Tivoli® IBM Tivoli Monitoring

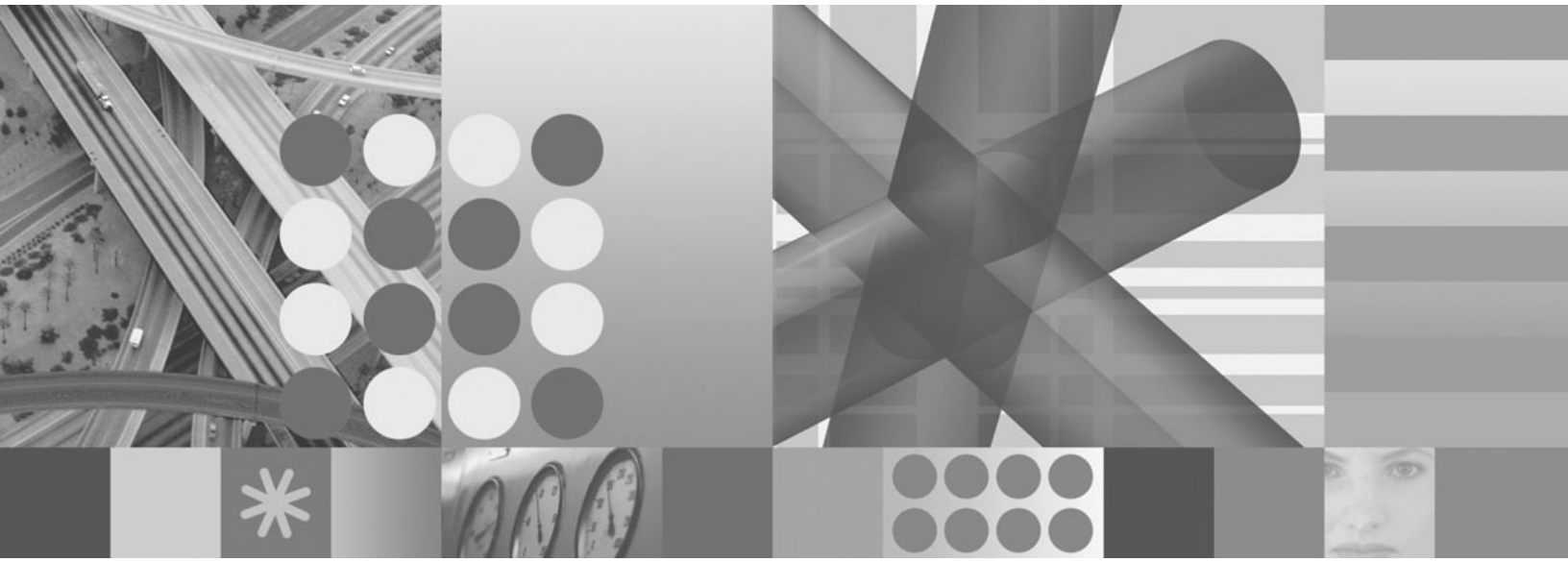
Version 6.1

Fix Pack 6 Readme and Documentation Addendum

GI11-8125-00

Tivoli® IBM Tivoli Monitoring

Version 6.1



Fix Pack 6 Readme and Documentation Addendum

GI11-8125-00

Note
Before using this information and the product it supports, read the information in “Notices,” on page 117.

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

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

Contents

Figures v

Tables vii

Chapter 1. Fix Pack 6 overview 1
Supported operating systems 3
Supported databases for Tivoli Enterprise Portal Server and Tivoli Data Warehouse 8

Chapter 2. Planning your fix pack installation 11
Determining which components need to be upgraded to Fix Pack 6 11
General guidelines for upgrading components 11
Determining which components are present on a specific computer 12
Sequencing the upgrade procedures 12
Base versus application monitoring agents 14
Fix pack installation planning worksheets 14
Preserving user customizations 17
Files that are preserved on upgrade 17
Files that are not preserved on upgrade 18
Special exceptions 18
Changes in the behavior of the autostart scripts 19
Understanding the GA versions of the IBM Tivoli Monitoring version 6.1 agent CDs for Windows platforms 20
Identifying a refreshed version of IBM Tivoli Monitoring agent CD images 21
Summary of this section 21

Chapter 3. Fix pack installation instructions 23
Locations of installation logs 24
Preparing for installation 26
Overall preparations for Daylight Savings Time (DST) issues 26
Adapting to Daylight Savings Time in the United States 26
Backing up IBM Tivoli Monitoring 26
New (non-upgrade) installation checklist 29
Single-server quick installation checklist 31
Monitoring server checklist 34
Portal server checklist 37
Portal desktop client checklist 40
Monitoring agent checklist - local installation 41
Monitoring agent checklist - remote deployment 43
Validating what you installed 46
Sample output for the kincinfo command on Windows 47
Sample output for the cinfo command on UNIX or Linux 50
Installing the fix pack for the i5/OS monitoring agent 51
Special instructions 52
Installing the i5/OS agent fix pack checklist 52
Installing the IBM Tivoli Enterprise Console event synchronization fix pack 54
Determining which level of event synchronization is installed 54
Fix pack prerequisites 55
Notes regarding rule bases 55
Important information for Windows users 56
Installation instructions 57
Modifying your rule base after installation. 61
Closing sampled events in IBM Tivoli Enterprise Console 61
Verifying the installation of the event synchronization fix pack 62

© Copyright IBM Corp. 2007

Uninstalling the IBM Tivoli Enterprise Console event synchronization 62

Chapter 4. After you finish installing the fix pack 65
Clearing the Tivoli Enterprise Portal browser cache 65
Determining what components were installed 65
Installing Global Services Kit (GSKit) if you use silent installation 65
Securing your Linux or UNIX IBM Tivoli Monitoring installation 65
secureMain 66
Installing the upgrade toolkit on Solaris computers 67
Installing Java Web Start 68
Installing upgrades to monitoring agents 68
Understanding deployment options 68
Tivoli Widget Sample Utility 68
IBM Tivoli Open Process Automation Library (OPAL) 68

Chapter 5. Known limitations and workarounds 71
General installation and configuration issues 71
Installation 71
Configuration 74
IBM Tivoli Enterprise Console installation and configuration 75
Documentation of installation and configuration 76
Remote deployment issues 82
Tivoli Enterprise Monitoring Agent 84
Tivoli Enterprise Monitoring Server 85
Tivoli Enterprise Monitoring Server on distributed platforms issues 86
Tivoli Enterprise Monitoring Server on z/OS systems issues 89
Tivoli Enterprise Portal desktop and browser clients 92
Tivoli Enterprise Portal Server 93
Historical data collection issues 97
Summarization and Pruning Agent 99
Warehouse Proxy Agent 101
Tivoli Universal Agent issues 102
Globalization 103
Online help 104

Chapter 6. APARs addressed by Fix Pack 6 107
Documentation APARs 107
Installation component APARs 107
Event Synchronization APARs 108
Tivoli Enterprise Monitoring Agent APARs 108
Tivoli Enterprise Monitoring Server APARs 109
Tivoli Enterprise Portal APARs 111
Tivoli Enterprise Portal Server APARs 111
Tivoli Data Warehouse APARs 112
Tivoli Universal Agent APARs 113
i5/OS monitoring agent APARs 114
Linux OS monitoring agent APARs 114
UNIX OS monitoring agent APARs 114
Windows OS monitoring agent APARs 115

Appendix. Notices 117
Trademarks 118

Figures

1. Installation flow for upgrading a monitoring environment to Fix Pack 6. 1
2. Levels for all components following the installation of Fix Pack 6 47

© Copyright IBM Corp. 2007

Tables

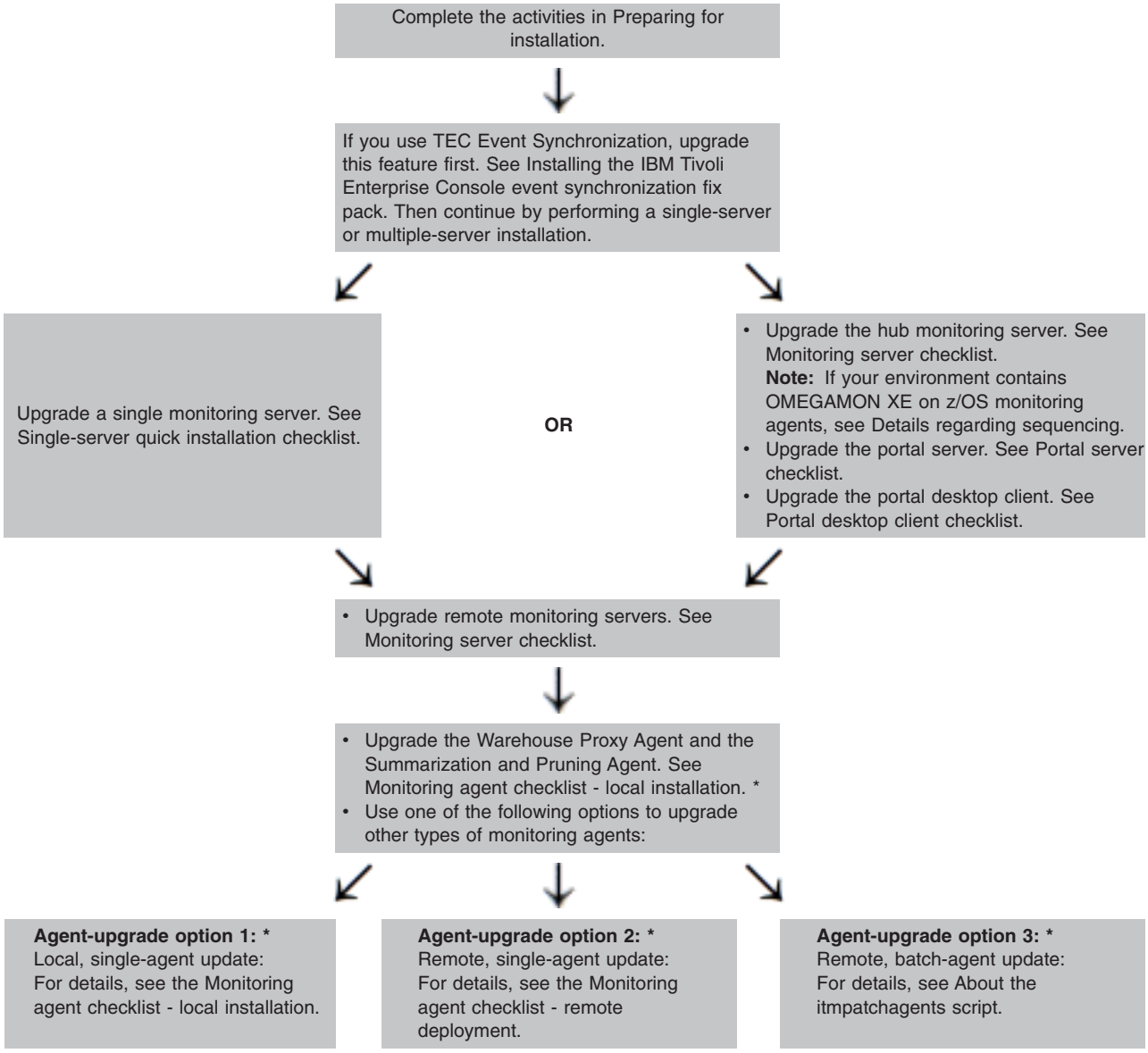
1. Fix Pack 6 file names 2
2. Supported Windows operating systems for IBM Tivoli Monitoring V6.1 Fix Pack 6 monitoring components 3
3. Supported UNIX, i5/OS, and z/OS operating systems for IBM Tivoli Monitoring V6.1 Fix Pack 6 monitoring components 4
4. Supported Linux operating systems for IBM Tivoli Monitoring V6.1 Fix Pack 6 monitoring components 5
5. Supported databases for the portal server 8
6. Supported databases for the Tivoli Data Warehouse 9
7. Overall planning steps for Fix Pack 6 11
8. Fix pack planning worksheet 15
9. Overall installation steps for Fix Pack 6 23
10. Installation and startup log file names and locations 24
11. Checklist for a new (non-upgrade) installation 29
12. Checklist for installing the fix pack on a local host computer 31
13. Checklist for installing the fix pack on the monitoring server on distributed platforms 34
14. Checklist for installing the fix pack on the monitoring server on z/OS systems 36
15. Checklist for installing the fix pack on the portal server 38
16. Checklist for installing the fix pack on the portal desktop client 40
17. Checklist for locally installing the fix pack on an agent 41
18. Checklist for remotely deploying the fix pack to an agent 43
19. Checklist for remotely deploying the fix pack to an i5/OS agent 52
20. Determining the level of IBM Tivoli Enterprise Console event synchronization installed by platform 55
21. Rule base options for IBM Tivoli Enterprise Console event synchronization 57
22. Configuration fields IBM Tivoli Enterprise Console event synchronization 58

© Copyright IBM Corp. 2007

Chapter 1. Fix Pack 6 overview

Fix Pack 6 for IBM Tivoli Monitoring includes the fixes delivered in previous Version 6.1.0 fix packs plus additional fixes. This readme and documentation addendum document provides details about installing the fix pack and information about its changes to IBM Tivoli Monitoring. Chapter 6, “APARs addressed by Fix Pack 6,” on page 107 lists APARs that are fixed in Fix Pack 6 and in the interim fixes for Fix Pack 5.

The basic flow of the installation process to upgrade to Fix Pack 6 is shown in Figure 1. Refer to this figure as you work with the upgrade procedures in this document. If you are installing IBM Tivoli Monitoring components on computers that do not currently host components, see “New (non-upgrade) installation checklist” on page 29. You must upgrade or install new components according to the sequence described in “Sequencing the upgrade procedures” on page 12.



* Only the local agent-upgrade option is valid for the monitoring agents that enable historical reporting.

Figure 1. Installation flow for upgrading a monitoring environment to Fix Pack 6

© Copyright IBM Corp. 2007

You can download the IBM Tivoli Monitoring, Fix Pack 6 files from Passport Advantage® or from the **Downloads** section of the IBM® Software Support Web site: http://www-306.ibm.com/software/sysmgmt/products/support/IBMTivoliMonitoringV6.html. The files listed in Table 1 are available on the IBM Software Support Web site. See *IBM Tivoli® Monitoring Passport Advantage Readme First* for details on fix pack file names and downloading the files from Passport Advantage.

When the Fix Pack 6 image is downloaded from the IBM Software Support Web site, these rules apply:

- You may only locally install the fix pack on a system that already hosts a licensed copy of IBM Tivoli Monitoring. Similar to other upgrade software, the fix pack image cannot be locally installed on a computer where the product software is not already installed.
- You may populate agents to the depot.
- You may remotely deploy agents to existing or new installations.

When the Fix Pack 6 image is downloaded from Passport Advantage, these rules apply:

- You may locally install the fix pack on a system that already hosts a licensed copy of IBM Tivoli Monitoring.
- You may locally install the fix pack on a system that does not already host a licensed copy of IBM Tivoli Monitoring.
- You may populate agents to the depot.
- You may remotely deploy agents to existing or new installations.

Table 1. Fix Pack 6 file names

Category	Fix pack file name	Specific operating system (or application)
Windows®	6.1.0-TIV-ITM_TMV-Windows-FP0006.zip	Windows platforms
UNIX®	6.1.0-TIV-ITM_TMV-AIX-FP0006.tar	UNIX platforms - AIX®
	6.1.0-TIV-ITM_TMV-HPUX-FP0006.tar	UNIX platforms - HP-UX Integrity, HP-UX native processors
	6.1.0-TIV-ITM_TMV-Solaris-FP0006.tar	UNIX platforms - Solaris
Linux®	6.1.0-TIV-ITM_TMV-LinuxIA64-LinuxX64-FP0006.tar	Linux on x86-64 and IA-64
	6.1.0-TIV-ITM_TMV-Linuxip-FP0006.tar	Linux on pSeries®
	6.1.0-TIV-ITM_TMV-Linuxz-FP0006.tar	Linux on zSeries®
	6.1.0-TIV-ITM_TMV-LinuxIA32-1-FP0006.tar[1]	Linux Intel® platforms (Part 1 of 2)
	6.1.0-TIV-ITM_TMV-LinuxIA32-2-FP0006.tar[2]	Linux Intel platforms (Part 2 of 2)
z/OS®	PTFs for the Tivoli Enterprise Monitoring Server on z/OS	z/OS

Notes:

1. Used to upgrade all installations, *except for* computers where the Tivoli Enterprise Portal Server is running.*
2. Used to upgrade computers where the Tivoli Enterprise Portal Server is running.*

* Because of increases in the size of product components, support for Linux Intel platforms is split into two files. Some components are included on both files to satisfy installation prerequisites.

