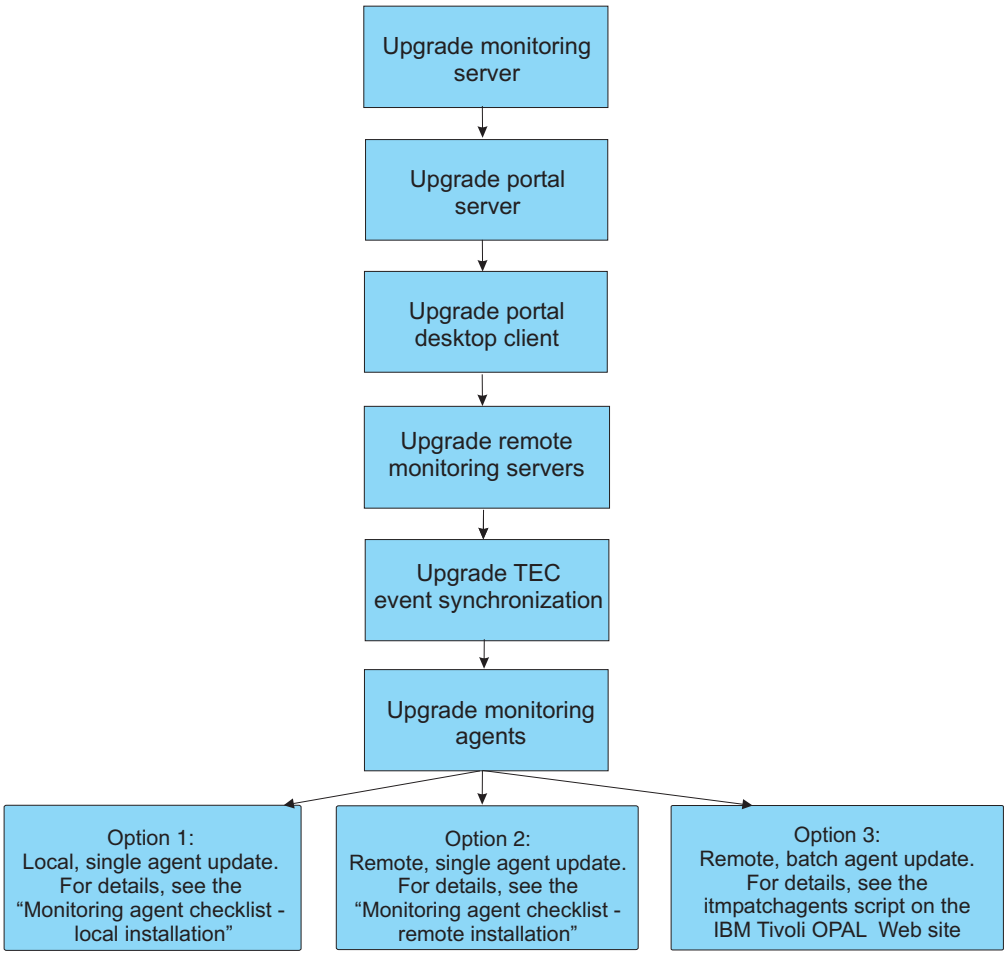
Installation checklists

The following checklists provide the installation steps for upgrading the IBM Tivoli Monitoring components.

Notes:

1. If your Warehouse Proxy agent or Summarization and Pruning agent are on machines other than the monitoring server or portal server, use the instructions in the "Monitoring agent checklist - local installation" on page 32 to install the updates.
2. These checklists provide the order and procedures for installing the fix pack.

Install your environment in the following order:



You can use the "Fix pack installation planning worksheets" to gather the information required for the installation.

Note: 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.

Fix pack installation planning worksheets

Use the following worksheet 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.

Table 10. 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	"Monitoring server checklist" on page 25	
Remote monitoring server host name	Portal server Portal desktop client Warehouse Proxy Summarization and Pruning agent	Manage Tivoli Enterprise Monitoring Server	"Monitoring server checklist" on page 25	
Remote monitoring server host name	Portal server Portal desktop client Warehouse Proxy Summarization and Pruning agent	Manage Tivoli Enterprise Monitoring Server	"Monitoring server checklist" on page 25	
Remote monitoring server host name	Portal server Portal desktop client Warehouse Proxy Summarization and Pruning agent	Manage Tivoli Enterprise Monitoring Server	"Monitoring server checklist" on page 25	
Remote monitoring server host name	Portal server Portal desktop client Warehouse Proxy Summarization and Pruning agent	Manage Tivoli Enterprise Monitoring Server	"Monitoring server checklist" on page 25	
Remote monitoring server host name	Portal server Portal desktop client Warehouse Proxy Summarization and Pruning agent	Manage Tivoli Enterprise Monitoring Server	"Monitoring server checklist" on page 25	
Portal server host name	Monitoring server Portal desktop client Warehouse Proxy Summarization and Pruning agent	Manage Tivoli Enterprise Monitoring Server	"Portal server checklist" on page 28	

Table 10. 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	"Portal desktop client checklist" on page 30	
Warehouse Proxy agent location	Monitoring server Portal server Portal desktop client Summarization and Pruning agent	Manage Tivoli Enterprise Monitoring Server	"Monitoring server checklist" on page 25 "Portal server checklist" on page 28	
Warehouse Summarization and Pruning agent location	Monitoring server Portal server Portal desktop client Warehouse Proxy	Manage Tivoli Enterprise Monitoring Server	"Monitoring server checklist" on page 25 "Portal server checklist" on page 28	
Agent types to update (product codes)		**tacmd listSystems**	"Monitoring server checklist" on page 25 "Monitoring agent checklist - local installation" on page 32	

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

Table 11. 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)	

Quick installation checklist

The following checklist provides the fix pack installation steps for installing all components on a local host computer.

Notes:

1. The installation procedures are the same as used for the GA level installation. For detailed installation procedures, see Chapter 5, "Installing IBM Tivoli Monitoring" in the *IBM Tivoli Monitoring Installation and Setup Guide*.
2. Only hub monitoring servers support SOAP servers.
3. If you are installing agents from a CD for HP-UX computers, you must use the procedure described in "Mounting a CD drive on HP-UX" on page 44 to mount your CD.

Table 12. 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 19.
	2. Based on the platform of your local host computer, download and extract the necessary fix pack files to a temporary location on your computer. You can use the space below 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`
	From the component list, select only the components that you have previously installed for upgrade. **Note:** Reconfiguration is required. 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. 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.

Table 12. Checklist for installing the fix pack on a local host computer (continued)

✓	Installation step
	5. On Linux and UNIX computers, install application support on your local monitoring server, portal server, and portal desktop client for the IBM Tivoli Monitoring OS agents. **Note:** On Windows computers, the option to add application support for each OS agent is automatically selected when you choose to upgrade your monitoring server, portal server, and portal desktop client. If you deselected this option, click on the setup.exe file in the \WINDOWS subdirectory in the patch directory that you specified to rerun the installation, ensuring that you select the option to add application support for your OS agents. a. Stop the monitoring server, portal server, and portal desktop client. b. Run the following command to install application support: `./install.sh` c. When prompted for the IBM Tivoli Monitoring home directory, press Enter to accept the default (/opt/IBM/ITM) or type the full path to the installation directory you used. d. Continue through the installation steps, ensuring that you install "Tivoli Enterprise Monitoring Server support", "Tivoli Enterprise Portal Browser Client support", "Tivoli Enterprise Portal Server support", and "Tivoli Enterprise Portal Desktop Client support".

	6. On Linux and UNIX computers, reseed 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.
	Note: The monitoring server must be specified within the structure of *install_dir*.
	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`
	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*

Table 12. Checklist for installing the fix pack on a local host computer (continued)

✓	Installation step

	7. On Linux or UNIX computers, reseed application support on your portal server.
	a. Run the following command to stop the portal server:
	`./itmcmd agent stop cq`
	b. Run the following command to configure the portal server with the new agent information:
	`./itmcmd config -A cq`
	Complete the configuration as prompted.
	c. Run the following command to restart the portal server:
	`./itmcmd agent start cq`

	8. On Linux or UNIX computers, reseed application support on your portal desktop client. Run the following command to configure the portal desktop client with the new agent information: `./itmcmd config -A cj` Complete the configuration as prompted.
	9. 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 Chapter 5, ″Installing IBM Tivoli Monitoring″ in the *IBM Tivoli Monitoring Installation and Setup Guide*.

Monitoring server checklist

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

Notes:

1. The installation procedures are the same as used for the GA level installation. For detailed installation procedures, see Chapter 5, ″Installing IBM Tivoli Monitoring″ in the *IBM Tivoli Monitoring Installation and Setup Guide*.
2. Only hub monitoring servers support SOAP 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.

Table 13. Checklist for installing the fix pack on the monitoring server

✓	Installation step
	1. Gather information about the monitoring components in your environment. See “Fix pack installation planning worksheets” on page 19.
	2. Based on the platform of your local host computer, download and extract the necessary fix pack files to a temporary location on your computer. You can use the space below to write down the location of your patch directory. **Patch directory:**

Table 13. Checklist for installing the fix pack on the monitoring server (continued)

✓	Installation step

	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 **Tivoli Enterprise Monitoring Server** from the component list.
	Note: Reconfiguration is required. 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. 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.

	5. On Linux and UNIX computers, install application support on your monitoring server for the IBM Tivoli Monitoring OS agents.
	Note: On Windows computers, the option to add application support for each OS agent is automatically selected when you choose to upgrade your monitoring server. If you deselected this option, click on the setup.exe file in the \WINDOWS subdirectory in the patch directory that you specified to rerun the installation, ensuring that you select the option to add application support for your OS agents.
	a. Run the following command to stop the monitoring server:
	`./itmcmd server stop tems_name`
	where *tems_name* is the name of the monitoring server.
	b. Run the following command to install application support:
	`./install.sh`
	c. When prompted for the IBM Tivoli Monitoring home directory, press Enter to accept the default (/opt/IBM/ITM) or type the full path to the installation directory you used.
	d. Continue through the installation steps, ensuring that you install "Tivoli Enterprise Monitoring Server support".

Table 13. Checklist for installing the fix pack on the monitoring server (continued)

✓	Installation step

	6. On Linux and UNIX computers, reseed 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. Usually 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.
	Note: The monitoring server must be specified within the structure of *install_dir*.
	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`
	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`

	7. Install the fix pack on the remaining components: portal server, portal desktop client, and monitoring agents (local and remote).

Portal server checklist

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

Note: The installation procedures are the same as used for the GA level installation. For detailed installation procedures, see Chapter 5, "Installing IBM Tivoli Monitoring" in the *IBM Tivoli Monitoring Installation and Setup Guide*.