General points regarding Table 1:

- If you are running your monitoring server on a z/OS system, apply the z/OS Fix Pack 6 PTFs, available from IBM Software Support. See the “Monitoring server checklist” on page 34 for more information.
- There are no updates for help in this fix pack.
- The *IBM Tivoli Monitoring Version 6.1: Installation and Setup Guide* (Revised April 2007) (GC32-9407-00) and *IBM Tivoli Monitoring: Problem Determination Guide* (Revised April 2007)

(GC32-9458-00) were refreshed for this fix pack. If you have an older version of these documents on your workstation, download the new versions from http://publib.boulder.ibm.com/infocenter/tivihelp/v15r1/index.jsp?toc=/com.ibm.itm.doc/toc.xml.

- If you are running OMEGAMON® XE products and plan to upgrade to IBM Tivoli Monitoring version 6.1 Fix Pack 6, refer to the **Planning Upgrades** section of the following Web site for OMEGAMON XE recommended maintenance levels: http://www-306.ibm.com/software/sysmgmt/products/support/IBMTivoliMonitoringV6.html
- See "Base versus application monitoring agents" on page 14 for a description of the categories of agents, including the agent types that come with the base installation package of IBM Tivoli Monitoring.

See Chapter 3, "Fix pack installation instructions," on page 23 for detailed installation procedures.

Supported operating systems

Fix Pack 6 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 Summarization and Pruning agent. Support that was added in Fix Pack 6 is marked **New**. See Table 3 on page 4.

For the latest OS support information, see http://www-306.ibm.com/software/sysmgmt/products/support/Tivoli_Supported_Platforms.html.

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

Table 2. Supported Windows operating systems for IBM Tivoli Monitoring V6.1 Fix Pack 6 monitoring components

Operating system	Monitoring server	Portal server	Portal client[1]	OS monitoring agent[2]	Warehouse Proxy	S&P agent[3]
Windows 2000 Professional[4]			X	X		X
Windows 2000 Server	X	X	X	X	X	X
Windows 2000 Advanced Server	X	X	X	X	X	X
Windows XP[4]			X	X	X	X
Windows 2003 Server SE (32-bit) with Service Pack 1 and higher	X	X	X	X	X	X
Windows 2003 Server EE (32-bit) with Service Pack 1 and higher	X	X	X	X	X	X
Windows Server 2003 Data Center (32-bit)				X		
Windows 2003 SE (64-bit)	New	New	New	X	New	New
Windows 2003 EE (64-bit)	New	New	New	X	New	New
Windows Server 2003 Data Center (64-bit)				X		
Windows 2003 Server on Itanium				X		
Windows Vista (32-bit)[4]			X			
Windows Vista (64-bit)[4]			X			

Notes for the preceding table:

1. The Tivoli Enterprise Portal desktop client is supported on marked platforms. However, the browser client can be accessed only from Windows computers running Internet Explorer 6 or 7.
2. The **OS monitoring agent** column refers to the availability of a monitoring agent for the operating system. These and other types of agents are described in “Base versus application monitoring agents” on page 14. An "X" symbol in the column indicates that an operating system agent is available for the specific operating system that is named in the row where the "X" is located.
3. Summarization and Pruning agent
4. 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.

   Note: Closely monitor the support matrix for Windows 2000 Professional, so that you are aware of any revisions regarding this platform.

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 for IBM Tivoli Monitoring V6.1 Fix Pack 6 monitoring components

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

Table 3. Supported UNIX, i5/OS, and z/OS operating systems for IBM Tivoli Monitoring V6.1 Fix Pack 6 monitoring components (continued)

Operating system	Monitoring server	Portal server	Portal client	OS monitoring agent[1, 2]	Warehouse Proxy	S&P agent[9]
z/OS 1.9[8]	X			X		

Notes for the preceding table:

1. The **OS monitoring agent** column refers to the availability of a monitoring agent for the operating system. These and other types of agents are described in “Base versus application monitoring agents” on page 14. An "X" symbol in the column indicates that an operating system agent is available for the specific operating system that is named in the row where the "X" is located.
2. If you are installing the OMEGAMON XE for Messaging agent on a 64-bit operating system, you must install the 32-bit version of the agent framework. See the OMEGAMON XE for Messaging bullet in Chapter 5, “Known limitations and workarounds,” on page 71 for details on installing this framework.
3. To use the IBM Tivoli Universal Agent on AIX V5.3, you must apply patch level `AIX 5300-05-02`.
4. The monitoring server and the Summarization and Pruning agent can run in both local and global zones on Solaris; however, the OS monitoring agent can run only in global zones.
5. You cannot use the remote deployment function for the agents on this operating system, which applies to both fresh installations and upgrades. Instead, you must install locally.
6. For HP-UX, patch PHSS_30970 is required.
7. You cannot upgrade either the OS or Log Alert agents that you currently have running on an HP-UX 11i v2 (B.11.23) on an Integrity (IA64) computer in PA-RISC mode prior to Fix Pack 4. Fix Packs prior to Fix Pack 4 did not run in native 64-bit mode by default. You must first uninstall the agent if the version is previous to the Fix Pack 4 version.
8. For information about installing the monitoring server on z/OS, refer to the program directory that comes with that product. The OS monitoring agent for z/OS computers is part of the IBM Tivoli OMEGAMON for z/OS product.
9. Summarization and Pruning agent.

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

Table 4. Supported Linux operating systems for IBM Tivoli Monitoring V6.1 Fix Pack 6 monitoring components

Operating system	Monitoring server	Portal server	Portal client	OS monitoring agent[1, 5]	Warehouse Proxy	S&P agent[6]
Asianux 2.0 for Intel 64	X	X	X	X	X	X
Asianux 2.0 for x86-64				New		
Asianux 2.0 on Itanium® 64				X		
Red Flag 4.1 for Intel	X	X	X	X	X	X
Red Flag 5.0 for Intel	X	X	X	X	X	X
RHEL[9] 2.1 Intel				X		X
RHEL 3 on Intel				X	X	X
RHEL 3 on zSeries 31-bit				X	X	X
RHEL 3 on zSeries 64-bit				X	X	X
RHEL 4 Intel	X	X	X	X	X	X
RHEL 4 on x86-64				X		
RHEL 4 on Itanium 64-bit				X		

Table 4. Supported Linux operating systems for IBM Tivoli Monitoring V6.1 Fix Pack 6 monitoring components (continued)

Operating system	Monitoring server	Portal server	Portal client	OS monitoring agent[1, 5]	Warehouse Proxy	S&P agent[6]
RHEL 4 on iSeries® and pSeries				X		
RHEL 4 on zSeries 31-bit	X	X		X	X	X
RHEL 4 on zSeries 64-bit	X[3]	X[3, 4]		X	X	X
RHEL 5 Intel[7]	X	X	X	X[8]	X	X
RHEL 5 on x86-64[7]				X[8]		
RHEL 5 on Itanium 64-bit[7]				X[8]		
RHEL 5 on iSeries and pSeries[7]				X[8]		
RHEL 5 on zSeries 31-bit[7]				X[8]		
RHEL 5 for zSeries 64-bit[7]	X[3]	X[3, 4]		X[8]	X	X
SLES[9] 8 Intel				X	X	X
SLES 8 for zSeries 31-bit				X	X	X
SLES 8 for zSeries 64-bit				X	X	X
SLES 9 Intel	X	X	X	X	X	X
SLES 9 on x86-64				X		
SLES 9 on Itanium 64-bit[2]				X		
SLES 9 for iSeries and pSeries				X		
SLES 9 for zSeries 31-bit	X	X		X	X	X
SLES 9 for zSeries 64-bit	X[3]	X[3, 4]		X	X	X
SLES 10 Intel	X	X	X	X[8]	X	X
SLES 10 on x86-64				X[8]		
SLES 10 on Itanium 64-bit[2]				X[8]		
SLES 10 for iSeries and pSeries				X[8]		
SLES 10 for zSeries 64-bit	X[3]	X[3, 4]		X[8]	X	X

Notes for the preceding table:

1. The **OS monitoring agent** column refers to the availability of a monitoring agent for the operating system. These and other types of agents are described in “Base versus application monitoring agents” on page 14. An "X" symbol in the column indicates that an operating system agent is available for the specific operating system that is named in the row where the "X" is located.
2. You cannot use the remote deployment function for the OS agent on this operating system, which applies to both fresh installations and upgrades. Instead, you must install locally.

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

   ```
   KUICCN064E An appropriate installation image for the target platform, LINUX,
   could not be found on the local server.
   ```
3. This component supports the operating system in 64-bit tolerance mode.
4. 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: SLES 9 must be at SP3 or higher.

5. The Linux OS Monitoring Agent requires the installation of the latest versions of the following libraries:

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

   These libraries are available on the Linux operating system installation media and Service Packs. Each library can have multiple packages, and each must be installed.
6. Summarization and Pruning agent.
7. This environment is only supported when operating system settings for SELinux Security and Firewall Security are set to disabled.
8. There is a limitation and workaround regarding the **korn** shell that is used in SLES 10 and RHEL 5. See “Limitation regarding the korn shell of newer Linux operating systems” on page 73.
9. SLES refers to SUSE Linux Enterprise Server. RHEL refers to Redhat Enterprise Linux.

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. For the latest database support information, see http://www-306.ibm.com/software/sysmgmt/products/support/Tivoli_Supported_Platforms.html; refer to the "Database Support" tab.

Table 5 shows the supported databases for the portal server. Notice 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″)[1, 2]	
	IBM DB2 UDB[3]	**MS SQL**
AIX[4]	V8.1 with Fix Pack 10 or higher fix packs V8.2 with Fix Pack 3 or higher fix packs V9.1 is supported when you apply the workaround that is described in APAR IY95415.	—
Linux[5]	V8.1, with Fix Pack 10 or higher fix packs V8.2 with Fix Pack 3 or higher fix packs V9.1 is supported when you apply the workaround that is described in APAR IY95415.	—
Windows	V8.1, with Fix Pack 10 or higher fix packs V8.2 with Fix Pack 3 or higher fix packs V9.1	MS SQL 2000 EE SP3

Notes:

1. ″TEPS″ is the default database name for the database used by the portal server.
2. Your portal server database must be located on the computer where the portal server is installed.
3. Support is for 32-bit and 64-bit databases.
4. If you run IBM DB2 on an AIX computer, see the following document for information on a memory shortage problem that you might encounter in IBM DB2: http://www-1.ibm.com/support /docview.wss?rs=203 &uid=swg21258694&loc=en_US&cs=UTF-8&lang=all
5. If the Tivoli Enterprise Portal Server runs on a 64-bit Linux zSeries computer, 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: SLES 9 must be at SP3 or higher.

Table 6 on page 9 shows the supported databases for the Tivoli Data Warehouse.

Table 6. Supported databases for the Tivoli Data Warehouse

Tivoli Data Warehouse database ("WAREHOUS")[1]		
IBM DB2	**MS SQL**	**Oracle**
Supported versions: • V8.1 with Fix Pack 10 or higher fix packs • V8.2 with Fix Pack 3 or higher fix packs • V9.1 and fix packs[3] Support applies to the following operating systems: • AIX V5.3 • Windows 2003 Server • Solaris 10 • RHEL 4 for Intel and zSeries[4] • RHEL 5 for Intel and zSeries[5] • SLES 9 for Intel and zSeries[4] • SLES 10 for Intel and zSeries[5] **Note:** If you run the database for the Tivoli Enterprise Portal *and* the database for the warehouse in the same instance of IBM DB2, you must follow the support requirements in Table 5 on page 8.	MS SQL 2000 EE SP3 MS SQL 2005	Supported versions: • V9.2, 10g Release 1 • V9.2, 10g Release 2 Support applies to the following operating systems: • AIX V5.3 • Windows 2003 Server • Solaris 10[2] • RHEL 4 for Intel and zSeries • RHEL 5 for Intel and zSeries • SLES 9 for Intel and zSeries • SLES 10 for Intel and zSeries

Notes:

1. "WAREHOUS" is the default database name for the database used by Tivoli Data Warehouse. Your Tivoli Data Warehouse database can be located on the same computer as your portal server or on a remote computer.
2. See the Oracle company support Web site (www.oracle.com) for information about installing and configuring Oracle on Solaris V10.
3. Support for data warehousing in IBM DB2 UDB V9.1 was added beginning with IBM Tivoli Monitoring V6.1.0 Fix Pack 4.

   Do not use DB2 V9 Fixpack 2 for the Tivoli Data Warehouse. Use of DB2 V9 FP2 can cause the Warehouse Proxy Agent and the Summarization and Pruning Agent not to function properly. Use an earlier version, such as DB2 V9 Fix Pack 1, or upgrade to a level which contains the fix for APAR JR26744, such as DB2 V9 Fix Pack 3.
4. SLES refers to SUSE Linux Enterprise Server. RHEL refers to Redhat Enterprise Linux.
5. "Limitation regarding the korn shell of newer Linux operating systems" on page 73 describes a required workaround for monitoring agents on SLES 10 and RHEL 5.

Chapter 2. Planning your fix pack installation

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

Table 7. Overall planning steps for Fix Pack 6

Goal	Where to find information
Determine which components must be upgraded.	"Determining which components need to be upgraded to Fix Pack 6"
Gather the information you need to perform the installation.	"Fix pack installation planning worksheets" on page 14
Learn how to preserve your customization.	"Preserving user customizations" on page 17
Understand how the autostart script works.	"Changes in the behavior of the autostart scripts" on page 19
Understand issues about the Windows versions of general availability (GA) CDs.	"Understanding the GA versions of the IBM Tivoli Monitoring version 6.1 agent CDs for Windows platforms" on page 20

Determining which components need to be upgraded to Fix Pack 6

This section helps you determine on which components to install Fix Pack 6. The section also explains the proper sequence of installation. The following specific topics are covered:

- "General guidelines for upgrading components"
- "Determining which components are present on a specific computer" on page 12
- "Sequencing the upgrade procedures" on page 12

General guidelines for upgrading components

The following guidelines can help you plan deployment of Fix Pack 6:

- **Fix Pack 6 and monitoring servers.** It is a best practice to apply Fix Pack 6 to all monitoring servers in your environment. However, you can perform the upgrade during a several-day period. The older versions of the server are compatible with Fix Pack 6.
- **Fix Pack 6 and base monitoring agents.** The following points apply to base monitoring agents:
  - You use Fix Pack 6 to upgrade base monitoring agents.

    In contrast, Fix Pack 6 has no effect on application monitoring agents. The more recent versions of the application monitoring agents are *compatible* with an IBM Tivoli Monitoring environment that you upgrade to Fix Pack 6. ("Base versus application monitoring agents" on page 14 explains the distinction between base monitoring agents and application monitoring agents.)
  - Base monitoring agents from the original release of IBM Tivoli Monitoring V6.1 are supported by Fix Pack 6. See the last Note in this list.
  - Base monitoring agents that are upgraded to fix packs prior to Fix Pack 6 are supported by Fix Pack 6. See the last Note in this list.
  - To learn whether Fix Pack 6 adds a required fix or feature to your base monitoring agents, review the Chapter 6, "APARs addressed by Fix Pack 6," on page 107. In particular, the following sections might list fixed APARs that affect specific set of agents in your monitoring environment. These fixes might validate a decision to make the effort to upgrade that set of agents.
    - "Tivoli Universal Agent APARs" on page 113
    - "UNIX OS monitoring agent APARs" on page 114
    - "Windows OS monitoring agent APARs" on page 115
    - "i5/OS monitoring agent APARs" on page 114

© Copyright IBM Corp. 2007

- "Linux OS monitoring agent APARs" on page 114

– The best practice is to upgrade all base monitoring agents to Fix Pack 6.

- **Fix Pack 6 and the Tivoli Universal Agent.** For local installations, if you have the Tivoli Universal Agent installed on a UNIX or Linux computer, you must upgrade the Tivoli Universal Agent at the same time that you upgrade any other component to Fix Pack 6.
- **Fix Pack 6 and application monitoring agents.** Fix Pack 6 does not have to be applied to application monitoring agents. In fact, you cannot apply Fix Pack 6 to application monitoring agents because that category of agent is separate from the base installation of IBM Tivoli Monitoring and is updated by separate fix packs. "Base versus application monitoring agents" on page 14 explains the basic differences among agents.
- **Fix Pack 6 and the Warehouse Proxy Agent and the Summarization and Pruning Agent.** See "Historical data collection issues" on page 97.

Determining which components are present on a specific computer

In the "Fix pack installation planning worksheets" on page 14 you compile a comprehensive list of the monitoring components in your environment. The data in this list might be sufficient to complete an upgrade, depending on the operating system of the computer that hosts the components:

- **Windows:** The details in the list are sufficient for components on the Windows operating system, because the fix pack installer for Windows identifies the components that require upgrading and automatically upgrades them. By completing the worksheets you have information ready when the installer prompts you to provide specific values.
- **Linux and UNIX:** The details in the list are *not* sufficient for components on the Linux and UNIX operating systems, but they provide an good starting point. In addition, you must review the installed components to identify which components need to be upgraded, as follows:
  1. Enter the following command to list the installed components and their version number.

     ```
     cinfo -i
     ```

     For example, components might have the version number, which refers to the original released version of IBM Tivoli Monitoring. You need to upgrade these components to Fix Pack 6.
  2. Refer to the list while you are installing Fix Pack 6, to ensure that all components are upgraded.

Sequencing the upgrade procedures

You must upgrade your IBM Tivoli Monitoring components and OMEGAMON XE monitoring agents on z/OS in the general order that is described in this section. This installation sequence also minimizes the possibility for problems when you must perform an upgrade in an active monitoring environment (also known as a *rolling upgrade*):

Key concept: hierarchy of upgrades

The following guidelines govern the deployment of fix packs:

- Any fix pack version that you apply to a hub Tivoli Enterprise Monitoring Server must be the highest version that is present in the IBM Tivoli Monitoring environment.
- Any fix pack version that you apply to a remote Tivoli Enterprise Monitoring Server must be higher than or equal to the version that is present on the agents that report to that remote monitoring server.
- The fix pack version that is present on any agent must not be higher than the fix pack version that is running on the following components:
  – Hub and remote monitoring servers
  – Tivoli Enterprise Portal Server to which the agent reports

Overview of sequencing

In past fix packs, the best practice (upgrade the hub Tivoli Enterprise Monitoring Server first; then remote Tivoli Enterprise Monitoring Server; and then Tivoli Enterprise Portal Server) is replaced by the following guideline:

First: Hub Tivoli Enterprise Monitoring Server

Second: Tivoli Enterprise Portal Server

Third: Remote Tivoli Enterprise Monitoring Server

Note: The First and Second sequential items are installed or upgraded automatically in a single-server installation, which is described in "Single-server quick installation checklist" on page 31.

This revised protocol reflects the fact that the remote Tivoli Enterprise Monitoring Server can be upgraded at a later time. See Details regarding sequencing.

In contrast, a hub Tivoli Enterprise Monitoring Server and Tivoli Enterprise Portal Server are to be upgraded within one upgrade session. This requirement applies to components that you install on distributed systems. The requirement does not apply to a hub Tivoli Enterprise Monitoring Server that runs on z/OS, because you cannot run an upgrade operation simultaneously on z/OS and on one of the types of system that is supported for the portal server (The portal server only runs on distributed systems.)

Details regarding sequencing

The following details represent best practices and can help ensure success of upgrades in a variety of monitoring environments:

Note: This section provides best practices, not mandatory procedures. Alternate scenarios are valid. For example, you have the option to initially upgrade a remote monitoring server that runs on a z/OS system, before you upgrade the hub monitoring server.

1. Perform the core upgrade procedures.
   a. (*For TEC Event Synchronization users only*) If you use IBM Tivoli Enterprise Console Event Synchronization, upgrade this component first.
   b. Upgrade the hub monitoring server.

      Note: Documentation of upgrade procedures sometimes references the default path for the installation of IBM Tivoli Monitoring. If you did not install the product in the default path, you must specify the correct path whenever the upgrade procedures require a path specification.

   c. If your environment does not contain OMEGAMON XE on z/OS monitoring agents, go to Step 1e.
   d. If your environment contains OMEGAMON XE on z/OS monitoring agents, complete the following tasks:
      1) Upgrade all remote monitoring servers defined as sysplex proxies or eligible to serve as sysplex proxies. (A sysplex proxy monitoring server is a data consolidation point for sysplex monitoring.)
      2) Upgrade to V4.1.0 or higher any OMEGAMON XE on z/OS monitoring agents configured in the hub and in each of the remote monitoring servers you just upgraded (that is, proxy and proxy-eligible monitoring servers).
      3) Re-register the OMEGAMON XE on z/OS monitoring agent with each of these monitoring servers, to ensure that sysplex data collection rules (UADVISORs) use the format that corresponds to IBM Tivoli Monitoring V6.x.
   e. Upgrade the Tivoli Enterprise Portal Server and any Tivoli Enterprise Portal desktop clients.
2. Upgrade the remaining remote monitoring servers and monitoring agents all at once, or one at a time in a staged rollout. Adhere to the following guidelines:

- Upgrade a remote Tivoli Enterprise Monitoring Server before upgrading the agents connected to it.
- If you decide upon a staged upgrade, be sure to check the Preventive Services Planning (PSP) bucket and apply current maintenance to any monitoring agents remaining at the V3.1.0 level after the monitoring server to which they connect is upgraded to the V6.1 Fix Pack 6 level.
- See also, “Key concepts: the hierarchy of upgrades” on page 12.

Base versus application monitoring agents

This section describes the types of monitoring agents that are available for use with IBM Tivoli Monitoring: base monitoring agents and application monitoring agents.

Base monitoring agents

Base monitoring agents are part of the base installation package for IBM Tivoli Monitoring. If you are installing any of the following agents, launch the installation using the **setup.exe** or **install.sh** files that are part of the base IBM Tivoli Monitoring installation package:

- OS Agents (agents that monitor specific types of operating systems)
  - i5/OS Agent
  - Linux OS Agent
  - UNIX OS Agent
  - Windows OS Agent
- ITM 5.x Endpoint
- UNIX Log Agent
- Tivoli Universal Agent
- Warehouse Proxy Agent
- Warehouse Summarization and Pruning Agent

Application monitoring agents

Application monitoring agents are not part of the base package for IBM Tivoli Monitoring. If you are installing agents that are not included in the base package (for example, DB2 or Microsoft Exchange agents), launch the agent installation using the **setup.exe** or **install.sh** files that are part of the various installation packages for these monitoring agents.

See the appropriate agent documentation for more information. Typically, this information is located in a configuration chapter in the user’s guide for the agent.

Note: Application monitoring agents are updated by Fix Packs that are released separately from the Fix Pack for the base components of IBM Tivoli Monitoring (which includes base monitoring agents). The upgrade of application monitoring agents is independent from the Fix Pack 6 upgrade described in this document.

Fix pack installation planning worksheets

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

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

Table 8. Fix pack planning worksheet

IBM Tivoli Monitoring installation directory (CANDLEHOME environment variable): **Note:** This directory is referred to as *itm_home* 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.				
Host name: _____ **Host operating system (OS): _____**	**Other components also installed on this computer (circle those that apply)**	**Where to obtain this information**	**When this information is used**	**Notes**
Host name of hub monitoring server: _____ OS: _____	Portal server Portal desktop client Warehouse Proxy S&P Agent*	Manage Tivoli Enterprise Monitoring Server	"Monitoring server checklist" on page 34	
Host name of remote monitoring server: _____ OS: _____	Portal server Portal desktop client Warehouse Proxy S&P Agent*	Manage Tivoli Enterprise Monitoring Server	"Monitoring server checklist" on page 34	
Host name of remote monitoring server: _____ OS: _____	Portal server Portal desktop client Warehouse Proxy S&P Agent*	Manage Tivoli Enterprise Monitoring Server	"Monitoring server checklist" on page 34	
Host name of remote monitoring server: _____ OS: _____	Portal server Portal desktop client Warehouse Proxy S&P Agent*	Manage Tivoli Enterprise Monitoring Server	"Monitoring server checklist" on page 34	
Host name of remote monitoring server: _____ OS: _____	Portal server Portal desktop client Warehouse Proxy S&P Agent*	Manage Tivoli Enterprise Monitoring Server	"Monitoring server checklist" on page 34	
Host name of remote monitoring server: _____ OS: _____	Portal server Portal desktop client Warehouse Proxy S&P Agent*	Manage Tivoli Enterprise Monitoring Server	"Monitoring server checklist" on page 34	
Host name of portal server host name: _____ OS: _____	Monitoring server Portal desktop client Warehouse Proxy S&P Agent*	Manage Tivoli Enterprise Monitoring Server	"Portal server checklist" on page 37	

Table 8. Fix pack planning worksheet (continued)

IBM Tivoli Monitoring installation directory (CANDLEHOME environment variable): **Note:** This directory is referred to as *itm_home* 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.				
Host name: _____ **Host operating system (OS): _____**	**Other components also installed on this computer (circle those that apply)**	**Where to obtain this information**	**When this information is used**	**Notes**
Portal desktop client locations: _____	Monitoring server Portal server Warehouse Proxy S&P Agent*	Manage Tivoli Enterprise Monitoring Server	"Portal desktop client checklist" on page 40	
Warehouse Proxy agent location: _____	Monitoring server Portal server Portal desktop client S&P Agent*	Manage Tivoli Enterprise Monitoring Server	"Monitoring agent checklist - local installation" on page 41	
Warehouse S&P Agent* location: _____	Monitoring server Portal server Portal desktop client Warehouse Proxy	Manage Tivoli Enterprise Monitoring Server	"Monitoring agent checklist - local installation" on page 41	
Agent types to update (product codes): _____		**tacmd listSystems**	"Monitoring server checklist" on page 34 "Monitoring agent checklist - local installation" on page 41	
* Summarization and Pruning Agent				

Preserving user customizations

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

These general rules apply to how user customizations are preserved:

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

The configuration process works with two basic types of files:

- **`*.ini`** (initialization) files are used to collect the inputs from the installation process. This input information is the set of responses to installation questions that are captured as keyword-value pairs. This information is laid down with default values and basic information about the installed components.
- **`*.config`** (configuration) files are generated by the values in the .ini files and the values entered during configuration.

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

To recover a lost, manual customization after installing a new fix pack, do the following:

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

Files that are preserved on upgrade

This section lists and describes the files that are preserved when you upgrade the IBM Tivoli Monitoring environment. If you have modified these files or settings, you can expect the changes to be preserved on upgrade:

- **-D flags in Applet.html**: Any changes made to the -D flags in file is preserved.
- **Bannerimage.html** in the **CNB** directory. If you add a customer image for your own banner, this is preserved.
- **-D flags in "cnp" batch or script files:** Any changes made to the -D flags on the Java™ calls of these files are preserved. The specific file names are as follows:
  - **On UNIX or Linux systems:** `cnp.sh` and `cnp_`*`inst`*`.sh`
  - **On Windows systems:** `cnp.bat` and `cnp_`*`inst`*`.bat`

  where *inst* can be the name of an instance of the Tivoli Enterprise Portal to connect to. See “The -D flags in a cnp.sh file are not preserved on upgrade” on page 72 for an exception; the **-D** flags in **cnp.sh** are not preserved.
- **ENV** files: The current settings from ENV files are preserved by checking “key = value” and adding keys that did not exist in the new file from the old file and replacing the value from the old file in the new file. Keys with default values are preserved. The exception is the **lnxenv** file for which there is a limitation; see “A Linux configuration file (lnxenv) is not preserved on upgrade” on page 72.

- **INI** files: The ini files are preserved as generally described above. If a change was made using a provided configuration tool, the values is always preserved. If you were instructed by a technote or by an IBM support engineer to make a manual change, the value is most likely, but not always, preserved (depending on what you changed and why).
- **OM_TEC.config** in one of the following directories:
  - **On Windows systems:** *itm_home*\cms\TECLIB
  - **On UNIX or Linux systems:** *itm_home*/tables/*temsname*/TECLIB
- **tecserver.txt** in one of the following directories:
  - **On Windows systems:** *itm_home*\cms\TECLIB
  - **On UNIX or Linux systems:** *itm_home*/tables/*temsname*/TECLIB

Files that are not preserved on upgrade

You must not modify these files because they will be replaced or regenerated during the upgrade process:

For components running on all types of distributed (non-mainframe) computers:

The following IBM Tivoli Enterprise Console event synchronization files:

- In the TEC_CLASSES directory of the rulebase created during IBM Tivoli Enterprise Console event synchronization install: omegamon.baroc, Sentry.baroc.
- In the TEC_RULES directory of the rulebase created during IBM Tivoli Enterprise Console event synchronization install: omegamon.rls.

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

Note: These **.baroc** and **.rls** files are backed up only if you choose to automatically upgrade the specified rulebase.

For components running on Windows computers:

- On the Tivoli Enterprise Portal Server, the **CNP.bat** and **applet.html** files are built based on the content of the CNPS, CNP, and CNB directories. Except for the -D flags, everything in this file is regenerated.
- The **buildpresentation.bat** file is generated by during installation. Any updates to this file are lost.

For components running on UNIX or Linux computers:

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

Special exceptions

On UNIX, several IBM Tivoli Monitoring configuration files exist whose values do not typically persist during an upgrade. However, the values in these files do persist:

- *itm_home*/tables/*TEMS_name*/*.txt, where ***.txt** refers to all file names that have the text (**.txt**) tag, including **partition.txt** and **glb_site.txt**.
- The following files are generated from **kbbenv.ini** and **ms.ini** respectively:
  - *itm_home*/tables/*TEMS_name*/KBBENV
  - *itm_home*/config/.ConfigData/*hostname*_ms_*TEMS_name*.config.

  Changes made to these files are saved in the same way that changes made to the source **.ini** files are saved.

Changes in the behavior of the autostart scripts

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

- In Fix Pack 3, the installation process produced an autostart script with only one entry using a generic `CandleAgent start all` command and users modified this file as required.
- In Fix Pack 4, the installation process generated individual entries for each application in a particular installation, but the values captured in the file could not be overridden.
- In Fix Pack 5, the multiple entries remained and an override capability was added.

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

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

where:

USER The ID that is used to start the application. By default, *USER* is the owner of the bin directory for the application. For the UNIX Log Alert agent, *USER* is the owner of the *itm_home*/*PLAT*/ul/bin directory.

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

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

product_code Is the two-character code for this application. Refer to “Sample output for the kincinfo command on Windows” on page 47 for a list of the component codes.

instance Is the instance name required to start this application.

PLAT Is the platform directory where the application is installed.

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

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

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

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

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

1. Remove the comment indicator (the exclamation point, !) so that the product code item looks like <product_code>.
2. Copy a product code section.

3. Customize the product code section and activate it, rather than create new sections from scratch.

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

Notes:

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

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

The General Availability (GA) versions of the IBM Tivoli Monitoring version 6.1 agent CDs for the Windows operating system must *NOT* be installed into an IBM Tivoli Monitoring version 6.1 Fix Pack 6 environment or be used to populate a Tivoli Enterprise Monitoring Server depot. The IBM Tivoli Monitoring version 6.1 agent CDs have been refreshed for use with Fix Pack 6.

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

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

- The agent framework component is replaced by an older version.
- The OS agent fails.
- You cannot administer the system remotely.

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

If you have already installed a GA-level agent after Fix Pack 6 installation, there is a way to recover. Obtain the refreshed IBM Tivoli Monitoring version 6.1 GA agent and run the installer from the refreshed agent CD, which allows the Tivoli Enterprise Monitoring Agent component to be restored to the correct level. The agent version is NOT updated. The agents remain at the GA level.

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

See Appendix A in the *IBM Tivoli Monitoring Administrator's Guide* for more information about using the **tacmd removeBundles** and **tacmd addBundles** commands to remove agents from and add agents to the agent depot. For example, the following command adds the updated agent software to your deployment depots:

```
itm_home/bin/tacmd addBundles -i patch_file
```

where *itm_home* is the directory where you installed IBM Tivoli Monitoring and *patch_file* is the location of the fix pack.

Identifying a refreshed version of IBM Tivoli Monitoring agent CD images

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

```
[COMPONENT INFO]
Product Code=GL
Desc=Tivoli Enterprise Monitoring Agent Framework
ComponentID=KGLWICMA
PlatformCode=WI
DPlatformCode=Windows
VRMF=06100301
```

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

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

where *pc* is one of the products codes in the KINCINFO command output, found at “Sample output for the kincinfo command on Windows” on page 47.

Summary of this section

Every general availability (GA) version of the IBM Tivoli Monitoring version 6.1 agent for Windows operating system CD and installation image must be replaced with the refreshed version. Every GA version of the IBM Tivoli Monitoring version 6.1 agent bundle for the Windows operating system installed in a depot must be replaced with the refreshed version before it can be deployed into an IBM Tivoli Monitoring version 6.1 Fix Pack 6 environment. You will encounter this scenario only when you install a GA-level application agent *AFTER* you have deployed the Fix Pack 1, Fix Pack 2, or Fix Pack 4 OS agent.