Table 14. 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 19.
	2. Based on the platform of your local host computer, download and extract the necessary fix pack files to a temporary location on your computer. You can use the space below 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 **Tivoli Enterprise Portal Server** from the component list.
	Note: Reconfiguration is required. 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. On Linux and UNIX computers, install application support on your portal server for the IBM Tivoli Monitoring OS agents.
	Note: On Windows computers, the option to add application support for each OS agent is automatically selected when you choose to upgrade your portal server. If you deselected this option, click on the setup.exe file in the \WINDOWS subdirectory in the patch directory that you specified to rerun the installation, ensuring that you select the option to add application support for your OS agents.
	a. Run the following command to stop the portal server:
	`./itmcmd agent stop cq`
	b. Run the following command to install application support:
	`./install.sh`
	c. When prompted for the IBM Tivoli Monitoring home directory, press Enter to accept the default (/opt/IBM/ITM) or type the full path to the installation directory you used.
	d. Continue through the installation steps, ensuring that you install both "Tivoli Enterprise Portal Browser Client support" and "Tivoli Enterprise Portal Server support".

Table 14. Checklist for installing the fix pack on the portal server (continued)

✓	**Installation step**

	5. On Linux or UNIX computers, reseed application support on your portal server.
	a. Run the following command to stop the portal server:
	`./itmcmd agent stop cq`
	b. Run the following command to configure the portal server with the new agent information:
	`./itmcmd config -A cq`
	Complete the configuration as prompted.
	c. Run the following command to restart the portal server:
	`./itmcmd agent start cq`

	6. 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 Chapter 5, "Installing IBM Tivoli Monitoring" in the *IBM Tivoli Monitoring Installation and Setup Guide*.
	7. Install the fix pack on the remaining components: portal desktop client and monitoring agents (local and remote).

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 Chapter 5, "Installing IBM Tivoli Monitoring" in the *IBM Tivoli Monitoring Installation and Setup Guide*.

Table 15. 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 19.
	2. Based on the platform of your local host computer, download and extract the necessary fix pack files to a temporary location on your computer. You can use the space below 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 **Tivoli Enterprise Portal Desktop Client** from the component list.
	Note: Reconfiguration is required. 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. On Linux and UNIX computers, install application support on your portal desktop client for the IBM Tivoli Monitoring OS agents. **Note:** On Windows computers, the option to add application support for each OS agent is automatically selected when you choose to upgrade your portal desktop client. If you deselected this option, click on the setup.exe file in the \WINDOWS subdirectory in the patch directory that you specified to rerun the installation, ensuring that you select the option to add application support for your OS agents. a. Stop the portal desktop client. b. Run the following command to install application support: `./install.sh` c. When prompted for the IBM Tivoli Monitoring home directory, press Enter to accept the default (/opt/IBM/ITM) or type the full path to the installation directory you used. d. Continue through the installation steps, ensuring that you install "Tivoli Enterprise Portal Desktop Client support".
	5. On Linux or UNIX computers, reseed application support on your portal desktop client. Run the following command to configure the portal desktop client with the new agent information: `./itmcmd config -A cj` Complete the configuration as prompted.
	6. 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 Chapter 5, "Installing IBM Tivoli Monitoring" in the *IBM Tivoli Monitoring Installation and Setup Guide*.

Table 15. Checklist for installing the fix pack on the portal desktop client (continued)

✓	**Installation step**
	7. Install the fix pack on the monitoring agents (local and remote).

Monitoring agent checklist - local installation

The following checklist provides the high-level local 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.

Notes:

1. The installation procedures are the same as used for the GA level installation. For detailed installation procedures, see Chapter 5, "Installing IBM Tivoli Monitoring" 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. To use remote deploy, use the steps in the "Monitoring agent checklist - remote installation" on page 33.
3. If you are installing agents from a CD for HP-UX computers, you must use the procedure described in "Mounting a CD drive on HP-UX" on page 44 to mount your CD.

Table 16. 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 19.
	2. Based on the platform of your local host computer, download and extract the necessary fix pack files to a temporary location on your computer. You can use the space below 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: Reconfiguration is required. 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 Chapter 5, "Installing IBM Tivoli Monitoring" in the *IBM Tivoli Monitoring Installation and Setup Guide*.

Monitoring agent checklist - remote installation

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). 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
```

Table 17. 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* -n 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 17. 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:
	• AX (UNIX) or GL (Windows) - Tivoli Enterprise Monitoring Agent
	• UI - Common install component (INST fix pack)
	• LZ - Linux OS agent
	• UL - UNIX Log agent
	• UM - Universal agent
	• UX - UNIX OS agent
	• NT - Windows OS 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`

	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" section of Chapter 5, "Installing IBM Tivoli Monitoring" in the *IBM Tivoli Monitoring Installation and Setup Guide*.

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 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

Use the following steps to install the fix pack:

1. Copy the fix pack tar file (6.1.0-TIV-ITM_i5OS-FP0004.tar) to a computer with ftp access to the i5/OS agent system.
2. Extract the fix pack tar file. This creates a directory structure that includes the save file for the updated i5/OS agent, a4520cma.sav.
3. On the i5/OS agent's system command line, create a CCCINST library, if this library does not already exist:

   ```
   CRTLIB  LIB(CCCINST)
   ```

4. Determine which version of the agent, if any, is currently installed using the **DSPSFWRSC** command. If product 0KA4430, 0KA4440, or 0KA4610 are listed then an agent is already installed.

   If 0KA4430, 0KA4440, or 0KA4610 is already installed, skip to Step 5. If no agent was previously installed, skip to Step 9.
5. 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.
6. 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.
7. 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
8. 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**.
9. Create a save file on the target i5/OS for the fix pack:

   ```
   CRTSAVF   CCCINST/A4520CMA  TEXT('ITM 6.1 Fix Pack 4')
   ```

10. 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
```

11. 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)
       ```

12. Optionally delete the installation library, which is no longer needed:

    ```
    DLTLIB CCCINST
    ```

13. 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.

Uninstalling the fix pack

Use the following steps to uninstall the fix pack:

1. Save the configuration file QAUTOTMP/KMSPARM(KBBENV) to create a backup of the current settings.
2. Stop the agent by using **GO OMA** Option 3.

   Make sure the agent stopped by looking at WRKACTJOB. The subsystem QAUTOMON should not be running and all the jobs in QAUTOMON subsystem must be ended.
3. Exit out of the **GO OMA** menu completely.
4. Create a save file on the target i5/OS 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 and the save file name can be any 10-character string.

   ```
    CRTSAVF   yourlib/FP04KA4BKP
   SAVLICPGM LICPGM(0KA4610) DEV(*SAVF) SAVF(yourlib/FP04KA4BKP)
   ```

   Note: Step 1 is required even if the existing agent saved. When you install using the saved file, it creates a new QAUTOTMP/KMSPARM(KBBENV) and it does not have any previous configurations.
5. Enter the following command to uninstall the agent:

   ```
   DLTLICPGM 0KA4610
   ```

6. Delete Authorization list QAUTOMON in QSYS:

   ```
   DLTAUTL QSYS/QAUTOMON
   ```

7. Delete short-term history files.

   Short-term history files exist in the location set for CTIRA_HIST_DIR in QAUTOTMP/KMSPAR(KBBENV). The default location is /QIBM/USERDATA/IBM/ITM/HIST Save the files in this directory and delete the files and the directory. There is no need to save these files if warehousing is configured. These files are warehoused at every 24-hour interval.

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

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.

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"
- "Installing from the command line" on page 40
- "Installing from the command line using a silent installation" on page 42

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 18. 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 4 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 Fix Pack 4 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 Fix Pack 4 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 4 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 4 is applied.

Uninstalling the IBM Tivoli Enterprise Console event synchronization

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

Note: 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.

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.

Additional installation information

Be sure to review the following important additional installation information.

Installing on a computer with no previous IBM Tivoli Monitoring components

When you are installing the full product media, which has been updated to include the Fix Pack 004 changes and related agent fix packs, there are no other special installation instructions except what is noted in this file.

Note that, on Windows computers, you can choose to install into any directory, such as "C:\Program Files," when performing a full product media installation. The default installation directory is still C:\IBM\ITM. If you want to install into a different directory, you must alter the default directory.

Uninstalling the GA level of code

The following items describe how to uninstall the GA (general availability) version of IBM Tivoli Monitoring after applying a fix pack, if you choose to do so:

- If you install the GA code, you uninstall it with the GA code uninstaller. Use the Add/remove programs function on your computer or the silent setup.exe uninstallation option from the GA CD.
- If you install the GA code, and then run the fix pack installer, you still uninstall with the GA code uninstaller. Use the Add/remove programs function on your computer or the silent setup.exe uninstallation option from the GA CD.

Mounting a CD drive on HP-UX

Product CDs for IBM Tivoli Monitoring for HP-UX platforms are formatted for the Rock-Ridge file system type, which is an extension to the International Standards Organization ISO-9660 file system type. HP-UX uses a mechanism called portable file system (PFS) on PA-RISC machines to mount Rock-Ridge CDs. The following procedure guides you through using PFS to mount a CD drive as the root user on a Linux platform or as the root user on a UNIX-based operating system platform:

1. Log on as root.
2. Determine the CD device name by using the ioscan command or the sam system maintenance interface.

   Run the /usr/sbin/ioscan -funC disk command to return a table of disk devices. If you cannot determine the name of the CD device, run the sam system maintenance interface to find more information about disk devices.

3. Start the pfsd daemon. PFS mounting is not active on HP-UX computers by default. The pfsd daemon must be running to mount a CD device. To start the daemon, run the following commands:

   ```
   # /usr/sbin/pfs_mountd &
   # /usr/sbin/pfsd &
   ```

4. Insert the product CD.
5. Use the following command to mount the CD:

   ```
   # /usr/sbin/pfs_mount -t rrip -o xlat=unix /dev/dsk/c0t0d0 /cdrom
   ```

   The CD drive is the /dev/dsk/c0t0d0 device. The /cdrom directory is where the CD drive mounts. The rrip parameter forces the CD drive to mount in the Rock Ridge Interchange Format. The xlat=unix parameter translates file names properly for HP-UX.

Alternative mounting procedures

The mount command can fail on any CD that contains files with long file names. Use one of the following procedures if you have a problem with mounting the CD because it contains files with long names:

Editing the pfs_fstab file: Use the following procedure to edit the pfs_fstab file:

1. Log in as a user with root authority.
2. In the /etc directory, add the following line to the pfs_fstab file:

   ```
   /dev/dsk/c0t0d0 mount_point pfs-rrip ro,hard
   ```

   Where `mount_point` represents the mount point of the CD.
3. Start the pfs daemon by entering the following commands (if they are not already running):

   ```
   /usr/sbin/pfs_mountd &
   /usr/sbin/pfsd 4 &
   ```

4. Insert the CD in the drive and enter the following commands:

   ```
   mkdir /cdrom
   /usr/sbin/pfs_mount /cdrom
   ```

   Where `/cdrom` represents the mount point of the CD.