Notes:

1. After you update the GA version of the IBM Tivoli Monitoring version 6.1 agent bundle with the refreshed version, that agent bundle *cannot* be used to remotely uninstall the GA version of the agent from an endpoint system.
2. If you install the Fix Pack 6 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 6 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 1 was released.
3. If you install the Fix Pack 6 Windows OS agent after installing the GA version of the application agent, the agent framework is updated to the refreshed version. However, if you modify the GA version of the application agent installation by adding another agent from the same image, the **KGLWICMA.ver** file will no longer be accurate and it will appear as if the agent framework is at the unrefreshed GA version.
4. Do not use the **tacmd updateAgent** command to update a GA version of an IBM Tivoli Monitoring version 6.1 agent on Windows computers that hosts a refreshed version. If you do, you can cause the installation of the refreshed agent to create a duplicate entry in the Add/Remove Programs list on the computer that you are updating. If this occurs, delete the duplicate entry by running a local uninstallation of the agent after you remove the refreshed version of the IBM Tivoli Monitoring version 6.1 agent.

   To avoid this problem, you can use the **tacmd updateAgent** command to update a GA version of the agent with the agent *fix pack* image (and not the full image). **Note: Since Fix Pack 4, this note applies to non-OS agents only.**

Chapter 3. Fix pack installation instructions

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

On Windows, you can use an installation wizard to install the fix pack. Keep in mind the following distinctions:

- **First-time installations and upgrades:** If you are performing a fresh installation (or upgrading), selecting a check box installs or upgrades the product or support option that you select.
- **Updates and Modifications:** If you are updating an existing installation (you selected **Modify** in the Welcome window), all check boxes on the Select Features window reflect your choices during the initial installation. Clearing a check box has the effect of uninstalling the component. Clear a check box only if you want to remove a component.

Note: Table 9 lists available fix pack installation checklists. However, the sequence of the checklists in the table does not apply to all monitoring environments. For information on best practices for sequencing installation, see "Sequencing the upgrade procedures" on page 12.

Table 9. Overall installation steps for Fix Pack 6

Goal	Where to find information
Ensure that you are installing product components on a supported operating system.	"Supported operating systems" on page 3
Note: The panels of the installation wizard display options to install *all* components. The options include components that *might not be supported* on the operating system that you are using. If you make an incorrect choice and click **Next**, the wizard alerts you with an error message. To avoid seeing this error message, always consult the list of supported operating systems.	
Ensure your monitoring environment is prepared for fix pack installation.	"Preparing for installation" on page 26
Complete installation of IBM Tivoli Monitoring components on computers that do not currently host IBM Tivoli Monitoring components.	"New (non-upgrade) installation checklist" on page 29
If your Tivoli Enterprise Monitoring Server, Tivoli Enterprise Portal Server, and Tivoli Enterprise Portal desktop client are running on the same system, update that single server.	"Single-server quick installation checklist" on page 31
Update your hub Tivoli Enterprise Monitoring Server	"Monitoring server checklist" on page 34
Update your Tivoli Enterprise Portal Server	"Portal server checklist" on page 37
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 54
Update your remote Tivoli Enterprise Monitoring Servers	"Monitoring server checklist" on page 34
Update your Tivoli Enterprise Monitoring desktop clients	"Portal desktop client checklist" on page 40
Update your local Tivoli Enterprise Monitoring Agents	"Monitoring agent checklist - local installation" on page 41
Remotely update other Tivoli Enterprise Monitoring Agents	"Monitoring agent checklist - remote deployment" on page 43
Update your local i5/OS OS agents, if applicable.	"Installing the fix pack for the i5/OS monitoring agent" on page 51

Notes:

1. Because of increases in the size of product components, support for Linux Intel platforms is split into two files. See Table 1 on page 2 for the fix pack file that you must use for upgrading the IBM Tivoli Monitoring components.

© Copyright IBM Corp. 2007

2. If your Warehouse Proxy agent or Summarization and Pruning agent are on computers other than the monitoring server or portal server, use the instructions in the “Monitoring agent checklist - local installation” on page 41 to install the updates.
3. As you upgrade the various components of the system, the installer shows you defaults based on your previous settings, the choices you made the last time you configured the component. If nothing has changed, you can press Enter to advance through the installation. However, if this is the first time a component has been configured, the installer presents common default settings.
4. If you use Fix Pack 6 to upgrade a remote Tivoli Enterprise Monitoring Server before you upgrade the hub monitoring server and the remote monitoring server is a computer with multiple IP interfaces, it might be necessary to set the KDEB_INTERFACE to the IP address of the primary remote monitoring server interface. The main symptom of this problem is empty Tivoli Enterprise Portal workspaces for agents that are attached to this remote monitoring server. To correct this problem, add the statement KDEB_INTERFACELIST=<*IP_Address_of_Primary_Interface*> to the KBBENV file for the remote monitoring server. For general information on sequencing upgrades see “Sequencing the upgrade procedures” on page 12.
5. Fix Pack 5 made changes to the WAREHOUSELOG table, adding a column named WPSYSTEM. This column represents the system name of the computer where the Warehouse Proxy Agent is installed. If the user ID used by the Warehouse Proxy Agent to connect to the warehouse database is not authorized to alter a table in the database, you might have to run the following command as database administrator from a SQL command prompt. The command is the same for DB2, ORACLE, or Microsoft SQL databases:

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

   When fix pack installation is complete, this command must be run one time, before you restart the IBM Tivoli Monitoring components.
6. These checklists provide the order and procedures for installing the fix pack. Perform the tasks in the order shown.

The basic flow of this installation process is shown in Figure 1 on page 1.

Locations of installation logs

If the installation of some component of the fix pack fails, that failure is typically documented in the installation logs. To find the installation logs for IBM Tivoli Monitoring components, look for the installation log files described in Table 10.

Table 10. Installation and startup log file names and locations

Activity	Windows	UNIX or Linux systems
During installation	*itm_home*\InstallITM\Abort IBM Tivoli Monitoring *date_time*.log	$*itm_home*/logs/candle_installation.log

Table 10. Installation and startup log file names and locations (continued)

Activity	Windows	UNIX or Linux systems
While starting a component	• For the Tivoli Enterprise Portal: *itm_home*\CNP\logs\kcjerror.log *itm_home*\CNP\logs\kcjras1.log • For errors with distributed Tivoli Enterprise Monitoring Agents: *itm_home*\TMAITM6\logs*hostname_pc_key*.log • For errors on the Tivoli Enterprise Portal Server, Tivoli Enterprise Monitoring Server, or warehouse proxy agent: *itm_home*\logs*hostname_pc_key*.log where *hostname* is the hostname of the computer where the component is running, *pc* is the two-letter product code, and *key* is a hexadecimal identifier. Refer to the product code appendix in the *IBM Tivoli Monitoring: Installation and Setup Guide* for a list of product codes or to the output for the kincinfo info command found in “Sample output for the kincinfo command on Windows” on page 47.	$*itm_home*/logs/ *hostname_pc_key*.log

Preparing for installation

This section lists activities to perform prior to installation of the fix pack.

Overall preparations for Daylight Savings Time (DST) issues

Technote 1283245 at http://www-1.ibm.com/support/docview.wss?uid=swg21283245 describes the existing behavior of IBM Tivoli Monitoring, version 6.1 related to the DST (Daylight Saving Time) fall back on November 4, 2007 at 2:00AM. The document describes the potential side effects and the recommended corrective actions.

Adapting to Daylight Savings Time in the United States

US Customers Only: If you have not done so already, adapt your system and the product set to **daylight savings time** changes. The switch to **daylight savings time** occurred 3 weeks earlier (March 11, 2007) this year in the United States than it did last year and also ends 1 week later on November 4, 2007. For more information, see **URGENT Actions Required: Changes to Daylight Saving Time will affect IBM Tivoli Monitoring 6.1 and IBM Tivoli OMEGAMON 350/360 and their associated Operating Systems** at the following URL: http://www-1.ibm.com/support/docview.wss?uid=swg21254621.

In IBM Tivoli Monitoring version 6.1 Fix Pack 6, the Java Runtime Environments (JREs) for some operating systems have been patched using the JTZU utility. If you have installed J2RE 1.4.2 IBM Windows 32 build cn142-20070317 (SR8) or higher this patch has been applied.

- **Upgrading from any Fix Pack:** All customers upgrading to IBM Tivoli Monitoring version 6.1 Fix Pack 6 from an earlier IBM Tivoli Monitoring Fix Pack must run the JTZU utility to update the IBM Tivoli Monitoring version 6.1 JREs. Refer to the sections “Patching Java” and “Java Update First Steps” in the flash for more information. If you have already run the JTZU utility against your JRE, it is not necessary to run it again after applying this fix pack. However, if you choose to run JTZU again, it will report that the JRE has already been updated.
- **New Linux and UNIX users:** New Linux and UNIX users can begin using IBM Tivoli Monitoring version 6.1 with a JRE that is already corrected for Daylight Saving Time. You do not need to run the JTZU utility to update the IBM Tivoli Monitoring version 6.1 JREs. If you need to use the the JTZU utility, see Technote 1254621 at the following URL: http://www-1.ibm.com/support/docview.wss?uid=swg21254621.
- **Upgrading from Fix Pack 5:** The IBM Tivoli Monitoring installer checks for prerequisite software. During an upgrade from Fix Pack 5 to Fix Pack 6, the installation prerequisite window might show a required version of Java that is later then the current version displayed, you must upgrade to the "Required Version" to support DST. For example, you might see the following:

  ```
  Current version: J2RE 1.4.2 IBM Windows 32 build cn142ifx-20060209 (SR4-1)
  Required version:  J2RE 1.4.2 IBM Windows 32 build cn142-20070317 (SR8) or higher
  ```

  In this case, you must select the **Upgrade IBM JAVA** option to allow the installer to upgrade the Java software.
- **Upgrading browser clients:** The browser client for IBM Tivoli Monitoring requires a version of IBM Java at Service Release 8 (SR8) or higher. To use a browser client from a computer that has no IBM Tivoli Monitoring components installed and which has an older version of IBM Java (any version earlier than IBM Java SR8), you must uninstall the existing Java on that computer before you launch the browser. If you do not uninstall the older version, the portal server does not install the new version which has the Java DST patch.

Backing up IBM Tivoli Monitoring

Before installing a fix pack, make a backup copy of your current IBM Tivoli Monitoring installation in case you decide to revert to it. The following procedures describe valid methods for creating a backup.

Note: Typically an enterprise has a standard process for preserving a backup image of all computer systems, including the IBM Tivoli Monitoring environment. In most cases, the standard process for

your enterprise is preferable to the processes described in this section. Use the instructions in this section only in unusual circumstances, when a standard backup process is not available.

You must perform the following instructions when no other activity is running on the system. The user accounts that you use to perform these activities must have **root** or **Administrator** privileges.

Backing up a UNIX or Linux installation

Follow these steps to back up a UNIX or Linux installation.

Note: Typically an enterprise has a standard process for preserving a backup image of all computer systems, including the IBM Tivoli Monitoring environment. In most cases, the standard process for your enterprise is preferable to the processes described in this section. Use the instructions in this section only in unusual circumstances, when a standard backup process is not available.

1. Close the Tivoli Enterprise Portal browser and desktop clients.
2. Stop the Tivoli Enterprise Portal Server, the Tivoli Enterprise Monitoring Server, the Eclipse Help Server, and all the monitoring agents running on the system.
3. If the Tivoli Enterprise Portal Server is installed, run the following command:

   ```
   ./itmcmd execute cq "runscript.sh migrate-export.sh"
   ```

4. Use the tar command to compress the contents of *itm_home* (the directory where IBM Tivoli Monitoring is installed), using a command that is similar to the following:

   ```
   tar -cvf /tmp/itm_home.backup.tar itm_home
   ```

5. Add the following files to the tar file created in step 4 above:
   - On AIX:

     ```
     /etc/rc.itm*
     tar -uvf /tmp/itm_home.backup.tar /etc/rc.itm*
     ```

   - On HP-UX:

     ```
     /sbin/init.d/ITMAgents*
     tar -uvf /tmp/itm_home.backup.tar /etc/init.d/ITMAgents*
     ```

   - On other UNIX or Linux systems:

     ```
     /etc/initd/ITMAgents*
     tar -uvf /tmp/itm_home.backup.tar /etc/init.d/ITMAgents*
     ```

6. Use the appropriate database commands to back up the Tivoli Enterprise Portal Server and Tivoli Data Warehouse databases.

You are now ready to proceed with installation of the Linux or UNIX fix pack.

Always contact IBM Software Support before attempting to use the files generated in this procedure to restore the IBM Tivoli Monitoring environment. The support staff can help ensure success of the restoration. Otherwise, errors made during the modification of the Windows registry could lead to a corrupted operating system.

Backing up a Windows installation

Follow these steps to back up a Windows installation. In Step 4 on page 28 of this procedure, you record the current configuration settings. In Step 9 on page 28, you apply these settings again.

Note: Typically an enterprise has a standard process for preserving a backup image of all computer systems, including the IBM Tivoli Monitoring environment. In most cases, the standard process for your enterprise is preferable to the processes described in this section. Use the instructions in this section only in unusual circumstances, when a standard backup process is not available.

1. Close any browser or desktop clients for the Tivoli Enterprise Portal.
2. Launch the **Manage Tivoli Monitoring Services** (`KinConfg.exe`) utility.

3. *On the computer where you are applying the fix pack*, stop the Tivoli Enterprise Portal Server, the Tivoli Enterprise Monitoring Server, the Eclipse Help Server, and all the monitoring agents running on the system.

   Note: You perform this step on the local computer where you are applying the fix pack. Remote computers are not involved in this procedure.
4. Perform the following steps to record the current configuration settings for IBM Tivoli Monitoring. (For example, you can make a record on a sheet of paper or in a buffer file.)
   a. Right-click in the row of the component that you want to configure.
   b. Select **Reconfigure**.

      Note: You make no changes in the series of windows that are displayed.
   c. Record the settings for the component in the series of configuration windows.

      You record details such as port numbers, host names, protocols for communication, firewall settings, and settings for the data warehouse.
   d. Click **OK** in each window and accept all prompts, *without making changes*.

      Note: If you click **Cancel** at any point, the **Reconfigure** process fails to display all configuration windows. You must start the **Reconfigure** process again.

   You must *unconfigure* the monitoring environment in the next step. This action restores the Windows registry to a known state that ensures success, if you restore the environment later.
5. Perform the following steps to unconfigure each IBM Tivoli Monitoring component, except the Tivoli Enterprise Portal desktop client. Do not perform the following steps for the desktop client.
   a. Right-click in the row of a component in the **Manage Tivoli Monitoring Services** window.
   b. Select **Advanced >> Unconfigure** in the pop-up menu.

      When you are finished, all components except the Tivoli Enterprise Portal desktop show **No** in **Configured** column of the **Manage Tivoli Monitoring Services** window.
6. Use a compression command to compress the contents of the directory where IBM Tivoli Monitoring is installed.
7. Use the appropriate database commands to back up the Tivoli Enterprise Portal Server and Tivoli Data Warehouse databases.
8. Export the entire Windows registry to a backup file as follows:
   a. Select **Run** in the Windows **Start** menu.
   b. Type **regedit** in the **Open** field.
   c. Click **OK**. The Registry Editor is displayed.
   d. Ensure that the **MyComputer** node at the top of the registry is selected, so that all values in the registry are exported.
   e. Select **Export** in the **File** menu.
   f. Save the copy of the registry to the following path and filename: `C:\WinRegistryBeforeInstall.reg`

   At this time, the backup process is complete.
9. Perform the following steps to return IBM Tivoli Monitoring to its normal configuration and status:
   a. Right-click in the row of each unconfigured component.

      "Unconfigured" components show **No** in the **Configured** column of the **Manage Tivoli Monitoring Services** window.
   b. Select **Advanced >> Configure Advanced** in the pop-up menu.
   c. In the series of dialog boxes that is displayed, enter the original parameter settings that you recorded in Step 4.
   d. Click **OK** in each configuration window and accept other prompts to save your changes.

When you are finished, all components show **Yes** in **Configured** column and **Stopped** in the **Status** column.

You are ready to proceed with the installation of the Windows fix pack.

Restoring a backup

Always contact IBM Software Support before attempting to use the files generated in this procedure to restore the IBM Tivoli Monitoring environment. The support staff can help ensure success of the restoration. Otherwise, errors made during the modification of the Windows registry might cause the operating system to become corrupted.