Using pfs_mount to read the Rock Ridge system type: Use the following procedure to read the Rock Ridge system type:

1. The standard HP-UX mount procedure does not read the Rock Ridge file system type correctly. You must mount the CD using the pfs_mount command. Start pfs daemons by entering the following commands:

   ```
   pfs_mountd&
   pfsd&
   ```

2. Mount the CD as shown in the following example, where device represents the raw device (for example, /dev/rdsk/c0t0d0), and mntpnt represents the mount point (for example, /cdrom):

   ```
   pfs_mount -x unix device /mntpnt
   ```

3. Add the following line to /etc/pfs_exports, where remotemnt represents the mount point, and server represents the name of the HP-UX computer where you are installing the product:

   ```
   /remotemnt -access=server
   ```

4. Enter the following command:

   ```
   pfs_exportfs -a
   ```

5. Run the following procedure on the local HP-UX computer:

a. Log in as root.
b. Start pfs daemons by entering the following commands:

```
pfs_mountd&
pfsd&
```

c. Enter the following command, where remote_server represents your remote system, remotemnt represents the CD-ROM drive on the remote HP-UX computer, and localmnt represents the mount point on your local HP-UX computer:

```
pfs_mount -x unix remote_server:/remotemnt /localmnt
```

d. Change the directory to the package location, where localmnt represents the directory mount point.

```
cd /localmnt/tas
```

Unmounting the CD

After installation, you can use the following command to unmount the CD:

```
/usr/sbin/pfs_umount  /cdrom
```

Adding agents to a patched environment

If you plan to add monitoring agents (both OS and non-OS agents) to your monitoring environment after you have applied Fix Pack 004 and you want to use the remote deployment function (instead of installing locally), you must use the **tacmd createNode** command (for OS agents) or **tacmd addSystem** command (for non-OS agents) to deploy the *GA* level of the agent and then upgrade that agent to the fix pack level using the **tacmd updateAgent** command.

Note: If you plan to use both the **tacmd createNode** command and the **tacmd addSystem** command, you must run the **tacmd createNode** command first. An OS agent must be present on a host before you can use the **tacmd addSystem** command.

For agents based on a fix pack previous to Fix Pack 004, you cannot have both the fix pack full image and the fix pack update image in the agent depot. If your agent depot already contains the full image, you can use the **tacmd removeBundles** command to remove the image from the depot. For example, to remove the AIX 5.3 UNIX OS agent full image bundle, run the following command:

```
tacmd removeBundles –i /mnt/bundles –t ux –p aix513 –v 06100301
```

For more information about the **tacmd removeBundles** command, see the "Command Reference" appendix in the *IBM Tivoli Monitoring Installation and Setup Guide*.

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 004, the upgrade toolkit upgrades to the Fix Pack 004 version of the agents.

For Fix Pack 004, 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.

About the GA versions of the IBM Tivoli Monitoring V6.1 agent CDs for Windows platforms

The General Availability (GA) versions of the IBM Tivoli Monitoring V6.1 agent CDs for the Windows operating system must *NOT* be installed into an IBM Tivoli Monitoring V6.1 Fix Pack 004 environment or be used to populate a Tivoli Enterprise Monitoring Server depot. The IBM Tivoli Monitoring V6.1 agent CDs have been refreshed for use with Fix Pack 004.

A problem with the installer on the GA version of the IBM Tivoli Monitoring V6.1 agent CDs for the Windows operating system will cause a currently installed Fix Pack 004 Tivoli Enterprise Monitoring agent framework component to be replaced by the older GA version. When this occurs, the IBM Tivoli Monitoring V6.1 Fix Pack 004 Windows OS agent fails. The problem exists only on the Windows version of the IBM Tivoli Monitoring V6.1 agent CDs.

The IBM Tivoli Monitoring V6.1 agent CDs for the Windows operating system have been refreshed with an updated agent installer as well as a Fix Pack 1 level of the Tivoli Enterprise Monitoring agent framework component. In case a GA version of an IBM Tivoli Monitoring V6.1 agent CD was used to install an agent on a Windows operating system after installing IBM Tivoli Monitoring V6.1 Fix Pack 004 Windows OS agent, running the installer from the refreshed IBM Tivoli Monitoring V6.1 agent CD allows the previous version of Tivoli Enterprise Monitoring agent framework component to be restored to the Fix Pack 004 version. The agent version is *NOT* updated. The agents remain at the GA version.

It is important to note that when the Tivoli Enterprise Monitoring agent framework is overlaid by the GA version on computers where the IBM Tivoli Monitoring V6.1 Fix Pack 004 Windows OS agent has been installed, there is no way to administer the system remotely because the Windows OS agent is the prerequisite to all remote administration capabilities. The local installation procedure described above is the only recovery mechanism.

You need to replace your GA version of the IBM Tivoli Monitoring V6.1 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 V6.1 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 V6.1 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 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\KUD\061000000\VERFILES
```

Summary of this section

Every General Availability (GA) version of the IBM Tivoli Monitoring V6.1 agent for Windows operating system CD and installation image must be replaced with the refreshed version. Every GA version of the IBM Tivoli Monitoring V6.1 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 V6.1 Fix Pack 004 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 V6.1 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 004 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 004 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 004 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 V6.1 agent on Windows computer 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 V6.1 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).

Securing your IBM Tivoli Monitoring installation

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

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.

Chapter 3. 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.

Known problems and workarounds

The following section identifies known problems and the workarounds that are available to resolve the problems.

- 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.
- 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 cannot delete a situation by clicking the **Delete** icon on the Situation Editor toolbar.

  Right-click on the situation name and select **Delete**.
- Creating a situation and deleting it without saving it first causes the situation to fire with a "problem" status.

If you create a situation that has the wrong attribute group or is under the wrong node do not try to delete the situation. You must use the Situation Editor dialog to cancel the situation. You can then use the Situation Editor again to create your situation.

- Upgrading from OMEGAMON XE or OMEGAMON 360 to IBM Tivoli Monitoring V6.1 can cause the Tivoli Enterprise Portal Server logon to fail.

  Perform the following steps to edit the HOME\CNPS\KFWENV file:

  1. Change KFW_LOADLIB=KfwServices to KFW_LOADLIB=KfwMain.
  2. Save the KFWENV file.
  3. Restart the Tivoli Enterprise Portal Server.

- Some instances of the Universal Agent do not start or appear as if they have not been upgraded after installing Fix Pack 004.

  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.

- 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 machine. 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 machine.

- 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.
  - Copy the CD to the remote computer and install.
  - Use a network drive that the remote computer can access for the installation.

  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.

- The Tivoli Data Warehouse does not connect after you complete the upgrade.

  After upgrading the Warehouse Proxy agent, you must stop the agent, reconfigure the agent, and start the agent again to complete the upgrade process.
- After performing an upgrade from OMEGAMON 350, events are not displayed in the situation event console view.

  You must recycle the Tivoli Enterprise Portal Server and the Tivoli Enterprise Portal to complete the upgrade process.
- After upgrading to Fix Pack 004 on a UNIX or Linux computer, some of your Universal Agent instances 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 004 and manually restart any Universal Agent instances that did not restart.
- Running the CandleManage command line binary on AIX 5.3, and other versions of AIX, with the background specifier might cause a Java™ core. For example, `CandleManage &`.

  Run the command without the background specifier, `CandleManage`.
- On SUSE Linux Enterprise Server 10 computers, you cannot start the Universal Agent through the CandleManage GUI.

  From the command line, run the um_console (validate , import , unpack) command.
- The Tivoli Enterprise Monitoring Server and local agents running on the Tivoli Enterprise Monitoring Server might not restart when you install products on the Tivoli Enterprise Monitoring Server depot.

  Start the Tivoli Enterprise Monitoring Server and local agents manually.
- Callpoints can potentially execute code that is long running. You are not notified that the process is running and it appears that configuration is hanging.

  Continue to allow the process to run until it successfully completes.
- 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.
- 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.
- 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.
- Fix Pack 004 installation fails on AIX V5.3 computers.

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

- The upgrade from Tivoli Distributed Monitoring sometimes stops while upgrading the Tivoli Distributed Monitoring profiles and profile managers.

  Do not enable Tivoli Enterprise Console forwarding until your upgrade is complete. See the *IBM Tivoli Monitoring Installation and Setup Guide* for details on enabling Tivoli Enterprise Console forwarding.

  Note: Do not edit the baseline XML file for Tivoli Enterprise Console forwarding. Keep the <HubServer tec_forwarding_endpoint=""> and <EventServerList eventServerLabel="" eventServerTarget="" /> files in the baseline XML file and do not edit the defaults.
- 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/.
- When the SYSADMIN user is created on Windows computers, the "Password never expired" option is not checked by default. When IBM Tivoli Monitoring V6.1 is installed on Windows computers, the installer creates SYSADMIN user as a Windows user ID. If the "Password never expired" option is not checked, your password will expire and you will not be able to log in.

  Use the following procedure to ensure that the "Password never expired" option is selected after you install IBM Tivoli Monitoring on a Windows computer:

  1. Select **Start → All Programs → Admin Tools → Admin Computer**.
  2. Select **System tools → local users and groups → Users**.
  3. Right-click user "**SYSADMIN**" and select **properties**.
  4. Select "**Password never expired**".
- 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.
- When you use the Situation Editor icon to create a new situation under "MVS™ System", new OMEGAMON 4.1 attributes are not displayed.

  Do not use the Situation Editor icon to create new situations. Instead, right-click in the navigation tree node where you want to associate the situation and select **Situations**. Click the **Set Situation filter criteria** icon and select **Associated with Monitored Application** and **Associated with this object**. The attributes display correctly.
- The following message is displayed when returning to the Situation Editor to view a situation that you created using OMEGAMON 4.1 attributes:

  ```
  KFWITM375W Situation formula contains invalid attributes.
  ```

Do not use the Situation Editor icon to create new situations. Instead, right-click an item in the navigation tree and select **Situations**. In the **Situations for item** window, right-click on the item and select **Create New...**. The attributes display correctly.

- When viewing custom workspaces after upgrading from OMEGAMON 350 to Fix Pack 004, the "Status" column in the Situation Event Console does not reflect the state assigned to the situation that 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.

- The application support installer used to apply patches to agent application support in fix packs prior to Fix Pack 004 incorrectly sets the field ″sizeAll″ instead of ″sizeALL″ in the *install path*/registry/*pc*.ver file, where *pc* is the two-letter product code for an agent. The following warning message might be displayed after you confirm the installation selections:

  ```
  WARNING - could not determine the required disk space.
  ```

  This message is harmless. To eliminate this message, you can edit the *install_path*/registry/*pc*.ver files that have ″sizeAll″ instead of ″sizeALL″ before you upgrade your application support or monitoring server using the Fix Pack 004 installer.

- 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.

- 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.

- 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:
  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.

- If you encounter Internet Explorer crashes (memory could not be 'read' message) while using the Tivoli Enterprise Portal, perform the following steps:
  1. Contact IBM Customer Support to obtain an updated IBM JRE. The required release is IBM Java 1.4.2 Service Release 6 (Windows / IA32) (cn142-20060824) or higher. The file name is ibm-java2-jre-142.exe.
  2. On your Tivoli Enterprise Portal Server computer, navigate to the *ITM Root*\CNB\java directory.
  3. Rename the ibm-java2.exe file to some other name in case it needs to be restored.
  4. Copy the ibm-java2-jre-142.exe file to the *ITM Root*\CNB\java directory and rename it to ibm-java2.exe.
  5. For each browser client that you want to receive the new release, uninstall any existing IBM Java release.
  6. Connect each browser client to the Tivoli Enterprise Portal Server. The browser guides you through the installation of the updated IBM JRE.
  7. After the installation is complete the Internet Explorer crashes no longer occur.

- If you receive one of the following symptoms when using the backspace on UNIX computers, you have incorrectly configured the backspace key:
  - When you press the backspace key, characters such as ″^?″ and ″^H″ are displayed on the screen.
  - The backspace key seems to be working correctly when entering text, but you later find characters such as ″^?″ and ″^H″ in configuration files and your software malfunctions.

  Configure your terminal and ″stty erase″ to use the same key code for backspace. Consider using ″^?″ as the key code. Verify your configuration with the IBM Tivoli Monitoring distributed utility, Install: BackspaceCheckUtility.
- On Windows computers, updating application support files for the monitoring server, portal server, and portal client using the Application Support Installer (ASI) might fail if the installation path has spaces, such as ″C:\Program Files\IBM\ITM.″ To address this issue, for Windows installations where these components are installed into a path with spaces, if an agent is based on a fix pack prior to Fix Pack 004, copy the 6.1.0-TIV-ITM_INST-FP0003/ASI/setup.jar and 6.1.0-TIV-ITM_INST-FP0003/ASI/libwinjni.dll from the Fix Pack 004 INST component fix pack to the CD-ROM directory of the Fix Pack 002 location.
- 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.

- 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.

- If you are running the OMEGAMON XE for Messaging agent (a 32-bit agent) on a Linux or UNIX computer, you must install the 32-bit agent framework to support the application agent. Use the following steps to install the 32-bit framework:
  1. In the directory where you extracted the base IBM Tivoli Monitoring V6.1 installation files, run the following command:

     ```
     ./install.sh
     ```

  2. When prompted for the IBM Tivoli Monitoring home directory, press Enter to accept the default (/opt/IBM/ITM) or type the full path to a different directory.
  3. If the installation directory does not already exist, you are asked if you want to create it. Type `y` to create this directory and press Enter.
  4. The following prompt is displayed:

     ```
     Select one of the following:
     1) Install products to the local host.
     2) Install products to depot for remote deployment (requires TEMS).
     3) Exit install.

     Please enter a valid number:
     ```

     Note: This prompt might vary depending on the installation image from which you are installing.

     Type 1 to start the installation and press Enter.
  5. Type the number that corresponds to the language in which you want to display the software license agreement in and press Enter.
  6. Press Enter to display the agreement.

7. Type 1 to accept the agreement and press Enter.
8. Type a 32-character encryption key and press Enter. Use the same as the key that was used during the installation of the monitoring server to which this monitoring agent connects.

   A numbered list of available operating systems is displayed.
9. Type the number for the *32-bit version* of the operating system that you are installing on. For example, if you are installing on a 64-bit AIX V5.3 computer, type the number that corresponds to 32-bit AIX V5.3. The default value is your current operating system. Press Enter.
10. Type `y` to confirm the operating system and press Enter.

    A numbered list of available components is displayed.
11. Type the number that corresponds to "Tivoli Enterprise Services User Interface V06.10.02.00" and press Enter.

    A list of the components to install is displayed.
12. Type `y` to confirm the installation.

    The installation begins.
13. After all of the components are installed, you are asked whether you want to install components for a different operating system. Type `n` and press Enter.

You can now install the OMEGAMON XE for Messaging agent.

- In some instances when upgrading custom workspaces from OMEGAMON 350 to IBM Tivoli Monitoring V6.1 Fix Pack 004, 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.
- 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**.

- When migrating data from an existing OMEGAMON 360 data warehouse to the IBM Tivoli Monitoring V6.1 Tivoli Data Warehouse, the migration fails with the following error message:

  ```
  JVMST100: Unable to allocate an array object, Array  element exceeds IBM JDK
  limit of 268435455 elements.
  ```

  You might also receive a message that the JVM is out of memory. This problem can occur when the source database is in Microsoft SQL server.

  When configuring the migration tool, specify the following value for the KHD_SOURCE_URL and KHD_TARGET_URL variables in the KHDENV_MIG file (located in the itm_installdir/tmaitm6 directory):

  `jdbc:microsoft.sqlserver://`*`server`*`;`*`port`*`;DatabaseName=`*`database`*`;selectMethod=cursor`

  The instructions for configuring and running the warehouse migration tool to migrate an existing OMEGAMON 360 data warehouse to the IBM Tivoli Monitoring V6.1 Tivoli Data Warehouse are documented in the *IBM Tivoli Monitoring V6.1 Installation and Setup Guide*.

  The installation guide documents the SQL Server URL specification shown above (on page 44 of the August, 2006 Revised version), but the selectMethod=cursor string is omitted. Without the cursor, the migration tool attempts to migrate a large table in a single transfer. With the cursor, the migration tool moves the data in segments without exceeding available memory.

Known limitations

The following section identifies known limitations that do not have an available workaround.

- On Windows computers, you receive the following error message at the end of an installation or upgrade:

  ```
  Unhandled Exception
  Error Number: 0x80040707
  Description: DLL function call crashed: ISRT._ListReadFromFile  Setup will now terminate.
  ```

  This error is a result of InstallShield defect 1-LFYW9. The installation is attempting to examine the current installation log for errors. If errors are found, they are displayed on the final dialog. However, the InstallShield defect is limiting the examination of the installation log and produces the error. If you receive this error, the setup will abort, however, your installation is still intact.
- You receive the following error when you select "Run LTA" (Log and Trace Analyzer) from the Event tools workspace:

  ```
  The specified path does not exist.
  ```
- After upgrading the Universal Agent to Fix Pack 004, the correct version is not displayed. The agents have been upgraded as expected, however.
- Data is not displayed in the CPU and Memory graphs in the Tivoli Enterprise Portal desktop while trying to view it in the CMDB "Configuration Tracking and Discovery Infrastructure" workspace. The data is displayed when you reopen the Tivoli Enterprise Portal desktop, however, a refresh of the workspace causes the data to disappear again. The is not a limitation in the Tivoli Enterprise Portal browser.

- Remote Tivoli Enterprise Monitoring Servers with high CPU causes the remote Tivoli Enterprise Monitoring Server to crash. The problem is caused by monitoring agents failing to connect to the remote Tivoli Enterprise Monitoring Server.
- If your workspace views display historical data across multiple pages, data is displayed only on the first page (and not displayed on subsequent pages).
- In the Tivoli Enterprise Portal, a user with Administrator authority (including the new Workspace Administration permission) can see only global workspaces; that user cannot see workspaces created by individual users. Only the user who created a custom workspace can see it in the Navigation tree.
- 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.

Appendix A. New configuration options for z/OS components

The following sections provide information about new configuration options for z/OS components. Fix Pack 004 adds the following options:

- Use the network interface list to specify network interfaces to be used by the monitoring server on z/OS and by a monitoring agent installed in a separate address space from the monitoring server.
- Configure a Tivoli Enterprise Monitoring Server or monitoring agent address space to redirect z/OS Take Action commands to NetView through the Program to Program Interface (PPI).

Network interface list

The new Network interface list parameter is required if your site runs more than one TCP/IP interface or network adapter on the same z/OS image. When this parameter is set, you can direct the monitoring server on z/OS and the monitoring agent (if installed in a separate address space from the monitoring server) to connect to a specific TCP/IP local interface.

In the Network interface list field of an IP communication protocol panel in the Configuration Tool, specify the host names of one or more network adapters to be used for input and output. Separate the entries with a space. If your site uses the Domain Name System (DNS), you can enter either short host names or dotted-decimal IP addresses. If your site does not use DNS, you must enter the fully qualified host names. The Configuration Tool then generates the KDEB_INTERFACE parameter in members KDSENV (for the monitoring server) and K*pp*ENV, where *pp* is the monitoring agent, of the *&rhilev.* *&rtename.*RKANPARU library.

Take-Action command authorization and execution through NetView

You can configure a Tivoli Enterprise Monitoring Server or monitoring agent address space to redirect z/OS Take Action commands to NetView through the Program to Program Interface (PPI). Take Action commands issued in NetVew make full SAF calls for authorization. NetView uses the Tivoli Enterprise Portal user ID to determine the NetView operator on which the command authorization is performed. If command authorization passes, the command is executed on the NetView operator. Messages are written to the NetView log to provide an audit trail of the commands and the users that issued them.

Use the following parameters to configure the Tivoli Enterprise Monitoring Server or monitoring agent while using the configuration tool. Use the "SPECIFY CONFIGURATION VALUES" configuration panel for configuring the monitoring server and the "SPECIFY ADVANCED AGENT CONFIGURATION VALUES" configuration panel for configuring the monitoring agent.

Program to Program Interface (PPI) information
(Optional) Specify the PPI values that enable forwarding of Take Action commands to NetView for z/OS for authorization and execution. If you enable forwarding, you must also enable NetView to authorize the commands (see “Enabling NetView to authorize Take Action commands” on page 65).

Forward Take Action commands to NetView for z/OS?
Indicate if you want the Tivoli Enterprise Monitoring Server to forward z/OS console commands issued as Take Action commands for authorization and execution.

NetView PPI receiver
Specify the name of the PPI receiver on NetView that will receive Take Action commands. This name must match the receiver name that is specified on the NetView APSERV command. (The default name is CNMPCMDR.) If the specified name is incorrect or the receiver is not active on NetView for z/OS, default (MGCR) command routing is performed. The configuration tool generates the KGLHC_PPI_RECEIVER parameter in the KDSENV member of the *&rhilev*.*&rtename*.RKANPARU library.

The value must be a 1-8 character, unique identifier for the receiver program. The value can contain alphabetic characters A-Z or a-z, numeric characters 0-9, and the following special characters: dollar sign ('$'), percent sign ('%'), ampersand ('&'), at sign ('@'), and number sign ('#'). This value must match the value specified in the NetView DSIPARM initialization member, CNMSTYLE (see "Enabling NetView to authorize Take Action commands" on page 65).

For monitoring agents, this value defaults to the NetView for z/OS PPI receiver used by the Tivoli Enterprise Monitoring Server if one is configured in this runtime environment. Otherwise, the default is CNMPCMDR.

This value is required if you specified `Y` to the **Forward Take Action commands to NetView for z/OS** field.

TEMS PPI sender
Optionally, specify the optional name of the PPI sender. The value must be a 1-8 character, unique identifier for the receiver program. It can contain alphabetic characters A-Z or a-z, numeric characters 0-9, and the following special characters: dollar sign ('$'), percent sign ('%'), ampersand ('&'), at sign ('@'), and number sign ('#'). This name must not conflict with any NetView for z/OS domain name, as it is used in logging the command and command response in the NetView log. If a value is specified on this field, the configuration tool generates the KGLHC_PPI_SENDER parameter in the KDSENV member of the *&hilev*.*&rtename*.RKANPARU library.

If you do not specify a value in this field, the default is the job name of the Tivoli Enterprise Monitoring Server that is the source of the command.

Notes:

1. If you enable NetView command authorization on the Tivoli Enterprise Monitoring Server, you must also enable NetView to execute the commands. See "Enabling NetView to authorize Take Action commands" on page 65 for details.
2. Take Action forwarding requires NetView on z/OS V5.2 with APAR OA18449 applied.

Adding the NetView CNMLINK data set to the Tivoli Enterprise Monitoring Server started task

To connect to NetView, the Tivoli Enterprise Monitoring Server must reference the NetView CNMLINK data set. Concatenate the NetView CNMLINK data set to the RKANMODL statement in the Tivoli Enterprise Monitoring Server started task.

To provide the location, uncomment the CNMLINK DD card in the Tivoli Enterprise Monitoring Server started task and specify the NetView CNMLINK data set. For example:

```
000350 //RKANMODL  DD DISP=SHR,
000351 //          DSN= &RHILEV.&SYS.RKANMODU
000352 //          DD DISP=SHR,
000353 //          DSN= &RHILEV.&SYS.RKANMODUL
000354 //          DD DISP=SHR,
000355 //          DSN= &RHILEV.&SYS.RKANMOD
000356 //*********************************************************************
000357 //* RKANMODL DD: CNMLINK
000358 //*********************************************************************
000359 //* Uncomment this DD card and specify the location of the CNMLINK
000360 //* load module for NetView for z/OS.  This library is required for the
000361 //* "Forward Take Action commands to NetView for z/OS" support which
000362 //* is enabled for this Agent.  The CNMLINK library must also be
000363 //* APF-authorized.
000364 //         DD DISP=SHR,
000365 //         DSN=NETVIEW.V5R2M0.CNMLINK
```

Contact your NetView for z/OS system programmer for the data set name, if necessary. The default NetView 5.2 CNMLINK data set is NETVIEW.V5R2M0.CNMLINK.

The CNMLINK library must be APF-authorized.

Enabling NetView to authorize Take Action commands

If you have configured Tivoli Enterprise Monitoring Server address spaces to forward z/OS Take Action commands to NetView, you must also enable NetView to receive and execute the commands. NetView does command authorization as part of the execution.

To enable execution of forwarded commands, complete the following steps:

1. Define Tivoli Enterprise Portal user IDs to NetView.

   For information on defining user IDs, see the section on "Defining operators for the NetView for z/OS Tivoli Enterprise Portal agent" in the *Tivoli NetView on z/OS: Security Reference*. You can find the NetView documentation in the Tivoli Netview for z/OS documentation information center at: http://publib.boulder.ibm.com/infocenter/tivihelp/v3r1/index.jsp?toc=/com.ibm.itnetviewforzos.doc/toc.xml
2. Optionally, define the NetView PPI receiver in the NetView DSIPARM member CNMSTYLE (see Figure 1 on page 66).

   Follow the instructions in the member. The PPI receiver for APSERV will be started during NetView initialization.
3. If you do not customize CNMSTYLE to define the receiver, start the NetView PPI receiver manually by issuing the APSERV command.

Figure 1. CNMSTYLE member after editing

```
*************************************************************************
*       Tivoli Management Services infrastructure server                *
*                                                                       *
* Uncomment the following (and, optionally, supply preferred OPID) to  *
* initialize support for commands and messages from Tivoli Management  *
* Services infrastructure and/or other APF authorized clients. See    *
* command help for APSERV for information about the function and       *
* clients depending on it.                                             *
*                                                                       *
*************************************************************************
function.autotask.APSERV = AUTOTMSI
*
AUTOTASK.?APSERV.Console = *NONE*      //
AUTOTASK.?APSERV.InitCmd = APSERV CNMPCMDR
```

Appendix B. APARs addressed by this fix pack

The following APARs are addressed by this fix pack.

Documentation APARs

The following APARs are addressed in Chapter 3, “Known problems and limitations,” on page 51 in the Fix Pack 004 readme:

APAR Number	Symptom
IY87195	TEPS database on MSSQL configured with "Windows only" authentication method.
IY88830	Unable to input into text field of the help of the TEPS Web client.

The following APAR was addressed in previous fix packs and carried forward in Fix Pack 004:

APAR Number	Symptom
IY89022	The Fix Pack 003 readme required update: • The descriptions of the environment variable and configuration file to modify on Linux and UNIX monitoring servers in order to enable log in validation were not clear. • The incorrect JDBC driver for Oracle was used. Instead of "ojdbc14_g.jar," the "ojdbc14.jar" JDBC driver must be used.

INST component APARs

The following APARs are addressed in Fix Pack 004:

APAR number	Symptom
IY70237	MQ agent configuration utility creates corrupt configuration file when backspace characters are used.
IY83509	SOAP hub monitoring server configuration is not saved when Manage Tivoli Enterprise Monitoring Services restarts.
IY86238	Situations supplied with the Tivoli Monitoring 5.x Endpoint Agent are missing after installing Fix Pack 001.
IY86733	Creation of Tivoli Enterprise Portal Server fails with no obvious error message.
IY89208	After ITM6.1 FP1 was installed, the CTIRA_HEARTBEAT=1 ENTRY was missing from the KBBENV file.
IY89240	Wrong file permissions when remotely installing an agent on Solaris 10.
IY89297	TEPS on AIX 5.3 fails to shutdown properly in ITM 6.1 FP03.
IY89660	Dependant jar files are not being patched on Windows.
IY89762	IBM Tivoli Monitoring, Version 6.1 universal database monitoring fails for a 32 bit instance on a 64 bit system.
IY89807	The bannerimage.html file is overwritten after fix pack install.
IY90798	The om_tec.config file is overwritten while applying TEMS patches.
IY91406	Status of tacmd listsit is different from the one of TEP.

The following APARs were addressed in previous fix packs and carried forward in Fix Pack 004:

APAR number	Symptom
IY80007	DB2 monitoring agent will not start when not installed as the DB2 instance owner.
IY80118	The Solaris OS agent fails due to missing GSKIT64 libraries.
IY80519	Situations are not firing when re-imported with tacmd and reassociated.
IY81101	GSKIT installed only on C drive one Windows systems. (New Installs only)
IY81412	Reconfiguring TEMS Windows service causes the service ″Log On″ account to revert to the Local System account, no matter what it was set to previously.
IY81610	When application support is added for an agent which requires a CLASSPATH update for the TEP desktop client, and there are more than one instance of the TEP desktop client, only one of those instances gets updated with the changed Java CLASSPATH.
IY81616	While using a proxy server, attempting to access a URL, the error ″Server refuses to serve document″ occurs.
IY83425	The install.sh script sets permissions for all installed products to 777.
IY83538	The ″tacmd viewsit″ command output is empty for situations for the Universal Agent.
IY83577	Caching error: unable to store or update files in the cache.
IY83660	If Reconfigure of Portal Browser Client is selected from Manage Tivoli Services, the loaded JAR file box show all JAR files as unchecked, even though the products are installed. Also, the Edit box is disabled.
IY83824	For Windows TEMS to UNIX/Linux createnode deploys, checking the disk space of the target install directory when the directory's parent doesn't exist can give incorrect results. Forward slashes are changed to backslashes when the parent is checked, which causes the free space method to return the temp space available.
IY84168	The ″tacmd″ command fails if the user's password includes ″@″
IY84275	The ″tacmd login″ command fails when the -p option is specified.
IY84338	DB2 agent causes core dumps when running multiple instances because a single history file is being utilized.
IY84339	When the DB2 agent was started, and then crashed, the core file would be put in the DB2 user home dir. The large core files, especially if there is more than a few, can get large and disrupt operations.
IY84518	ITM 6.1 does not install the JRE 1.4.2 on a system with Java 1.5 (new installation only)
IY84540	Unix agent creates temporary file .KUXTMP.XXXXXX in the tmp directory.
IY84844	When installing 6.1.0-TIV-ITM_INST-FP0001 or 6.1.0-TIV-ITM_INST-FP0002, the install_kui.sh script returns: Err_report fail product ″ui″ not installed for this architecture install_kui.sh failure: product ″ui″ not installed for this architecture.
IY85163	Backup copies of .ver files causes itmpatch command to fail on Windows with a Dr Watson error.
IY85477	HTTP proxy server configuration not saved when MTEMS restarts.
IY85824	Eliminate proxy server options for browser client configuration.
IY86257	After applying ITM 6.1 FP1 patch install for a remote TEMS on AIX 5.2 64-bit, the remote TEMS terminates with a core dump.
IY87503	The user login process fails when installing as a non-root user and configuring the TEMS for user security.
IY80187	User Security Validation does not work because the Manage Tivoli Monitoring Services GUI is not changing the owner of the required file [kdsvlunx] to root.

APAR number	Symptom
IY80546	Prior to Fix Pack 2, the user must run the ″SetPerm -s″ command to enable User Validation Security but the documented process failed to include this step.
IY82516	Running tacmd updateAgent core dumps on Solaris TEMS.
IY82519	The addSystem and configureSystem CLIs don’t allow encrypted password parameters.
IY82524	addSystem and configureSystem give false success messages when bad agent configuration data is entered.
IY83359	The ″tacmd addsystem″ command is failing with RC8 when deploying UA to a Windows Managed System.
IY84088	On Unix and Linux systems, ″itmpatch.exe″ creates the patchlogs directory with root only access.
IY84099	When a customer attempts to use the ″tacmd updateAgent″ command for a Universal Agent with multiple subnodes, the ″tacmd updateAgent″ command might terminate unexpectedly on all platforms.
IY84119	After installing Fix Pack 1 all situations are no longer associated.
IY84340	Installation of 6.1.0-TIV-ITM_INST-FP0001 may fail when the citnt.ver still exists on the system and install_kui.sh terminates with a memory fault (SIGSEGV).
IY84370	On Windows systems, ″itmpatch.exe″ program generates an Access Violation error message when attempting to run KinCInfo.exe -r.
IY84516	After installation of 6.1.0-TIV-ITM_INST-FP0001, the ″tacmd createNode″ command no longer works.

Tivoli Enterprise Monitoring Agent APARs

The following APARs are addressed in Fix Pack 004:

APAR number	Symptom
IY89899	TEMS crashes when one situation fires.
IY90352	The Warehouse Proxy Agent fails with "UserID decode failed. Status = 29″ on startup.
IY91689	ITM 6.1 communications infrastructure problem.
IY91926	After application of 6.1.0-TIV-ITM-FP0002, transport layer defects can cause loops (High CPU usage) and/or hangs resulting in loss of connectivity.

The following APARs were fixed in previous fix packs and carried forward in Fix Pack 004:

APAR number	Symptom
IY82134	We create a situation to monitor the ″file Info″ for Unix OS agent called test_file defined as: *IF *VALUE File_Information.File_U *NE ’ccc.txt’ --> this is true for all files on the unix box. The is correctly evaluated at agent and data seems to be sent to TEMS but the situation never becomes TRUE. This does not work for any file path specified.
IY84059	On some UNIX/Linux platforms, execute permissions are lost when a UA script is copied from the agent depot directory to the UA scripts directory.
IY86480	During an agent registration with it’s TEMS, if the TEMS is not available the agent is suspended using BSS1_Sleep. This can cause the agent to hang if the agent is shutdown while waiting for the BSS1_Sleep time to expire.

APAR number	Symptom
IY87818	KDCB0_HOSTNAME variable is not created in IBM Tivoli Monitoring V6.1 on z/OS by ICAT.
IY87841	With PTF: UA25220 the kwe messages sometimes get truncated.
IY87858	Remote TEMS loses connection to hub TEMS and fails to reconnect.
IY87902	Direct TEMA to bind to specific ip or interface.
IY87903	CMS registration gets wiped out if SPUFI is run.
IY81237	Warehouse Database tables have garbage in some columns, Data in historical files is corrupted and TEP historical reports show big negative numbers in the columns where they are not expected. The problem usually occurs on AIX5.2 and Solaris 5.9 64-bit machines that have in excess of 8 CPUs.
IY81988	The default Japanese UNIX/Linux code pages map the \ (0x5C) character to a Japanese character (0x7F), which causes problems in agent deploys from Windows TEMS to Japanese UNIX/Linux agent machines where the deploy agent code does not recognize the character as a \ and does not build the agent bundle depot correctly as a result.
IY82424	Take Action or Policy Commands directed at a z/OS(R) or OS/400(R) agent do not return their status data.
IY82431	Agents exhibit memory leak when processing historical reports.
IY82785	TEMS abends while processing history data record.

Tivoli Enterprise Monitoring Server APARs

The following APARs are addressed in Fix Pack 004:

APAR number	Symptom
IY82480	ITM 6.1 situation system action and attribute substitution fails.
IY85059	UNIX Log Agent situation does not fire when using 'scan for string within a string'.
IY86655	On Solaris 10, kdsvlunx.c crashes when attempting to validate a userid.
IY86939	Unable to delete managed system nodes.
IY87142	The ″tacmd addsystem″ command fails when running for the Solaris UNIX OS agent that is running as a non-root user.
IY87255	Changing or authoring policies causes high CPU usage by the TEMS.
IY87850	TEMS will not shutdown if kfaxcmon.c receives an error when executing KLE_XCFOpen().
IY88090	TEMS crashes when one situation fires.
IY89086	TEMS address space looping and/or using alot of CPU.
IY89212	SOAP users were only allowed to raise ″sampled″ events using CT_Alert method.
IY89229	IBM Tivoli Monitoring sends some Tivoli Enterprise Console events that are larger than 4K.
IY89584	TEMS crashes if agents do not provide the HOSTINFO and SYSNAME heartbeat column information.
IY89913	During DUPER processing, error messages are generated indicating that duplicate access list records are being inserted.
IY89918	Error messages indicating code <1136> are displayed when a situation’s distribution is modified.
IY89987	Very high CPU usage on hub TEMS in scale configuration.

APAR number	Symptom
IY89989	After upgrading Solaris 9 remote TEMS from OMEGAMON 350 to ITM 61, a core file is producing after starting it up.
IY90255	Ping response can result in no new connections to hub TEMS.
IY90352	The Warehouse Proxy Agent fails with "UserID decode failed. Status = 29″ on startup.
IY90485	Remote TEMS fails to reconnect to the hub TEMS sporadically.
IY90486	Remote TEMS reconnect leaves stale situation events at hub.
IY90508	Remote TEMS up before hub TEMS and may not propagate agent status properly upon initial connect to hub.
IY90677	Problems when retrieving OMEGAMON Mainframe Network data using NetView Web Console.
IY91123	Policy correlation-by-address is not working correctly. Sitmon fails to extract correct address from the node status entries.
IY91150	After application of 6.1.0-TIV-ITM-FP0002, transport layer defects can cause loops (High CPU usage) and/or hangs resulting in loss of connectivity.
IY91189	Abend 0c4 in KSMOMS in CSECT KO4LODGE.
IY91190	SITDB table does not get updated with new UADVISORY situations when user changes history configuration.
IY91689	ITM 6.1 communications infrastructure problem.
IY91750	The tacmd viewsystemlist fails when more than 50 records are there.
IY92033	Hub TEMS cannot create a new thread after many retries to reach FTO partner.
IY92034	Incorrect distribution of a versioned situation for OMEGAMON XE for Storage v410.
IY92036	KO41039 Error in request createUpdate. Status= 1120. Reason=.

The following APARs were fixed in previous fix packs and carried forward in Fix Pack 004:

APAR number	Symptom
IY80674	If an in-progress System Command is cancelled, the generation number of the request is zeroed to ensure the response is ignored. The request is then put back in the available pool for reuse. When a subsequent command is issued and this same request is reused, because the generation number is zero, the response to the command is discarded by the AsyncNotify process. Consequently, the requestor waits indefinitely for a response.
IY80809	TEMS shutdown hangs in KFAXCSRV.C when KFAXCMON.C receives an error executing KLE_XCFOPEN().
IY82460	Update to ″managed system list″ to add new target for situation distribution does not work.

APAR number	Symptom
IY82892	TEMS crashes when situation uses the SCAN function. Changes were made to both the portal and the monitoring server to correct the STR syntax to quote only the second argument, as follows. *STR 1,'my string' This is now interpreted correctly and accounts for the embedded space in the second argument, generating the correct value for the rule. If there are product-provided *STR functions that still contain the deprecated syntax and have a trailing space, the portal generates a syntax error 1203. The following is an example of such a function: `*STR '1 mystring '` Note the trailing space. To correct this problem, the TSITDESC.PDT *STR portion of the predicate should be modified using a Fix Pack 004 level portal to remove the first quote in the situation editor presentation of the string value. Save your changes - this will rebuild the PDT correctly. Product-provided situations should use quotes around only the second argument.