New (non-upgrade) installation checklist

This section describes the process for installing any IBM Tivoli Monitoring component on a computer that does not currently host IBM Tivoli Monitoring components. This type of installation follows the standard procedures that are provided in the *IBM Tivoli Monitoring Installation and Setup Guide*.

Table 11. Checklist for a new (non-upgrade) installation

✓	**Installation step**
	1. Gather information about the monitoring components in your environment. See “Fix pack installation planning worksheets” on page 14. The following sections can help you complete the worksheets and ensure the validity of your installation plans: • “Supported operating systems” on page 3 • “Supported databases for Tivoli Enterprise Portal Server and Tivoli Data Warehouse” on page 8
	2. Based on the platform of your local host computer, download and extract the required fix pack files to a temporary location on your computer. You can use the following space to write down the location of your patch directory. **Patch directory:** _____
	3. Follow the instructions in the *IBM Tivoli Monitoring Installation and Setup Guide* for the type of component that you want to install. The April, 2007 version of *IBM Tivoli Monitoring Installation and Setup Guide* provides more information on this topic in the following sections: • **Windows:** Chapter 5. "Installing IBM Tivoli Monitoring on One Computer." Section Installation Procedure, starts on page 58 • **UNIX:** Chapter 6. "Installing IBM Tivoli Monitoring." Refer to table 25 on page 65 and the procedures referenced therein.
	4. If the installation of this component failed refer to the installation logs found in Table 10 on page 24 for a description of installation problems.
	5. If you run the Tivoli Enterprise Portal client in a non-English locale, you must apply the fix pack for the language pack after you install Fix Pack 6. Otherwise, certain user interface strings are displayed in English instead of the default language. (This requirement also applies if you reconfigure any of the base components, such as the portal server.) The name of the installation image is **6.1.0-TIV-ITM-LP-FP0006**. This update to the language pack includes a fix regarding an expired certificate, which was identified in APAR IZ03654. For information about installing the language packs, see the “Installing the language packs” section of the *IBM Tivoli Monitoring Installation and Setup Guide*.

Issue: After a new (non-upgrade) installation of IBM Tivoli Monitoring (Tivoli Enterprise Portal Server, Tivoli Enterprise Monitoring Server, and monitoring agents), starting a Tivoli Enterprise Portal client and navigating to the Windows System Summary workspace can result in several of the views displaying the following error message:

```
KFWITM217E Request Error: Request failed due to offline managed system(s).
```

This message might also be displayed after you install a new agent and in other application workspaces that provide some kind of system summary workspace. Other product-provided workspaces return data without error. Only queries that are assigned to an application's default managed system list (for example, ***NT_SYSTEM**) are affected. This problem typically affects a single-server installation only, where Tivoli Enterprise Portal Server, Tivoli Enterprise Monitoring Server, and monitoring agents reside on the same machine. The problem is more likely to arise if you start the agent (local or remote) after the Tivoli Enterprise Portal Server is started.

Workaround: To resolve the error, recycle the Tivoli Enterprise Portal Server. After the recycle is complete, the system summary workspace returns the correct data.

Single-server quick installation checklist

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

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

Note: Only hub monitoring servers support SOAP servers.

Note: You can directly upgrade from any previous IBM Tivoli Monitoring V6.1.0 Fix Pack to Fix Pack 6. After the upgrade you must use the component software from Fix Pack 6 for all subsequent updates that you make to your monitoring environment. In particular, you must not use the installation media from Fix Packs 1, 2, or 3. Otherwise, you might damage your environment. For detailed information, see "(*If you installed Fix Pack 3 or earlier*) Comparison of installation processes for former fix packs versus recent fix packs" on page 81.

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 14.
	2. Based on the platform of your local host computer, download and extract the required fix pack files to a temporary location on your computer. You can use the following space to write down the location of your patch directory. **Patch directory:** _____

	3. Install the fix pack.
	For installations on Windows computers, if you plan to choose the option to upgrade the Java Runtime Environment, you must first stop all applications that are using the currently installed Java Runtime Environment. See "Ensuring success of Java Runtime Environment (JRE) upgrades on Windows" on page 72 for additional information.
	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 in Step 2.
	On Linux and UNIX computers, run the following command from the command line:
	`cd patch_dir`
	`./install.sh`
	Notes:
	a. From the component list, select only the components that you have previously installed for upgrade. The installer program displays the correct list of installed components from previous product or fix pack installations. If you clear an item that was selected, you will be removing or uninstalling the component rather than choosing not to upgrade it.
	b. On Windows computers, you must leave all of the items selected in the **Setup Type** window that is displayed after you install the fix pack.
	c. When you are prompted regarding the addition of application support for other products, add application support for the Tivoli Enterprise Portal Server, the browser client, and the desktop client.
	To become more familiar with the key options and settings for installation, see the "Installing IBM Tivoli Monitoring on one computer" topic in the *IBM Tivoli Monitoring Installation and Setup Guide*.

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

✓	Installation step
	4. On Linux and UNIX computers, reapply 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 itm_home] [-m] -t tems_name pc` "Parameters for the itmcmd support command" describes key parameters for the command. c. Run the following command to stop the monitoring server: `./itmcmd server stop tems_name` d. Run the following command to restart the monitoring server: `./itmcmd server start tems_name`
	5. On Linux and UNIX computers, reapply application support to the portal server as follows: a. Run the following command to stop the portal server: `./itmcmd agent stop cq` b. Run the following command to activate the application support on the portal server: `./itmcmd config -A cq` c. Run the following command to start the portal server: `./itmcmd agent start cq`
	6. If the installation of this component failed refer to the installation logs found in Table 10 on page 24 for a description of installation problems.
	7. If you run the Tivoli Enterprise Portal client in a non-English locale, you must apply the fix pack for the language pack after you install Fix Pack 6. Otherwise, certain user interface strings are displayed in English instead of the default language. (This requirement also applies if you reconfigure any of the base components, such as the portal server.) The name of the installation image is **6.1.0-TIV-ITM-LP-FP0006**. This update to the language pack includes a fix regarding an expired certificate, which was identified in APAR IZ03654. For information about installing the language packs, see the "Installing the language packs" section of the *IBM Tivoli Monitoring Installation and Setup Guide*.

Parameters for the itmcmd support command: The following list describes basic parameters for the **itmcmd support** command:

-h
(optional) Parameter to specify the installation directory if it is not the one in which this script is located. Typically, this parameter is not required. Also use this option to take action on an installation directory other than this one.

itm_home
The home directory that you created for IBM Tivoli Monitoring.

-m
(*Optional*) Option to skip the installation of the product-provided situations and policies.

-t Use this required option to specify the monitoring server name.

tems_name
Specifies the name of the monitoring server you are configuring. This argument is required.

Notes:
1. The monitoring server must be specified within the structure of *itm_home*.
2. Be very careful when you enter the *tems_name* on a UNIX or Linux system. If you enter the name incorrectly, you will create a new monitoring server instance instead of upgrading the existing one. To recover from this situation, refer to the appendix on uninstalling IBM Tivoli Monitoring components in the *IBM Tivoli Monitoring: Installation and Setup Guide*.

pc
The product code of the product that will connect to this monitoring server. You can specify one or more products for which to add application support. If you are specifying multiple products, you must separate the product codes with either a space or comma. To view the product code for the application support you just installed, run the `cinfo` command (for sample output, see "Validating what you installed" on page 46). The *pc* flag can be one of the following product codes:

- A4 - AS/400®
- LZ - Linux OS agent
- UL - UNIX Log agent
- UM - Tivoli Universal Agent
- UX - UNIX OS agent
- NT - Windows OS agent
- SY - Summarization and Pruning agent

Monitoring server checklist

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

Notes:

1. Only hub monitoring servers support SOAP servers. This clarifying statement is a result of APAR IY90757.
2. When a query through SOAP is issued to a monitoring agent such as the UNIX log agent, that query sometimes fails with a message such as ″Unable to start request.″ This failure is a timing error that occurs when the Tivoli Monitoring Services environment is starting up. The caching of nodes on a SOAP server is not complete when the first SOAP query is made.

   To recover from this situation, recycle the SOAP server and the hub and remote Tivoli Enterprise Monitoring Servers.
3. The process for updating the hub and remote monitoring servers is the same, although you must update the hub monitoring server first, as shown in the fix pack installation flow chart.
4. The process for updating distributed monitoring servers is shown in Table 13. The process for updating a monitoring server on z/OS is shown in Table 14 on page 36.

Note: You can directly upgrade from any previous IBM Tivoli Monitoring V6.1.0 Fix Pack to Fix Pack 6. After the upgrade you must use the component software from Fix Pack 6 for all subsequent updates that you make to your monitoring environment. In particular, you must not use the installation media from Fix Packs 1, 2, or 3. Otherwise, you might damage your environment. For detailed information, see “(*If you installed Fix Pack 3 or earlier*) Comparison of installation processes for former fix packs versus recent fix packs” on page 81.

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

✓	**Installation step**
	1. Gather information about the monitoring components in your environment. See “Fix pack installation planning worksheets” on page 14.
	2. In environments with multiple remote monitoring servers. to avoid communication problems after the installation, stop the monitoring agents associated with the monitoring server your are upgrading. Then stop the monitoring server you are upgrading.

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

✓	Installation step

	3. Install the fix pack.
	For installations on Windows computers, if you plan to choose the option to upgrade the Java Runtime Environment, you must first stop all applications that are using the currently installed Java Runtime Environment. See “Ensuring success of Java Runtime Environment (JRE) upgrades on Windows” on page 72 for additional information.
	On Windows computers, launch the installation wizard by double-clicking the **setup.exe** file in the `\WINDOWS` subdirectory in the patch directory that you specified previously.
	On Linux and UNIX computers, run the following command from the command line:
	`cd patch_dir`
	`./install.sh`
	Ensure that you select **Tivoli Enterprise Monitoring Server** from the component list.
	Note: Be very careful when you enter the *tems_name* on a UNIX or Linux system. If you enter the name incorrectly, you will create a new monitoring server instance instead of upgrading the existing one. To recover from this situation, refer to the appendix on uninstalling IBM Tivoli Monitoring components in the *IBM Tivoli Monitoring: Installation and Setup Guide*.
	Chapter 6, "Installing IBM Tivoli Monitoring," in the April, 2007 version of *IBM Tivoli Monitoring Installation and Setup Guide* provides additional information in the following sections:
	• **Windows:** "Installing and Configuring the Hub Tivoli Enterprise Monitoring Server" page 66, and "Installing and Configuring the remote Monitoring Servers" page 74
	• **UNIX:** "Installing and Configuring the Hub Tivoli Enterprise Monitoring Server" page 70, and "Installing and Configuring the remote Monitoring Servers" page 77

	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. **Note:** Follow these guidelines: • Be very careful when you enter the *tems_name* on a UNIX or Linux system. If you enter the name incorrectly, you will create a new monitoring server instance instead of upgrading the existing one. To recover from this situation, refer to the appendix on uninstalling IBM Tivoli Monitoring components in the *IBM Tivoli Monitoring: Installation and Setup Guide*. • The name of the configuration file for the Tivoli Enterprise Monitoring Server is case-sensitive on UNIX and Linux. If you fail to enter these case-sensitive commands correctly, you might find that the changes you made to the Tivoli Enterprise Monitoring Server configuration have not been picked up because a second configuration file has been generated and is not being used at monitoring server startup. To fix this problem: a. Look in the folder `/opt/IBM/ITM/config` to determine if there are two config files with similar names that differ only in the case of some part of the file name (for example, **/opt/IBM/ITM/config/winlnx1a_ms_WINLNX1A.config** and **/opt/IBM/ITM/config/WINLNX1A_ms_WINLNX1A.config**). b. Check the last modified timestamp of both files. Delete the older file and rename the new one as appropriate. **Regarding UNIX-based systems:** Chapter 6, "Installing IBM Tivoli Monitoring," in the April, 2007 version of *IBM Tivoli Monitoring Installation and Setup Guide* provides additional information in the following sections: • "Installing and Configuring the hub Tivoli Enterprise Monitoring Server," subsection "Configuring the hub monitoring servers," on page 71. • "Installing and Configuring the remote monitoring servers," subsection "Configuring the remote monitoring servers," on page 78.

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

✓	Installation step
	5. On the Linux and UNIX computers that you are upgrading, re-apply application support on your monitoring server. a. Run the following command to start the monitoring server: `./itmcmd server start tems_name` b. Run the following command to activate the application support on the monitoring server: `./itmcmd support [-h itm_home] [-m] -t tems_name pc` "Parameters for the itmcmd support command" on page 32 describes key parameters for the command. **Attention:** Do not reapply application support for any agent not listed here. Applying application support files for agents that were not updated as part of this fix pack might cause loss of customizations for those agents. c. Run the following command to stop the monitoring server: `./itmcmd server stop tems_name` d. Run the following command to restart the monitoring server: `./itmcmd server start tems_name`
	6. If you run the Tivoli Enterprise Portal client in a non-English locale, you must apply the fix pack for the language pack after you install Fix Pack 6. Otherwise, certain user interface strings are displayed in English instead of the default language. (This requirement also applies if you reconfigure any of the base components, such as the portal server.) The name of the installation image is **6.1.0-TIV-ITM-LP-FP0006**. This update to the language pack includes a fix regarding an expired certificate, which was identified in APAR IZ03654. For information about installing the language packs, see the "Installing the language packs" section of the *IBM Tivoli Monitoring Installation and Setup Guide*.
	7. If the installation of this component failed, refer to the installation logs found in Table 10 on page 24 for a description of installation problems.
	8. Install the fix pack on the remaining components: Be aware that you must upgrade additional product components, as described in Determining which components need to be upgraded to Fix Pack 6 • "General guidelines for upgrading components" on page 11 • "Determining which components are present on a specific computer" on page 12 • "Sequencing the upgrade procedures" on page 12

Table 14 shows the process for updating a Tivoli Enterprise Monitoring Server on z/OS systems.

Table 14. Checklist for installing the fix pack on the monitoring server on z/OS systems

✓	Installation step
	1. Gather information about the monitoring components in your environment. See "Fix pack installation planning worksheets" on page 14.
	2. Access the IBM Tivoli Monitoring Version 6 support page at http://www-306.ibm.com/software/sysmgmt/products/support/IBMTivoliMonitoringV6.html and select the link for Fix Pack 6. Select each of the levelset PTFs and install it using the typical z/OS SMP/E installation procedures.

Table 14. Checklist for installing the fix pack on the monitoring server on z/OS systems (continued)

✓	Installation step
	3. **Relink PTFs required for Fix Pack 6:** If you are running the monitoring agents for OMEGAMON XE version 4.1 or OMEGAMON XE for Messaging version 6.0, and have not applied the relink PTFs that were provided by the OMEGAMON products, apply the relink PTFs now. **Note:** The relink PTF's were required for Fix Pack 3. If you upgrade from Fix Pack 1 or 2 to Fix Pack 6, you should also apply the relink PTFs.Refer to the PSP information and ++HOLD information in the OMEGAMON XE relink PTFs for additional instruction. For additional OMEGAMON XE maintenance, refer to the Planning Upgrades section of the following Web site for OMEGAMON XE maintenance levels: http://www-306.ibm.com/software/sysmgmt/products/support/IBMTivoliMonitoringV6.html. Depending on how you configured your runtime environments (RTEs), you might need to reload your RTEs after applying maintenance. The RTE Load function is typically not required after applying maintenance for RTEs that share the SMP/E TARGET libraries. If your RTEs are not SMP/E-sharing RTEs, you will probably need to reload the RTEs after applying maintenance. Check the ++HOLD information associated with the PTFs for any additional installation or configuration requirements.
	4. Install the fix pack on the remaining components: portal server, portal desktop client, and monitoring agents (local and remote). The hub Tivoli Enterprise Monitoring Server, the Tivoli Enterprise Portal Server associated with the hub, and all of the Tivoli Enterprise Portal desktop clients that connect to that Tivoli Enterprise Portal Server must be upgraded to the same fix pack level. **Note:** This requirement also applies if you reconfigure any of the base components, such as the portal server.
	5. **For systems where the OMEGAMON XE on z/OS monitoring agent is used:** OMEGAMON XE on z/OS gives you the option to define a remote Tivoli Enterprise Monitoring Server as a sysplex proxy. (A sysplex proxy monitoring server is a data consolidation point for sysplex monitoring.) If you take advantage of this feature, *you must always start the sysplex proxy server first*. The next paragraph explains the reason for this requirement. See *Configuring Tivoli Enterprise Monitoring Server on z/OS* for IBM Tivoli Monitoring V6.1.0 for a description of "Starting the monitoring server on z/OS." The following scenario leads to an abnormal end of task (ABEND) or even a complete stoppage of IBM Tivoli Monitoring: a. As allowed in a system where OMEGAMON XE on z/OS is used, you define a Tivoli Enterprise Monitoring Server as a sysplex proxy. b. You fail to start the sysplex proxy first when you start monitoring activity. Instead, you start another monitoring server. c. The system recognizes that a sysplex proxy has been defined, but is missing, and the system configures the server that first starts as a sysplex proxy. d. When you launch the server that was defined as the sysplex proxy, a conflict is generated and this server experiences an abnormal end of task (ABEND). If this server is also defined as the hub monitoring server, the entire IBM Tivoli Monitoring environment stops functioning. To avoid this scenario, always start *first* the monitoring server that you define as the sysplex proxy.

For other monitoring server on z/OS issues, see "Tivoli Enterprise Monitoring Server" on page 85.

Portal server checklist

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

Note: You can directly upgrade from any previous IBM Tivoli Monitoring V6.1.0 Fix Pack to Fix Pack 6. After the upgrade you must use the component software from Fix Pack 6 for all subsequent updates that you make to your monitoring environment. In particular, you must not use the installation media from Fix Packs 1, 2, or 3. Otherwise, you might damage your environment. For detailed information, see "(*If you installed Fix Pack 3 or earlier*) Comparison of installation processes for former fix packs versus recent fix packs" on page 81.

Table 15. 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 14.
	2. Based on the platform of your local host computer, download and extract the required fix pack files to a temporary location on your computer. You can use the following space to write down the location of your patch directory. **Patch directory:** _____
	3. Before you install the fix pack on a Tivoli Enterprise Portal Server on a Windows computer, ensure that the Windows Script Host (WSH) is at least version 5.6. You can check the version by running the **cscript** command.
	4. Close any instances of the Tivoli Enterprise Portal browser client that might be open. Otherwise, these instances are unable to run updated **.jar** files.

	5. Install the fix pack.
	For installations on Windows computers, if you plan to choose the option to upgrade the Java Runtime Environment, you must first stop all applications that are using the currently installed Java Runtime Environment. See “Ensuring success of Java Runtime Environment (JRE) upgrades on Windows” on page 72 for additional information.
	On Windows computers, launch the installation wizard by double-clicking the setup.exe file in the \WINDOWS subdirectory in the patch directory that you specified above.
	On Linux and UNIX computers, run the following command from the command line:
	`cd patch_dir`
	`./install.sh`
	Ensure that you select **Tivoli Enterprise Portal Server** from the component list.
	Notes:
	a. On Windows computers, you must leave all of the items selected in the **Setup Type** window that is displayed during the installation process.
	b. When you are asked if you want to add application support for other products, add application support for the Tivoli Enterprise Portal Server.
	c. Confirm that the Tivoli Enterprise Portal Server is running after upgrade. If it is not, restart it.
	Chapter 6, "Installing IBM Tivoli Monitoring," in the April, 2007 version of *IBM Tivoli Monitoring Installation and Setup Guide* provides additional information in the following sections:
	• **Windows:** "Installing the Tivoli Enterprise Portal Server," page 79.
	• **UNIX:** "Installing the Tivoli Enterprise Portal Server," page 84.

	6. If you run the Tivoli Enterprise Portal client in a non-English locale, you must apply the fix pack for the language pack after you install Fix Pack 6. Otherwise, certain user interface strings are displayed in English instead of the default language. (This requirement also applies if you reconfigure any of the base components, such as the portal server.) The name of the installation image is **6.1.0-TIV-ITM-LP-FP0006**. This update to the language pack includes a fix regarding an expired certificate, which was identified in APAR IZ03654. For information about installing the language packs, see the “Installing the language packs” section of the *IBM Tivoli Monitoring Installation and Setup Guide*.
	7. If the installation of this component failed refer to the installation logs found in Table 10 on page 24 for a description of installation problems.

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

✓	Installation step
	8. On Linux and UNIX computers, apply application support to the portal server as follows: a. Run the following command to stop the portal server: `./itmcmd agent stop cq` b. Run the following command to activate the application support on the portal server: `./itmcmd config -A cq` c. Run the following command to start the portal server: `./itmcmd agent start cq` For UNIX-based systems, Chapter 6, "Installing IBM Tivoli Monitoring," in the April, 2007 version of *IBM Tivoli Monitoring Installation and Setup Guide* provides additional information in "Installing the Tivoli Enterprise Portal Server," subsection "Configuring the portal server on Linux or AIX: command line procedure," page 87.
	9. Install the fix pack on the remaining components: portal desktop client and monitoring agents (local and remote). You must upgrade the Tivoli Enterprise Portal Server and the Tivoli Enterprise Portal desktop and browser clients to the same fix pack level. For more information, see “Determining which components need to be upgraded to Fix Pack 6” on page 11.

If you are upgrading from IBM Tivoli Monitoring Version 6.1 Fix Pack 2 or earlier, you must migrate any custom workspaces containing Situation Event Console Views manually using this script and procedure:

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

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

where:

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

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

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

Portal desktop client checklist

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

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

Note: You can directly upgrade from any previous IBM Tivoli Monitoring V6.1.0 Fix Pack to Fix Pack 6. After the upgrade you must use the component software from Fix Pack 6 for all subsequent updates that you make to your monitoring environment. In particular, you must not use the installation media from Fix Packs 1, 2, or 3. Otherwise, you might damage your environment. For detailed information, see “(*If you installed Fix Pack 3 or earlier*) Comparison of installation processes for former fix packs versus recent fix packs” on page 81.

Table 16. 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 14.
	2. Based on the platform of your local host computer, download and extract the required fix pack files to a temporary location on your computer. You can use the following space to write down the location of your patch directory. **Patch directory:** _____
	3. Close the Tivoli Enterprise Portal desktop client on the system where you are installing the fix pack.

	4. Install the fix pack.
	For installations on Windows computers, if you plan to choose the option to upgrade the Java Runtime Environment, you must first stop all applications that are using the currently installed Java Runtime Environment. See “Ensuring success of Java Runtime Environment (JRE) upgrades on Windows” on page 72 for additional information.
	On Windows computers, launch the installation wizard by double-clicking the setup.exe file in the \WINDOWS subdirectory in the patch directory that you specified above.
	On Linux and UNIX computers, run the following command from the command line:
	`cd patch_dir`
	`./install.sh`
	Ensure that you select **Tivoli Enterprise Portal Desktop Client** from the component list.
	Notes:
	a. On Windows computers, you must leave all of the items selected in the **Setup Type** window that is displayed during the installation process.
	b. When you are asked if you want to add application support for other products, add application support for the desktop client.
	Chapter 6, "Installing IBM Tivoli Monitoring," in the April, 2007 version of *IBM Tivoli Monitoring Installation and Setup Guide* provides additional information in the following sections:
	• **Windows:** "Installing the Tivoli Enterprise Portal desktop client," page 103.
	• **UNIX:** "Installing the Tivoli Enterprise Portal desktop client," page 105.

Table 16. Checklist for installing the fix pack on the portal desktop client (continued)

✓	Installation step
	5. If you run the Tivoli Enterprise Portal client in a non-English locale, you must apply the fix pack for the language pack after you install Fix Pack 6. Otherwise, certain user interface strings are displayed in English instead of the default language. (This requirement also applies if you reconfigure any of the base components, such as the portal server.) The name of the installation image is **6.1.0-TIV-ITM-LP-FP0006**. This update to the language pack includes a fix regarding an expired certificate, which was identified in APAR IZ03654. For information about installing the language packs, see the "Installing the language packs" section of the *IBM Tivoli Monitoring Installation and Setup Guide*.
	6. If the installation of this component failed refer to the installation logs found in Table 10 on page 24 for a description of installation problems.
	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 OS monitoring agents that ship as part of base IBM Tivoli Monitoring. Other monitoring agents that ship as separate products are accompanied by readme files that contain additional information.

Notes:

1. The installation procedures are the same as used for the GA level installation. For detailed installation procedures, see the "Installing IBM Tivoli Monitoring" chapter in the *IBM Tivoli Monitoring Installation and Setup Guide*.
2. This checklist is for a local installation of the monitoring agents. You can also use the remote deployment function to deploy the monitoring agents across your monitoring environment. the remote deployment function, use the steps in the "Monitoring agent checklist - remote deployment" on page 43.
3. For local installations, if you have the Tivoli Universal Agent installed on a UNIX or Linux computer, you must upgrade the Tivoli Universal Agent at the same time that you upgrade any other component to Fix Pack 6.
4. You can directly upgrade from any previous IBM Tivoli Monitoring V6.1.0 Fix Pack to Fix Pack 6. After the upgrade you must use the component software from Fix Pack 6 for all subsequent updates that you make to your monitoring environment. In particular, you must not use the installation media from Fix Packs 1, 2, or 3. Otherwise, you might damage your environment. For detailed information, see "(*If you installed Fix Pack 3 or earlier*) Comparison of installation processes for former fix packs versus recent fix packs" on page 81.

Table 17. 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 14.
	2. Based on the platform of your local host computer, download and extract the required fix pack files to a temporary location on your computer. You can use the following space to write down the location of your patch directory. **Patch directory:** _____

Table 17. Checklist for locally installing the fix pack on an agent (continued)

✓	Installation step

	3. Install the fix pack.
	For installations on Windows computers, if you plan to choose the option to upgrade the Java Runtime Environment, you must first stop all applications that are using the currently installed Java Runtime Environment. See “Ensuring success of Java Runtime Environment (JRE) upgrades on Windows” on page 72 for additional information.
	On Windows computers, launch the installation wizard by double-clicking the setup.exe file in the \WINDOWS subdirectory in the patch directory that you specified above.
	On Linux and UNIX computers, run the following command from the command line:
	`cd patch_dir`
	`./install.sh`
	Ensure that you select the monitoring agents that you are upgrading from the component list.
	Note: On Windows computers, you must leave all of the items selected in the **Setup Type** window that is displayed after you install the fix pack.Chapter 6, "Installing IBM Tivoli Monitoring," in the April, 2007 version of *IBM Tivoli Monitoring Installation and Setup Guide* provides additional information in the following sections:
	• **Windows:** ″Installing monitoring agents,″ page 97.
	• **UNIX:** ″Installing monitoring agents,″ page 100.

	4. For OS agents, if you run the Tivoli Enterprise Portal client in a non-English locale, you must apply the fix pack for the language pack after you install Fix Pack 6. Otherwise, certain user interface strings are displayed in English instead of the default language. (This requirement also applies if you reconfigure any of the base components, such as the portal server.) The name of the installation image is **6.1.0-TIV-ITM-LP-FP0006**. This update to the language pack includes a fix regarding an expired certificate, which was identified in APAR IZ03654. For information about installing the language packs, see the “Installing the language packs” section of the *IBM Tivoli Monitoring Installation and Setup Guide*.
	5. If the installation of this component failed refer to the installation logs found in Table 10 on page 24 for a description of installation problems.

Monitoring agent checklist - remote deployment

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

Note: Only Tivoli-provided product agent bundles should be loaded into the IBM Tivoli Monitoring deploy depot. User provided or customized bundles are not supported. Use only Tivoli provided **tacmd** commands (as described in the checklist below) to process bundles and to execute agent remote deployments. Manual manipulation of the depot directory structure or the bundles and files within it is not supported and may void your warranty.

Consider increasing the default 30-minute timeout period of **tacmd** commands to ensure that fix pack deployment succeeds, as in the following example procedure:

1. Use a text editor to open the file that contains environment variables:
   - **On Linux and UNIX computers:** Edit the *itm_home*/bin/tacmd file.
   - **On Windows computers:** Edit the *itm_home*/bin/KUIENV file.
2. Update the timeout value to 60 minutes, as in this example: **TACMD_TIMEOUT=60**. The valid range for the timeout period is from 5 to 1440 minutes.

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

Note: You can directly upgrade from any previous IBM Tivoli Monitoring V6.1.0 Fix Pack to Fix Pack 6. After the upgrade you must use the component software from Fix Pack 6 for all subsequent updates that you make to your monitoring environment. In particular, you must not use the installation media from Fix Packs 1, 2, or 3. Otherwise, you might damage your environment. For detailed information, see “(*If you installed Fix Pack 3 or earlier*) Comparison of installation processes for former fix packs versus recent fix packs” on page 81.

Table 18. Checklist for remotely deploying the fix pack to an agent

✓	Installation step
	1. **tacmd login:** Run the following command to gain full authorization to use the **tacmd** command-line interface: `tacmd login -s host` where *host* specifies a hub Tivoli Enterprise Monitoring Server that you want to log into. See the *IBM Tivoli Monitoring Command Reference* for additional command reference information. 2. Respond to the **tacmd login** command prompts by providing a valid user name and password for the IBM Tivoli Monitoring environment.

Table 18. Checklist for remotely deploying the fix pack to an agent (continued)

✓	Installation step

	3. **tacmd addBundles:** Run the following command to add the updated agent software to your deployment depots:
	`itm_home/bin/tacmd addBundles -i descriptor_directory`
	
	where *itm_home* is the directory where you installed IBM Tivoli Monitoring and *descriptor_directory* is the path to the directory in the fix pack directory tree that contains the ***.dsc** files that describe the agent deploy bundles.
	• For UNIX images, the files are located in the **unix** directory in the fixpack directory tree. So, for example, if the fixpack is located at `/fp6dir/aix`, the command to use is as follows:
	`tacmd addBundles -i /fp6dir/aix/unix`
	• For Windows, the location is the `WINDOWS\Deploy` directory in the fix pack directory tree. So, for example, if the fix pack is located at `C:\temp\itmfp6`, the command to use is as follows:
	`tacmd addBundles -i C:\fp6dir\WINDOWS\Deploy`
	
	Note: If agents on your target machine connect to a remote monitoring server, you must add bundles on both the remote monitoring server and the hub monitoring server.
	See the *IBM Tivoli Monitoring Installation and Setup Guide* for additional information on using remote deploy. See the *IBM Tivoli Monitoring Command Reference* for additional command reference information.

	4. **tacmd listSystems:** On the hub monitoring server, run the **tacmd listSystems** command to obtain a list of managed systems. The following excerpt shows partial output only, but illustrates the typical format and syntax of the information:
	`./tacmd listSystems`
	`Managed System Name Product Code Version Status`
	`guru.lab.ibm.com:LZ LZ 06.10.06.00 Y`
	`NM15.lab.ibm.com:LZ LZ 06.10.06.00 Y`
	`Primary:X3A30S8:NT NT 06.10.06.00 Y`
	`Primary:X3A30S13:NT NT 06.10.06.00 Y`
	`HUB_X3A30S13 EM 06.10.06.00 Y`
	`apollo:KUX UX 06.10.06.00 Y`
	
	See the *IBM Tivoli Monitoring Command Reference* for additional command reference information.

	5. **tacmd updateAgent:** On the hub monitoring server, run the **tacmd updateAgent** command to remotely deploy the agent fix packs.
	`tacmd updateAgent -t pc -n node_name`
	
	where *pc* is the product code and *node_name* is a string that identifies the target computer and node, as provided by the **tacmd listSystems** command. The following example includes a name from the sample output in Step 4:
	`tacmd updateAgent -t NT -n Primary:X3A30S9:NT`
	
	See “Summary of tacmd updateAgent command information” on page 46 for further information on the parameters.

Table 18. Checklist for remotely deploying the fix pack to an agent (continued)

✓	Installation step

Deployment tips: The following tips help you improve or troubleshoot the deployment process:
• 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.
• The remote deployment of the Windows OS Agent now requires Java. If you use the `tacmd updateAgent` command to update an agent on a remote Windows workstation or server, the deployment can fail because of this new Java requirement. The following error messages are typical:
`KUICUA011I: Updating the NT agents.`
`KUICUA015E: The updateAgent command did not complete because an error occurred.`
`Refer to the following error returned from the server:`
If you see these messages, you have “Options for resolving a Java error” on page 45, which are listed after this table.	

	6. For OS agents, if you run the Tivoli Enterprise Portal client in a non-English locale, you must apply the fix pack for the language pack after you install Fix Pack 6. Otherwise, certain user interface strings are displayed in English instead of the default language. (This requirement also applies if you reconfigure any of the base components, such as the portal server.) The name of the installation image is **6.1.0-TIV-ITM-LP-FP0006**. This update to the language pack includes a fix regarding an expired certificate, which was identified in APAR IZ03654. For information about installing the language packs, see the “Installing the language packs” section of the *IBM Tivoli Monitoring Installation and Setup Guide*.
	7. If the installation of this component failed refer to the KUI log and the log for the monitoring server. The installation logs listed in Table 10 on page 24 can also help you trace installation problems.