IY83327	On multiple interface hosts where users may need to manually specify this value to regain connectivity. The connectivity issue is caused by the selection of an unreachable server interface on the client side.
IY83945	Running SPUFI and it was wiping out the cms registration. The kdstsns command is laid down in the cms directory it uses the kbhenv environment which sets the KDH_SERVICEPOINT, which in turn wipes out the cms registration.
IY85130	Startup processing when there are many custom manage lists incurred an enormous performance penalty due to inefficiencies in the nodelist expansion for user access lists. The TEMS would appear to be hung, but it was really just behaving poorly. The key to the issue was large number of custom manage lists.
IY86835	TEMS loops at startup.
IY87814	SYSPLEX product unable to collect data.
IY87850	TEMS shutdown hangs in kfaxcsrv.c when kfaxcmon.c receives and error executing kle_xcfopen().
IY87851	TEC events not forwarded w/ single quotes in managed system name.
IY87856	When a remote TEMS loses connectivity to the hub TEMS it is not always able to reconnect successfully.
IY87694	A SOAP request with a filter tag using HGBLSTMSTMP will crash the TEMS against ISITSTSH table.
IY87897	Direct TEMA to bind to specific ip or interface.
IY79123	A remote V350 or V360 TEMS connected to an ITM 6.1 TEMS HUB abends during startup. Various abends can result because the cause is a storage overlay in the remote TEMS. The storage overlay is a SOC 4 U0000.
IY79554	TEMS abends while processing history data record
IY79774	TEMS crashed when distributing a Situation with 21 scan functions.
IY79799	Trying to create UNIX OS situations using the ″File_Information″ attribute group, but every situation created shows a status of ″Problem″. These exact same situations worked in version 350, but do not work in ITM V6.1. There is no error message to say what the problem is and there is nothing in the logs to go on.
IY79985	Agent offline situation events not forwarded to TEC server (all platforms).

APAR number	Symptom
IY80322	Single quote in attribute data causes TEC server event parsing error
IY80433	The problem occurs when the user requests historical data collection of the TEMS TEIBLOGT table from a REMOTE TEMS.
IY81467	When the afilter tag is used against a z/OS(R) TEMS, the value remains in ASCII. The SELECT built by SOAP is not valid on z/OS with an ASCII value for non-UTF8 column.
IY81988	Installation of any additional agent (non Operating System) on Linux RedHat from TEPD fails if the locale is set to JA_jp.EUCJP.
IY82221	Need OTEA event mapping changes to match changes in BAROC files.
IY82471	Due to a problem in the msg slot formatting code, attributes name in the msg slot may be truncated. Also enum attribute values are not properly replaced with external values.
IY82475	When the TEC server is down, TEC event will be stored in the EIF cache file. When the cache file is full, the TEC EIF tec_put_event call will take upward of 2 minutes before it returns. This causes send requests to be backed up in the request queue causing memory growth.
IY82476	Situation events containing an attribute with the name ″state″ is not properly prefixed with the application prefix when being translated to a TEC event causing parse error on the TEC server.
IY82786	ITM610 TEP TakeAction command request directed to an ITM610 based Z/OS agent does not return a result status to the TEP UI.
IY82789	Agents can exhibit a gradual growth in memory utilization when reports for historical data are issued from the TEP.
IY82851	The Warehouse Proxy crashes when he attempting to insert a converted table name in the WAREHOUSEID column.
IY83311	Workspace views using filters eventually goes blank with no data after a continual automatic refresh.
IY83965	The TEMS goes in to a loop with high CPU and memory growth.

Tivoli Enterprise Portal APARs

The following APARs are addressed in Fix Pack 004:

APAR number	Symptom
IY88515	SUMPERF/SUMCAP/SUMAVAIL ″CUSTOM SQL″ queries do not work out of the box.
IY89377	If a TakeAction command containing a colon is saved and re-edited, all text up to and including the colon will be deleted.
IY89657	During the call to buildPresentation and WorkspaceMigrationUtility, all workspaces were not migrated correctly.
IY89875	Setting on ras1 trace of FLOW for SituationFormula will show entering collectPredicateInfo, but never shows exiting the function.
IY90222	Within the Topology view, the icon that represents the Tivoli Enterprise Portal Server shows offline without Server information.
IY90283	Historical view in TEPS does not show additional pages.
IY90323	Making changes to queries do not keep their settings.
IY90370	Creating a query that uses string attributes fails on the Linux OS agent Tivoli Enterprise Portal Server.

APAR number	Symptom
IY90515	When using the TEP browser client, the top level situation cannot be seen.
IY90633	The situation monitor changes the sitlogic to unusable SQLs.
IY90658	Duplicate SQL statement sent by TEPS to the warehouse.
IY90963	KFWITM071E Collection status request for < Mainframe Networks > at < null > failed: java.lang.NullPointerException when selecting a product from the Historical Data Collection configuration dialog.
IY90977	CMW created situations with the Local_Time.Time attribute are not editable via the situation editor.
IY91208	When launching in context into the TEP using the new FP3 APIs, the portal does not display situation information.
IY91305	ITM 6.1 sending TEC events to the TEC server which are too large (greater than 4k).
IY92766	Some workspaces vanish when new workspaces are created.

The following APARs were addressed in previous fix packs and carried forward in Fix Pack 004:

APAR number	Symptom
IY79662	Export to .csv file function failing to output historical data.
IY80530	TEP user can see certain navigator items that are not in their ″allowed applications″ list.
IY81417	TEP crashes when using the tep situation editor to edit omegamon xe for cics on z/os product provided situations.
IY81694	Attribute substitution in universal message action doesn't work in correlated situations.
IY81870	Adding a TEC console view to a workspace, but cancelling the TEC info dialog; the TEC info prompt is still presented. Workaround: To resolve any pre-existing problems of the being prompted for TEC information when a TEC console icon was drug into a workspace and then cancelled, delete the workspace that prompts for TEC Information and create a new workspace identical to that workspace. Save the Navigation view.
IY81881	Cannot use pound sign in value of situation predicate.
IY82484	The Manage Tivoli Enterprise Monitoring Services utility needs to have the -dcnp.navigator.branch.pagesize=100 parameter added to it.
IY82582	Event workspace is too large with display set to 1024x780
IY82638	Situation take action editor places extra quotes around system command.
IY82773	Portal displays situation both with and without underscores.
IY83733	TEP desktop fails to start with the -d parameters for http proxy and port.
IY84608	Kfwitm220e error when attempting to view historical situation.
IY84691	**Remove managed system** option is missing from the physical navigator tree.
IY84812	Pasting text from excel introduced control characters into situation definitions that caused errors on export.
IY85060	TEP is showing negative values when looking at historical summarized performance. The negative values are shown for the attributes: Processor performance (avg over months):processor interrupts/sec, Memory performance (avg over months):page faults/sec

APAR number	Symptom
IY85540	Reconfiguring the historical collection of a universal agent application fails as the lower buttons are greyed out.
IY85582	Truncation is occurring in take action command when a : (colon) is used.
IY86084	Custom physical navigator doesn't order managed systems alphanumerically.
IY74835	2035-NOT_AUTHORIZED error when trying to open a dead letter queue.
IY76788	SYSPLEX managed systems not displayed in physical navigator tree.
IY79546	Situations stopped when started running for no more than a few minutes.
IY79860	KFWITM023W error during situation edit specifying an action.
IY82892	TEMS crashes when a situation is distributed if the SCAN function argument is not enclosed in quotes.

Tivoli Enterprise Portal Server APARs

The following APARs are addressed in Fix Pack 004:

APAR number	Symptom
IY82206	Situation status is not updated when status changes.
IY89021	Workspace migration utility fails during upgrade to Fix Pack 003 in SQL Server environment.
IY89043	User IDs created for TEP while TEPS is connected to a case sensitive HUB TEMS that is enabled for user validation were not usable after upgrade to ITM 6.1 Fix Pack 3.
IY89602	MIGRATE-EXPORT.SH or MIGRATE-IMPORT.SH hangs when executing.
IY89647	TEPS fails to start on Linux after migrate-export is executed.
IY89654	The Summarization and Pruning agent creates tables incorrectly if KFWHISTBEHAVIOR does not exist in TEPS.
IY89694	Fix Pack 003 util.jar does not get downloaded when the Tivoli Enterprise Portal browser connects to the Tivoli Enterprise Portal Server through the java plugin, causing a failure.
IY89808	SQL0433N messages in TEPS log when it tries to import the results from most SYSPLEX situations.
IY89990	Occasional memory access violation in KFWSERVICES when managed system lists are retrieved.
IY91196	The TEPS consumes excessive memory resources, causes performance to slow down, and the TEPS may die.

The following APARs were addressed in previous fix packs and are carried forward in Fix Pack 004:

APAR number	Symptom
IY82270	Acknowledgement ″notes″ not updated properly when highlighting and acknowledging multiple situation events.
IY84784	The migrate-export utility shuts down the portal server.
IY86056	DOS2UNIX failure to convert files in importagentteps.sh causes the application support not to complete correctly.
IY86849	Running migration-export.bat as described in ITM 6.1 Administrators Guide cannot work as it contains a wrong database name.

APAR number	Symptom
IY87991	Situations are shown as stopped in the portal after switching from a remote TEMS to another.
IY87072	The migrate-import.bat has to run under control of db2admin user ID.
IY74835	2035-NOT_AUTHORIZED error when trying to open a dead letter queue.
IY76788	SYSPLEX managed systems not displayed in physical navigator tree.
IY79224	Situation severities are not correctly transferred to TEC.
IY79546	Situations stopped when started running for no more than a few minutes.
IY79860	KFWITM023W error during situation edit specifying an action.
IY81400	CTIRA_HOSTNAME value used to set up clustered agents to provide a unique windows system name in the TEP navigator is ignored.
IY84078	After completing the installation of the 6.1.0-TIV-ITM_TEPS-FP0001 patch, the TEP client renders a different set of workspaces at the Enterprise node level for DE licensed customers.

Tivoli Data Warehouse APARs

The following APARs are addressed in Fix Pack 004:

APAR number	Symptom
IY86540	When the number of characters of the variable KSZ_CLASSPATH exceed a certain value, the Summarization and Pruning agent will not start. Infinite loop when parsing the KSYENV file.
IY88012	The Summarization and Pruning agent does not end successfully when processing tables with names of 30 characters, like:AMX_DMXCpu_Percent_usage_CPU .
IY88651	The Warehouse Proxy Agent is crashing after ODBC error, ORA-01461, occurs.
IY88960	Problems with the Summarization and Pruning agent trying to validate timestamps.
IY89003	The Summarization and Pruning agent fails with the following error java.sql.SQLException: ORA-00001: unique constraint (ITMUSER.WHID_IDX) violated.
IY90242	Data is being sent by the Warehouse Proxy Agent, but no data is being written to the database.

The following APARs were addressed in previous fix packs and are carried forward in Fix Pack 004:

APAR number	Symptom
IY80894	Summarization and Pruning agent does not work correctly on when Warehouse database is on Oracle. The historical data are correctly loaded. However, summarization does not work and summarization tables are not created and filled for any resources for which the summarization was enabled. Also Pruning does not work.
IY82223	I found out that there is something in the remote control product (in this case DAMEWARE) that is affecting the operation of the Summarization and Pruning Agent (SPA). When one logs off the Windows account, then disconnects the remote control product, the SPA will be shut down.
IY82881	Summarization and Pruning agent does not properly handle the IBM Tivoli Monitoring 5.x tables.
IY87206	Summarization and Pruning agent fails with a SQL error: SQLCODE: -805 SQLSTATE: 51002

APAR number	Symptom
IY79253	Warehouse migration tool issue: UNIXDISK table is not migrated. The warehouse proxy agent older than V350 was changing the Disk table name to UNIXDISK and User to UNIXUSER for the UNIX agent. It was also changing the column name User to User_Name for the table OS400_Job for the OS400 agent. This behavior disappeared at V350. For all the customers that created those tables with a Warehouse Proxy version previous to V350, the migration tool is now successfully migrating the UNIXDISK table to the Disk table, the UNIXUSER table to the User table, and the User_Name column to the User column.
IY80343	The Summarization and Pruning agent is failing to summarize the table SYSTEM Error, which results in the log showing the following error trying to alter the table: ALTER TABLE ″ITMUSER″.″SYSTEM″ ADD ″LOAD_AVERAGE_1_MIN″ NUMERIC (31,2) For an unknown reason the data type of the column LOAD_AVERAGE_1_MIN had been created with a datatype Decimal in the MSSQL warehouse database. This datatype was not recognized by the S&P agent. Which is expecting a numeric datatype in that case. The S&P has been modified to recognize this datatype as well.
IY80350	The Warehouse Proxy crashes when it must insert a conversion for a table name in the WAREHOUSEID table.
IY80971	When using the warehouse migration tool, the tables are created in the Warehouse database without the index on the ORIGINNODE, TMZDIFF, WRITETIME.