The location of the depot directory in the monitoring server is as follows:

- On Windows, the depot directory is *itm_home*\CMS\Depot.
- On UNIX and Linux systems, the depot is *itm_home*/tables/TEMSServer_ms_TEMSName/depot.

For additional information about deployment issues, refer to the *IBM Tivoli Monitoring V6.1 Deployment Guide* found at the following URL in the Tivoli Open Process Automation Library (OPAL) Web site: http://www.ibm.com/software/tivoli/opal/?NavCode=1TW10TM4J.

Options for resolving a Java error

This section lists options for resolving the Java error that is described in the preceding table.

- **Option 1:** Review the list of fixed APARs, Chapter 6, “APARs addressed by Fix Pack 6,” on page 107. If the Windows OS agent does not need any of the fixes covered by these APARs, do not install the fix pack for the Windows OS agent.

  OR

- **Option 2:** Use the following workaround to install the fix pack:
  1. Log on to the remote system and open a command window.
  2. Navigate to the directory where the product is installed. (For example, on Windows the product is installed by default in the following directory path: `C:\IBM\ITM`.)
  3. Navigate to the `tmaitm6\agentdepot\061006000\InIBMJRE` directory.
  4. From that directory, install Java version 1.4.2 on the remote computer by launching **ibmjava142.exe** and accepting all the default values. You can choose a different installation drive, but do not change the directory structure for the installation.
  5. After Java is installed, run the `tacmd updateAgent` command from the original deployment server to deploy and update the agent.

Summary of *tacmd updateAgent* command information::

This section introduces some of the parameters for the **tacmd updateAgent** command that you use to apply a fix pack to an agent. See the *IBM Tivoli Monitoring Command Reference* for additional command reference information.

pc

Identifies the product that you want to update. You have the following choices:

- A4 - AS/400
- LZ - Linux OS agent (OS stands for "Operating System".)
- UL - UNIX Log agent
- UM - Tivoli Universal Agent
- UX - UNIX OS agent
- NT - Windows OS agent
- SY - Summarization and Pruning agent

node_name

Identifies the node, the directory on the monitoring system where the OS agent is installed, to which you want to add the agent. The name of a node includes the computer where the OS agent is installed and the product code for the OS agent. For example, **stone.ibm.com:LZ** is the name of the node on computer **stone.ibm.com**, which has a Linux OS agent installed.

Examples

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 Tivoli Universal Agent running on a UNIX computer to a specific fix pack level:

```
tacmd updateAgent -t um -n unix1:KUX -v 061003010
```

Validating what you installed

To validate that all components have been installed and are at the correct levels, open the Manage Tivoli Monitoring Services status window, and compare your screen to the levels shown in Figure 2 on page 47.

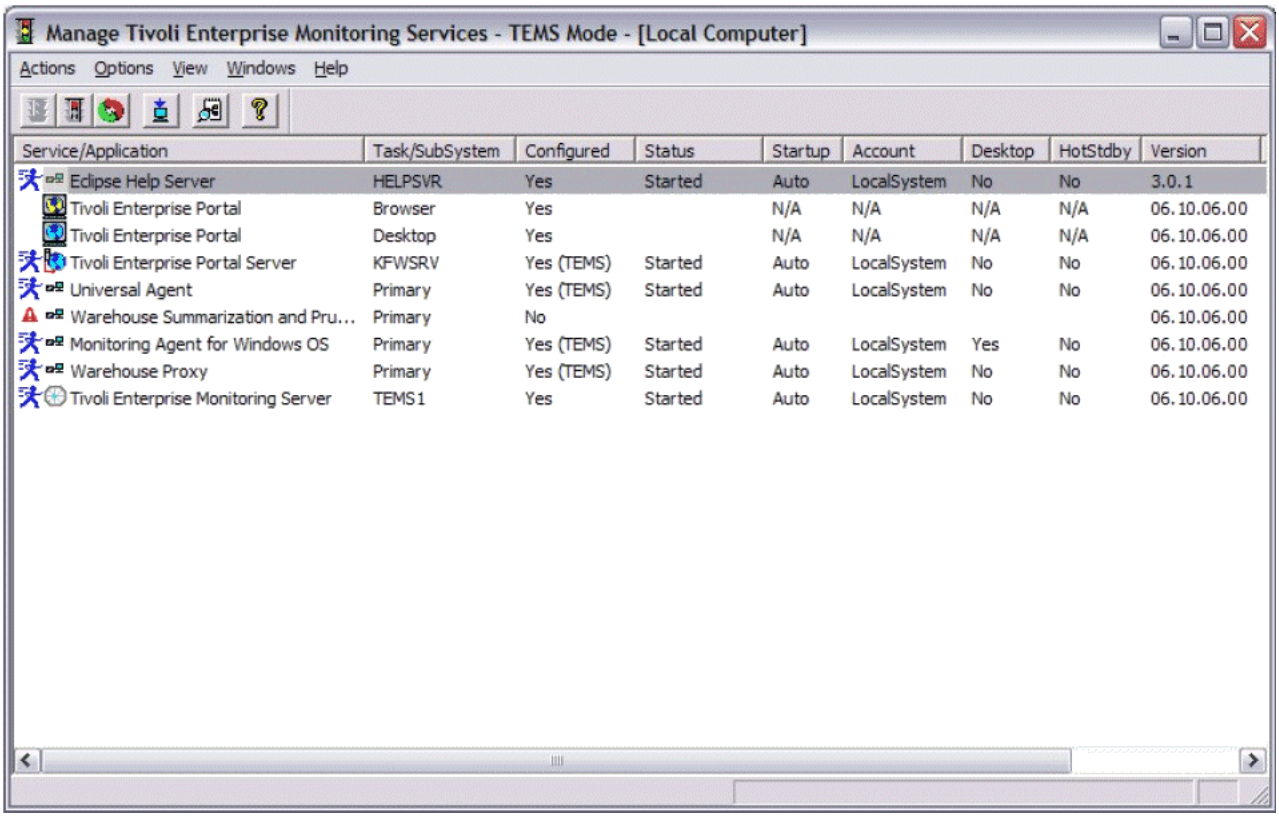


Figure 2. Levels for all components following the installation of Fix Pack 6

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

Note: The `kincinfo` and `cinfo` command output examples in the following sections show examples of components that can be updated. If you do not have all of these components installed, you do not see the same list when you run these commands.

Sample output for the kincinfo command on Windows

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

`kincinfo` *parameter*

where *parameter* is one of the following options:

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

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

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

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

```
A4        i5/OS Support
          WINNT Version: 06.10.06.00 Build: 200702230014

A4        i5/OS Support
          WINNT Version: 06.10.06.00 Build: 200702230014

A4        i5/OS Support
          WINNT Version: 06.10.06.00 Build: 200702230014

A4        i5/OS Support
          WINNT Version: 06.10.06.00 Build: 200702230014

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

CJ        Tivoli Enterprise Portal Desktop Client
          WINNT Version: 06.10.06.00 Build: 200705012123

CQ        Tivoli Enterprise Portal Server
          WINNT Version: 06.10.06.00 Build: 200705012135

CW        Tivoli Enterprise Portal Browser Client
          WINNT Version: 06.10.06.00 Build: 200705012123

GL        Tivoli Enterprise Monitoring Agent Framework
          WINNT Version: 06.10.06.00 Build: 200705012139

HD        Warehouse Proxy
          WINNT Version: 06.10.06.00 Build: 200705012139

IT        TEC GUI Integration
          WINNT Version: 06.10.06.00 Build: 200611010030

IT        TEC GUI Integration
          WINNT Version: 06.10.06.00 Build: 200611010031

IT        TEC GUI Integration
          WINNT Version: 06.10.06.00 Build: 200611010030

KF        IBM Eclipse Help Server
          WINNT Version: 06.10.06.00 Build: 200704171107

LZ        Linux OS Support
          WINNT Version: 06.10.06.00 Build: 200704301644

LZ        Linux OS Support
          WINNT Version: 06.10.06.00 Build: 200704301644

LZ        Linux OS Support
          WINNT Version: 06.10.06.00 Build: 200704301644

LZ        Linux OS Support
          WINNT Version: 06.10.06.00 Build: 200704301644

MS        Tivoli Enterprise Monitoring Server
          WINNT Version: 06.10.06.00 Build: 200705012139

NS        NLS Support
          WINNT Version: 03.50.03.00 Build: 200510061051

NT        Monitoring Agent for Windows OS
          WINNT Version: 06.10.06.00 Build: 200701160818

NT        Windows OS Support
          WINNT Version: 06.10.06.00 Build: 200701160818
```

```
NT        Windows OS Support
          WINNT Version: 06.10.06.00 Build: 200701160818

NT        Windows OS Support
          WINNT Version: 06.10.06.00 Build: 200701160818

NT        Windows OS Support
          WINNT Version: 06.10.06.00 Build: 200701160818

SY        Summarization and Pruning Agent
          WINNT Version: 06.10.06.00 Build: 200705012135

SY        Summarization and Pruning Agent
          WINNT Version: 06.10.06.00 Build: 200705012135

TM        IBM Tivoli Monitoring 5.x Endpoint Support
          WINNT Version: 06.10.06.00 Build: 200604051327

TM        IBM Tivoli Monitoring 5.x Endpoint Support
          WINNT Version: 06.10.06.00 Build: 200604051327

UI        Tivoli Enterprise Services User Interface
          WINNT Version: 06.10.06.00 Build: 200705012139

UL        UNIX Logs Support
          WINNT Version: 06.10.06.00 Build: 200701120847

UL        UNIX Logs Support
          WINNT Version: 06.10.06.00 Build: 200701120847

UL        UNIX Logs Support
          WINNT Version: 06.10.06.00 Build: 200701120847

UL        UNIX Logs Support
          WINNT Version: 06.10.06.00 Build: 200701120847

UM        Universal Agent
          WINNT Version: 06.10.06.00 Build: 200705012131

UM        Universal Agent Support
          WINNT Version: 06.10.06.00 Build: 200705012131

UM        Universal Agent Support
          WINNT Version: 06.10.06.00 Build: 200705012131

UM        Universal Agent Support
          WINNT Version: 06.10.06.00 Build: 200705012131

UM        Universal Agent Support
          WINNT Version: 06.10.06.00 Build: 200705012131

UX        UNIX OS Support
          WINNT Version: 06.10.06.00 Build: 200701161329

UX        UNIX OS Support
          WINNT Version: 06.10.06.00 Build: 200701161329

UX        UNIX OS Support
          WINNT Version: 06.10.06.00 Build: 200701161329

UX        UNIX OS Support
          WINNT Version: 06.10.06.00 Build: 200701161329

C:\ >
```