IY83743	The SQL UPDATE statements used during summarization take a long time to complete when using MS SQL Server 2000 in the back end.
IY84092	Daylight Savings Time change causes the Summary and Pruning Agent to process all data.
IY84255	The aggregation agent fails during processing due to an unexpected column.
IY84290	MS SQL Server 2000 FP3 JDBC driver fails when there are a large number of tables with many columns configured for aggregation. The SQL Server will generate several exceptions including ″Out of Memory″ exception.

Tivoli Enterprise Console APARs and defects

The following product defects were addressed in a previous fix pack and carried forward in Fix Pack 004:

- The omsync_maxentries configuration parameter of the omegamon.rls rule set file is not being honored.
- AIX only: TEC_FP1:Errors appear on terminal during console installation
- No backup of rule base
- Manual restart of TEC Server
- Loading Default rule base at end of uninstall

The following APARs were addressed in a previous fix pack and carried forward in Fix Pack 004:

APAR number	Symptom
IY81615	A pair of missing brackets in the omegamon.rls rule set file is causing 3 extra spaces to appear in the rules.trace file each time a rule is run. The brackets are missing from the check_sitforwarder_status timer rule, which by default runs every 10 minutes to check the status of the situation update forwarder, causing the file to grow to a large size.
IY84931	The installer checks every rule base for sentry.baroc and updates all rule bases that do not have sentry.baroc.

APAR number	Symptom
IY82191	In the rule set file omegamon.rls the administrator field is not being set when a situation received from IBM Tivoli Monitoring V6.l causes a Tivoli Enterprise Console event to be acknowledged or closed.

i5/OS OS monitoring agent APARs and defects

The following APARs are addressed in Fix Pack 004:

APAR number	Symptom
IY90659	Vision replication software causes i5/OS agent failures.
IY89976	IBM Tivoli Monitoring, V6.1 OS400 agent, QAUTOMON, is missing authority. i5/OS may hang with lack of authority on the system *PGM objects QNMDRGFN, QNMRGFN ,QPMLPFRD, and QPMWKCOL if data for performance collection services is collected.
IY88686	Garbage characters are found in unicode data and help text attributes in situations.

The following APARs were addressed in previous fix packs and are carried forward in Fix Pack 004:

APAR number	Symptom
IY82162	ITM agent loops when TCP/IP subsystem is shutdown. When the customer wants to perform a backup of the system, they bring down the TCP/IP subsystem. When they do that, the ITM 6.1 agent starts looping and consumes lots and lots of CPU (90%). Additional Information: Immediate workaround is to stop the agent before stopping TCP/IP and start the agent after the TCP/IP servers are started.
IY82485	When a situation checks for specific message ID in QSYSOPR, MSG. Situations that use the OS400_Message query receive the same message events repeatedly.
IY82901	Job resource details not displayed if subsystem name is blank. Some jobs would not display job resource details data when selected from the job resource table. The job resource details view displayed but no fields contained values. This occurred if the job's priority was zero, indicating a system job not assigned to a subsystem. Response time of the "Job Resource Information" view in "Jobs and Queues" workspace is improved. Job list will display quicker than before. To take advantage of this fix on OS/400 V5R2 you must install OS/400 option 12, OS/400 - Host Servers. If option 12 is not installed then the existing code will be used for the OS400_Job attribute group. If option 12 is installed, or if you are using i5/OS V5R3 or V5R4 then the new code delivered with this fix will be used. Additional Information: A query was changed in fix pack 2 to allow system jobs to display information. That change partially fixed this APAR. This fix pack completes the fix for the job resource details display being too slow.
IY83540	The ITM 6.1 agent for I5/OS pure event situation OS_400_SPOOL always fires. Situations that use the OS400_Message query receive the same message pure event repeatedly.
IY80507	Incorrect ODI change occurs for OS400_MESSAGE. Error message "KFWITM051 The Display Item feature cannot be used with this situation because you can only use Attributes from groups that return multiple rows. OS400_message does not return multiple rows." was received when attempting to use the 'Advanced->Display Item' function with an OS400_Message query in a situation.

APAR number	Symptom
IY80641	Performance problem with real-time monitoring. There were performance issues while doing real-time monitoring with ITM 6.1 agent. The time to display several of the predefined workspaces was too long. For certain workspaces, like Disk and I/O, the agent waited a certain time interval between collecting the performance related data and this time period was not acceptable.
IY82092	Disk usage percentage of ITM 6.1 I5/OS agent can show as negative. The Percent Used field in the Disk Unit table of the Disk and I/O workspace could show incorrect values including negative percentages. The computation would fail if the disk capacity or disk space used number of bytes was greater than about 21,475,000 kilobytes.
IY82901	Job resource details not displayed if subsystem name is blank. Some jobs would not display job resource details data when selected from the job resource table. The job resource details view displayed but no fields contained values. This occurred if the job's priority was zero, indicating a system job not assigned to a subsystem.

The following product defects were addressed in a previous fix pack and carried forward in Fix Pack 004:

- In the APPN Topology workspace the fly-over text doesn't match the table column header. There is no fly-over text for "Time", the fly-over text for "Time" appears in the next column header for "Node Congestion", and this continues through the rest of the window, each fly-over being the one for the header before.
- On the CFGOMA, Configure i5/OS Monitoring Agent, command a *NONE parameter can't be set for the port numbers.
- Added two attributes to the OS400_Job attribute group. The two new attributes are: Time Active - The amount of time (in seconds) that the job has been active, or zero if the job is not currently active. Time in System - The amount of time (in seconds) that the job has been in the system.
- Various exceptions occur using workspaces and situations including: MCH3601 exceptions with performance collections; agent fails on system with more than 10,000 jobs; agent fails when ending APPN related situation. Storage pool reports were inaccurate and slow

Linux OS monitoring agent APARs

The following APAR was addressed in previous fix packs and are carried forward in Fix Pack 004:

APAR number	Symptom
IY82465	The Linux OS Agent does not report CPU values correctly on long running systems.

Universal Agent APARs

The following APARs are addressed in Fix Pack 004:

APAR number	Symptom
IY80522	If the SNMP DP is collecting MIB data from a clustered system and the response to an SNMP GET request for a MIB variable arrives from a different IP address than the one which was the target of the request, the SNMP DP rejects the response as invalid and the TEP workspace does not get updated with that data row.
IY87545	Data does not appear for attribute groups in Socket data provider.
IY87828	API CLI port numbers saved as negative numbers in kumpinit file.

APAR number	Symptom
IY88033	UA shutdown occurs on Solaris platform even though the itmcmd agent um stop command was not issued.
IY88189	Hung script data provider processes on Linux 390 and Solaris not always terminated.
IY88799	UA odbc handler strips off leading @ characters before passing to odbc driver causing system variable such as @time to become time and the odbc driver returns sql errors.
IY89309	A UA startup that involves hundreds of monitored files, situations, and other high-volume activity, can result in a UA deadlock.
IY89659	UA must supply full host address information for TEC integration.
IY90523	UA summarization stops working due to deadlock.
IY90530	UA holds monitored file lock too long due to slow performance.
IY91110	UA abends at startup when loading mdl with invalid //APPL statement.
IY91461	Invalid HOSTNAMEACT:UAGENT00 entries inserted into the TEMS NODESTATUS table.
IY92443	HTTP 407: Proxy agent requires authentication not being handled.

The following APARs were addressed in previous fix packs and are carried forward in Fix Pack 004:

APAR number	Symptom
IY79012	On UNIX platforms, directly running KUMPCON causes KUMPV599E error
IY82812	UA metafile parser should not allow leading digit in APPL name
IY84293	Script DP not treating multiple arguments separately on UNIX platforms
IY84694	um_cleanup script does not remove UA work files from Linux-based TEPS
IY85346	TTL defaults to 0 for API and Socket Event tables, results in loss of data
IY85413	ManagedSystemName SOURCE parameter not supported in ODBC metafiles
IY85565	UA restart fails on UNIX/Linux platforms with an error message indicating that DCH port 1919 is already in use. This problem occurs if the Script Data Provider launched a script during the previous UA startup, and that script hasn't exited.
IY85529	If a script outputs greater than 4096 bytes in one script execution, the output data line at the 4K boundary is incorrectly broken into two separate rows.
IY86181	UA restart fails if script launched from Script DP is still running
IY86404	Redirected Socket DP table goes offline before its expiration time
IY86814	Socket DP record prefixing fails if using ManagedSystemName and UA instance
IY78337	Unreliable data delivery when Socket DP metafile uses invisible table
IY81503	File DP COPY mode fails if first file record is blank
IY81922	Dynamic filename switches not occurring
IY82435	UA crashes if derived attribute function has null input
IY82436	Script stops outputting data on UNIX if interrupt signal received
IY82438	Active stderr pipe on UNIX blocks stdout data in same script execution
IY82767	ENVFILE values not being set for script process on UNIX platforms
IY83756	Fix Socket DP handling of fully qualified hostnames
IY83757	Hung Script DP processes on AIX not always being terminated
IY85529	Large Script DP output > 4K not handled correctly
IY85697	File DP data sometimes displays in TEP under wrong managed system name

UNIX Log Agent APARs

The following APARs are addressed in Fix Pack 004:

APAR number	Symptom
IY87360	IBM Tivoli Monitoring, V6.1 UNIX Log Agent consumes high CPU.
IY89775	System slot in log entries view of AIX kul agent don't show correct hostname for /VAR/ADM/ERRLOG.
IY90902	Corrupt entries in the Description field of AIX errlogs.

The following APARs were addressed in previous fix packs and carried forward in Fix Pack 004:

APAR number	Symptom
IY83266	The agent's BAROC file used a reserved keyword ("class") as a slot name.
IY83975	The resource field of AIX errlogs is not mapped into the data collected by the UNIX Log Agent.
IY80825	The UNIX Log Agent does not display error log entries on 64-bit AIX systems.
IY81251	The UNIX Log Agent does not display log entries from utmp-style logs on 64-bit HP-UX systems.
IY81759	The Source and Description attributes for syslog entries are the same.

UNIX OS monitoring agent APARs

The following APARs are addressed in Fix Pack 004:

APAR number	Symptom
IY84291	UNIX agent doesn't go offline at TEMS after agent shutdown.
IY86207	The tacmd updateagent install does not stop the agent.
IY89636	UNIX Historical Workspace queries do not return data - Queries fail.
IY91526	UNIX OS Agent reports wrong Disk Utilization values.

The following APARs were addressed in previous fix packs and carried forward in Fix Pack 004:

APAR number	Symptom
IY83133	Incorrect percentages in TEDW for Unix agent.
IY83614 IY86219	No data for virtual memory stats on Solaris 8 when LANG=JA.
IY83868	Unable to export data from "System Detail" workspace view.
IY84123	Summarization and Pruning Agent improperly pruning UNIX OS, UNIX CPU, UNIX PROCESS and UNIX NFS tables
IY84933	UNIX OS agent does not support disk volumes over 2,147,483,647 and UNIX OS agent displaying negative numbers and values greater than 2,147,483,647 display negative numbers in portal fixed in UNIX OS and UNIX CPU tables
IY85020	UNIX OS agents fail to report 1 MIN and 15 MIN load averages for 64-bit AIX

APAR number	Symptom
IY85880	Seed file KUX_KCJ.SQL has all the -102 properties set to the default framework type. Thus, all UNIX workspace links failed when an OM350 agent is connected to an ITM 6.1 TEPS.
IY80163	On AIX 5.1 and 5.2 machines both On-line and Off-line Cpu's are displayed. Display only On-Line Cpu's similar to AIX 5.3.
IY80584	UNIX agent "LOGIN_TIME" column is null when no users logged-on, which in turn causes Summarization and Pruning Agent to fail.
IY80820	ITM 6.1 UNIX OS agent on HP-UX 11.11 cannot handle more than 20 PPAs. Systems with more than 20 PPAs (network interfaces) crash because the agent overwrites the bounds of the PPA array.
IY81880	ITM 6.1 UNIX OS agent on Solaris 8 64 bit crashes.
IY83133	Improper percentages in data warehouse for UNIX system VIRTUAL% on 32-bit.

Windows OS monitoring agent APARs

The following APARs are addressed in Fix Pack 004:

APAR number	Symptom
IY84072	Disk drive partitions that do not have an associated drive letter are not supported by the current agent and should be.
IY84811	Created a situation that monitors file size on a file that could be in different directories. I get no events from either file when the condition is true.
IY82493	Systems with a hidden partition and no drive letter assigned experience this issue. Also, the symptom does not appear until history collection is configured for Warehouse, and collection begun. With history collection off, the issue is not present.

Appendix C. 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.

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, DB2, i5/OS, iSeries, OMEGAMON, OS/400, pSeries, 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.

Intel is a trademark 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 is a registered trademark of Microsoft 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.

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

GI11-8053-00