Sample output for the cinfo command on UNIX or Linux

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

```
./cinfo
```

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

```
*********** Mon May  7 14:35:50 EDT 2007 ******************
User      : root         Group: root sys dasadm1 db2grp1 db2fgrp1
Host name : cvtlin01     Installer Lvl:06.10.06.00
CandleHome: /usr/IBM/ITM
***********************************************************

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

*********** Mon May  7 14:35:53 EDT 2007 ******************
User      : root         Group: root sys dasadm1 db2grp1 db2fgrp1
Host name : cvtlin01     Installer Lvl:06.10.06.00
CandleHome: /usr/IBM/ITM
***********************************************************
...Product inventory

a4      Monitoring Agent for i5/OS
         tms     Version: 06.10.06.00
         tpd     Version: 06.10.06.00
         tps     Version: 06.10.06.00
         tpw     Version: 06.10.06.00

ax      IBM Tivoli Monitoring Shared Libraries
         li6243  Version: 06.10.06.00

cj      Tivoli Enterprise Portal Desktop Client
         li6263  Version: 06.10.06.00

cq      Tivoli Enterprise Portal Server
         li6263  Version: 06.10.06.00

cw      Tivoli Enterprise Portal Browser Client
         li6263  Version: 06.10.06.00

hd      Warehouse Proxy
         li6243  Version: 06.10.06.00

it      TEC GUI Integration
         tpd     Version: 06.10.06.00
         tps     Version: 06.10.06.00
         tpw     Version: 06.10.06.00

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

kf      IBM Eclipse Help Server
         li6243  Version: 06.10.06.00

lz      Monitoring Agent for Linux OS
         li6263  Version: 06.10.06.00
         tms     Version: 06.10.06.00
         tpd     Version: 06.10.06.00
         tps     Version: 06.10.06.00
         tpw     Version: 06.10.06.00
```

```
ms      Tivoli Enterprise Monitoring Server
         li6243  Version: 06.10.06.00

nt      Monitoring Agent for Windows OS
         tms     Version: 06.10.06.00
         tpd     Version: 06.10.06.00
         tps     Version: 06.10.06.00
         tpw     Version: 06.10.06.00

sh      Tivoli Enterprise Monitoring SOAP Server
         li6243  Version: 06.10.06.00

sy      Summarization and Pruning Agent
         li6243  Version: 06.10.06.00
         tms     Version: 06.10.06.00

tm      Monitoring Agent for IBM Tivoli Monitoring 5.x Endpoint
         tms     Version: 06.10.06.00
         tps     Version: 06.10.06.00

uf      Universal Agent Framework
         li6243  Version: 06.10.06.00

ui      Tivoli Enterprise Services User Interface
         li6243  Version: 06.10.06.00

ul      Monitoring Agent for UNIX Logs
         li6243  Version: 06.10.06.00
         tms     Version: 06.10.06.00
         tpd     Version: 06.10.06.00
         tps     Version: 06.10.06.00
         tpw     Version: 06.10.06.00

um      Universal Agent
         li6243  Version: 06.10.06.00
         tms     Version: 06.10.06.00
         tpd     Version: 06.10.06.00
         tps     Version: 06.10.06.00
         tpw     Version: 06.10.06.00

ux      Monitoring Agent for UNIX OS
         tms     Version: 06.10.06.00
         tpd     Version: 06.10.06.00
         tps     Version: 06.10.06.00
         tpw     Version: 06.10.06.00

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

Installing the fix pack for the i5/OS monitoring agent

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

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

Special instructions

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

Special notes on i5/OS monitoring agent product information:

- The OS400_Comm_FunctnChk_Workaround situation has been deleted for this fix pack because this workaround is no longer required.
- 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. As a result, the situation formula changes 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.

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. Use the following process to restore the user authorities.

- **Before installing the agent fix pack:**

  Be aware that all user profiles that have been granted special authority to OMA objects. See the following example of locating special authority to one OMA object:

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

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

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

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

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

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

- **After installing the agent fix pack:**

  Restore the saved user profiles. Example:

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

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

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

  Verify that the special authorities have been restored.

Installing the i5/OS agent fix pack checklist

Use the following steps to install the fix pack:

Table 19. Checklist for remotely deploying the fix pack to an i5/OS agent

✓	Installation step
	1. Copy the **a4520cma.sav** agent binary to a computer with FTP access to the i5/OS agent system. You must copy the **a4530cma.sav** save file to `c:\temp` directory. (Step 9 on page 53 instructs yo to FTP the **a4520cma.sav** from `c:\temp`.) The **a4530cma.sav** save file is found in one of these locations: • **Windows CD image**: `OS400\TMAITM6` directory • **UNIX or Linux CD image:** `OS400/TMAITM6` directory

Table 19. Checklist for remotely deploying the fix pack to an i5/OS agent (continued)

✓	Installation step
	2. On the i5/OS agent's system command line, create a CCCINST library, if this library does not already exist: `CRTLIB LIB(CCCINST)`
	3. Determine which version of the agent, if any, is currently installed using the **DSPSFWRSC** command. If products 0KA4430, 0KA4440, or 0KA4610 are listed then an agent is already installed. If 0KA4430, 0KA4440, or 0KA4610 is already installed, skip to Step 4. If no agent was previously installed, skip to Step 8.
	4. Enter `GO OMA` to display the Tivoli Monitoring: i5/OS Agent panel. Use option 4, Configuration, and record the Tivoli Enterprise Monitoring Server values and port numbers. Use **F12** to exit without updating the existing configuration.
	5. Use **GO OMA** option 3 to end the agent and then use F3 to exit the OMA Menu. Make sure that no other users are displaying the Tivoli Monitoring: i5/OS Agent panel.

	6. Create a save file on the target i5/OS computer and save the existing agent if desired. Saving the current agent enables you to restore it if you later choose to remove the new version. This step is optional.
	`CRTSAVF yourlib/PREFP06KA4`
	`SAVLICPGM LICPGM(0KA4yyy) DEV(*SAVF) SAVF(yourlib/PREFP03KA4)`
	where *yyy* can be 430, 440, or 610

	7. Use command **DLTLICPGM 0KA4430** if product 0KA4430 exists on the system, or use command **DLTLICPGM 0KA4440** if product 0KA4440 exits on the system. It is not required to delete product 0KA4610, although you might choose to do so using command **DLTLICPGM 0KA4610**.
	8. Create a save file on the target i5/OS system for the fix pack: `CRTSAVF CCCINST/A4520CMA TEXT('ITM 6.1 Fix Pack 6')`

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

	10. Load the fix pack from the save file:
	a. If you are installing the product on a computer that has English uppercase and lowercase 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)`

Table 19. Checklist for remotely deploying the fix pack to an i5/OS agent (continued)

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

Installing the IBM Tivoli Enterprise Console event synchronization fix pack

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

- "Fix pack prerequisites" on page 55
- "Notes regarding rule bases" on page 55
- "Important information for Windows users" on page 56
- "Installation instructions" on page 57
- "Modifying your rule base after installation" on page 61
- "Closing sampled events in IBM Tivoli Enterprise Console" on page 61
- "Verifying the installation of the event synchronization fix pack" on page 62
- "Uninstalling the IBM Tivoli Enterprise Console event synchronization" on page 62

If you enable IBM Tivoli Enterprise Console event forwarding on IBM Tivoli Monitoring 6.1 at the Fix Pack 6 level, then IBM Tivoli Enterprise Console Event Synchronization is also required to be at the Fix Pack 6 level on the IBM Tivoli Enterprise Console server. This is required for the event server to correctly parse events coming from the IBM Tivoli Monitoring 6.1 Fix Pack 6 level monitoring server.

Note: When fix pack installation on all components is complete, you must restart the IBM Tivoli Enterprise Console server. Your modifications take effect after the restart. (If you choose to automatically update a rule base, the installer prompts you to restart the IBM Tivoli Enterprise Console server and gives you the option to manually restart the server.)

New (non-upgrade) installations

To install IBM Tivoli Monitoring and IBM Tivoli Enterprise Console event synchronization in a new environment, use the installer found with the installation media and named **setup***operating_system***.bin** (for Windows, this file has a **.exe** tag) and use the installation instructions provided in the ″Installing the IBM Tivoli Enterprise Console event synchronization″ chapter in the latest version of the *IBM Tivoli Monitoring Installation and Setup Guide*. These setup files should be used for new installs only. If you run them on a system where Event Synchronization is installed, the installer detects a previous installation and does not continue.

Determining which level of event synchronization is installed

To verify which level of IBM Tivoli Enterprise Console event synchronization is installed on your computer, perform one of the platform-specific actions shown in Table 20 on page 55.

Table 20. Determining the level of IBM Tivoli Enterprise Console event synchronization installed by platform

Platform	Action
Windows	1. Open or list the **vpd.properties** file, located in the *<Operating_System_Drive>\<OS_Name>* directory (for example, `C:\windows` or `c:\winnt`). 2. Verify that the value associated with the `TecEvntSyncInstaller` string is `|1|0|6|0|1.0.0.6`, which indicates that Fix Pack 6 has been applied.
HP11	Run the following command from a user ID with root or administrator privileges: `swlist -v TecEvntSyncInstaller` Verify that the value associated with the `ismp_key` parameter has a value of `1.0.0.6`, which indicates that Fix Pack 6 has been applied.
AIX	1. Change to the `/usr/lib/objrepos` directories. 2. Open or list the **vpd.properties** file. 3. Verify that the value associated with the `TecEvntSyncInstaller` string is `|1|0|6|0|1.0.0.6`, which indicates that Fix Pack 6 has been applied
Linux (SLES and RHEL)	1. Open or list the **vpd.properties** file is in the `/` or `/root` directory. 2. Verify that the value associated with the `TecEvntSyncInstaller` string is `|1|0|6|0|1.0.0.6`, which indicates that Fix Pack 6 has been applied.
Solaris	Run the following command from a user ID with root or administrator privileges: `pkginfo -l ISitmTecE` Verify that the displayed values for the `Version` parameter include a value of `1.0.6.0.DSP=1.0.0.6`, which indicates that Fix Pack 6 is applied.

Fix pack prerequisites

You must account for the following issues before installing IBM Tivoli Enterprise Console (TEC) event synchronization fix pack on your Tivoli Enterprise Console event server:

- Before you can install this fix pack as an upgrade, you must have installed one of the following on your computer, with an IBM Tivoli Enterprise Console event server:
  - The base IBM Tivoli Enterprise Console event synchronization available with the GA level of IBM Tivoli Monitoring Version 6.1

    OR
  - IBM Tivoli Monitoring and IBM Tivoli Enterprise Console Event Synchronization Fix Pack 1, available with the GA level of IBM Tivoli Monitoring Version 6.1 Fix Pack 1

  The IBM Tivoli Monitoring and IBM Tivoli Enterprise Console Event Synchronization Fix Pack 3, that comes with IBM Tivoli Monitoring Version 6.1 Fix Pack 3 is also a valid starting point for upgrading event synchronization to the Fix Pack 6 level.
- If you have IBM Tivoli Enterprise Console event synchronization installed on your computer already, first determine which version is installed (see Table 20 for assistance). If the version installed is 1.0.0.6 (Fix Pack 6), you are at the current level. If the version installed is earlier than version 1.0.0.6, you can install the version that comes with Fix Pack 6.
- Before installing the fix pack on RHEL 4 on AMD64/EM64T, RHEL 4 on System p™, or SUSE Linux Enterprise Server 9 on AMD64/EM64T computers, ensure that you have installed the required libraries. See the footnotes in Table 4 on page 5 for details.

Notes regarding rule bases

When you choose the installation option whereby the installer automatically updates the rule base, 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 IBM 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 IBM 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 IBM Tivoli Enterprise Console server to make the targeted rule base current.

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

- For Windows environments, issue this command:

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

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

  `. /etc/Tivoli/setup_env.sh`

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

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

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

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

Be aware 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

If you are using the Windows operating system, you must account for the following issues:

- **Invoking the required "install" mode in Windows 2003 operating system:** Before you launch the Windows fix pack executable (**setupwin32fp6.exe**) on a Window 2003 computer, you must access a command-line interface and run the **change user /install** command. This command initializes the required "install" mode. After the installation, run the **change user /execute** command to return the computer to its previous mode.

  You must perform this action before performing any form of installation (wizard, command line, and so on). Otherwise, the fix pack executable does not properly recognize when a base IBM Tivoli Enterprise Console® Event Synchronization is installed. You see the following error message if ″install″ mode is not properly invoked:

```
Please read the information below.

Errors occurred during the installation.
- Unable to install IBM Tivoli Monitoring and Tivoli Enterprise Console Event
Synchronization Fix Pack 6: Patch is associated with a product that is not
installed on target machine.
```

You must cancel the installation, invoke ″install″ mode as described here, and then rerun the installation. After installation be sure to run the **change user /execute** command to return the computer to its previous mode.

- **Directory path for rule base files:** 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 file (**setupwin32fp6.exe**) 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 58
- “Installing from the command line using a silent installation” on page 60

Note: If you have IBM Tivoli Monitoring and IBM Tivoli Enterprise Console event synchronization installed on your computer already, first determine which version is installed (see Table 20 on page 55 for assistance). If the version installed is 1.0.0.6 (Fix Pack 6), you are at the current level. If the version installed is earlier than version 1.0.0.6, you can install the version that comes with Fix Pack 6.

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 **setupwin32fp6.exe** file in the temporary directory where you extracted the fix pack files.

   On Linux or UNIX computers, run the following command:

   ```
   setup<operating_system>fp6.bin
   ```

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

   ```
   setupAixfp6.bin
   ```

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

Table 21. Rule base options for IBM Tivoli Enterprise Console event synchronization

Option	Description
Automatically install rules and classes	The installation wizard prompts you for the rule base that contains the rule set and class files for event synchronization, and automatically execute the commands to perform updates in the rule base.

Table 21. Rule base options for IBM Tivoli Enterprise Console event synchronization (continued)

Option	Description
Manually install rules and classes	The installation wizard does not update any rule base containing event synchronization files. **IMPORTANT:** You are required to manually update the files in the rule base after the installation is complete. Refer to "Modifying your rule base after installation" on page 61.

5. If you selected the automatic update option, complete the following fields and click **Next**:

Table 22. Configuration fields IBM Tivoli Enterprise Console event synchronization

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.

6. Click **Next**.
7. Click **Next** on the preinstallation summary panel.

   The installation begins.
8. When the installation and configuration steps are finished, and if you selected the automatic update option, 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 must manually stop and restart your event server).

   Note: After you have completed fix pack installation of all components, you must stop and restart the event server for these changes to take effect.
9. 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:

   ```
   setupwin32fp6.exe -console
   ```

   On UNIX computers:

   ```
   setup<operating_system>fp6.bin -console
   ```

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

   ```
   setupAixfp6.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:

   ```
   [X] 1 - Automatically install rules and classes (recommended)
   [ ] 2 - Manually install rules and classes (advanced users)

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

6. Select one of the options (refer to Table 21 on page 57 for explanation of the options) and press Enter to continue.
   - If you chose the manual update option, skip to Step 10.
   - If you chose the automatic update option, the following prompt is displayed:

     ```
     Rule base Name []
     ```

7. 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 []
   ```

8. 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 []
   ```

9. 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]
   ```

10. 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]
    ```

11. 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]
    ```

12. 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]
```

13. Type 0 and press Enter to continue.

    The following prompt is displayed:

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

14. Type 3 to finish and press Enter.

Note: After you have completed fix pack installation of all components, 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:

   ```
   setupwin32fp6.exe -options-template filename
   ```

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

   On UNIX computers:

   ```
   setupoperating_systemfp6.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:

   ```
   setupAixfp6.bin -options-template filename
   ```

2. Edit the output file to specify the **rbInstallTypePanel.rbInstallType** variable. Refer to Table 21 on page 57 for an explanation of the options.
3. If you chose the automatic update option, edit the output file to specify the **rulebasePanel.rbName** variable. Define the name of a rule base that has IBM 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.

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

   On Windows computers:

   ```
   setupwin32fp6.exe -options filename -silent
   ```

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

   On UNIX computers:

   ```
   setup<operating_system>fp6.bin -options filename -silent
   ```

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

   ```
   setupAixfp6.bin -options filename -silent
   ```

Note: After you have completed fix pack installation of all components, you must stop and restart the event server for these changes to take effect. (The silent installation wizard can stop and restart the event server automatically, when you select the appropriate installation option.)

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%
```

Modifying your rule base after installation

With this fix pack, the installation wizard provides the option to have the installer automatically update the targeted rule base, or allow the user to manually perform the rule base modification steps after installation is complete.

If the option is chosen to manually perform the rule base modification steps after installation is complete, the necessary files are copied to:

- **On Windows computers:** `%BINDIR%\TME\TEC\OM_TEC\rules`
- **On UNIX computers:** `$BINDIR/TME/TEC/OM_TEC/rules`

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

- For Windows environments, issue this command:

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

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

  `. /etc/Tivoli/setup_env.sh`

Copy **omegamon.rls** from **OM_TEC/rules** to the **TEC_RULES** directory of the rule base. If you have made changes to this file, make sure to back up the changes and merge them into the new **omegamon.rls** file.

Copy **Sentry.baroc** and **omegamon.baroc** from **OM_TEC/rules** to the **TEC_CLASSES** directory of the rule base. If you have made changes to these files, back up the changes and merge them into the new **Sentry.baroc** and **omegamon.baroc** files.

Use the **wrb –comprules** *rule_base_name* command from a bash command prompt (on Windows systems) or command prompt (on UNIX systems) to compile the targeted 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 the rule base.

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

Closing sampled events in IBM Tivoli Enterprise Console

When a situation event is forwarded to IBM Tivoli Enterprise Console that is associated to a *sampled* situation and that event is subsequently closed in the event server, the behavior of event synchronization

is to send a request to IBM Tivoli Monitoring to acknowledge the situation with a specified timeout. The timeout is required because of problems with the situation triggering again after the close in IBM Tivoli Monitoring.

If the acknowledgement of the situation expires, and the situation is still true, then a new situation event is opened in IBM Tivoli Enterprise Console. If the situation becomes false, then it resets itself in IBM Tivoli Monitoring, and the event remains closed in IBM Tivoli Enterprise Console.

The default acknowledgement expiration time is 59 minutes. However this can be changed in the configuration file for situation timeouts on the event server (**sit_timeouts.conf**). Also, you can set an expiration time in this file for specific situations. The format for defining an expiration time for a single situation is as follows:

```
situation_name=expire_time
```

where *situation_name* is the actual name of the situation in IBM Tivoli Monitoring V6.1, and *expire_time* is the expiration time for acknowledgement, in minutes. After you edit this file, the new expiration times can be dynamically loaded into the IBM Tivoli Enterprise Console rule base using the **sitconfig.sh refresh** command in `$BINDIR/TME/TEC/OM_TEC/bin`.

Verifying the installation of the event synchronization fix pack

To verify that the IBM Tivoli Monitoring and IBM Tivoli Enterprise Console fix pack has been successfully installed, perform the operations listed in Table 20 on page 55. according to the operating system of the computer where your event server is running.

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 only the event synchronization fix pack. If you use these steps, you uninstall the entire event synchronization package from your event server.

1. (*Windows 2003 only*) Access a command-line interface and run the **change user /install** command. This command initializes the required “install” mode.

   You must perform this action before performing any form of uninstallation (wizard, command line, and so on). Otherwise, the uninstallation program does not properly register your action. Specifically, an entry in the **vpd.properties** file is not removed, and this entry causes subsequent installations of event synchronization to fail.
2. Before you use any of the commands, source the Tivoli environment as follows:
   - For Windows environments, issue this command:

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

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

     `. /etc/Tivoli/setup_env.sh`
3. 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`
4. Follow the prompts in the uninstallation program.
5. (*Windows 2003 only*) After the uninstallation is complete, access a command line interface and run the **changer user /execute** command. This command returns the computer to the previous execute mode.

You can also run perform an uninstallation in silent mode (by running the command 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 **_uninst***X*, 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 correctly uninstalls the product.

Chapter 4. After you finish installing the fix pack

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

Clearing the Tivoli Enterprise Portal browser cache

On systems running the Tivoli Enterprise Portal browser client, clear the browser cache to avoid inconsistent display.

1. From the Windows **Start** button, select **Control Panel**.
2. Double-click the **IBM Control Panel for Java** icon to display the Java Plug-In Control Panel.
3. Select the **Cache** tab.
4. Click the **Clear** button and click **Apply**.
5. To improve performance in most environments, set the **Size** to **Unlimited**.
6. If you changed the size of the cache, click the **Apply** button.
7. Close the Java Plug-In Control Panel.
8. Stop and restart your browser.

Determining what components were installed

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

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

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

Issue: You must install Global Services Kit (GSKit) from a user ID with root or administrator authority. If you are running the installer program interactively as non-root, the installer prompts you for the root password. If you do not supply the root password when prompted or if you supply an incorrect password, the installation fails.

Solution: First install GSKit manually, using a user ID that has **root** or **Administrator** authority. Then run the installer program to complete installation of other components.

Note: This solution also applies if you perform a silent installation with a non-root user account. In this case, the prompt for the root password is bypassed, and you must install GSKit manually.

Securing your Linux or UNIX IBM Tivoli Monitoring installation

Note: This section describes the basic functions and enhancements for the **secureMain** command. This information can be repeated in future versions of the *IBM Tivoli Monitoring Installation and Setup Guide*.

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

© Copyright IBM Corp. 2007

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.

secureMain

This topic describes the **secureMain** set of scripts. You use these scripts to modify permissions in IBM Tivoli Monitoring, version 6.x

The product installation process creates the majority of directories and files with **world write** permissions. This configuration creates a security situation that is not acceptable in many enterprises. **secureMain** helps you bring the monitoring environment into compliance with the security standards of your company.

Usage

This section describes the usage for **secureMain** commands.

```
secureMain [-h itm_home] [-g common_group] [-t type_code [-t type_code]] lock
secureMain [-h itm_home] [-g common_group] unlock
```

where variables are defined as follows:

- **itm_home** is the directory path for the IBM Tivoli Monitoring installation. If this parameter is not supplied, the script attempts to determine the installation directory.
- **common_group** is a group ID common to all of the user IDs that are used to run components in this installation. The user ID that is used to perform the installation must also be a member of the group ID specified. The only exception is that the **root** ID is not required to be a member of the group ID specified.
- **type_code** is a component code belonging to an installed component. You can specify multiple **-t** options to create a list of component codes to be processed.

If you invoke the **secureMain** command with no parameters, the usage text is displayed.

The **secureMain lock** command is used to tighten permissions in an IBM Tivoli Monitoring 6.1 installation. It should be run after installing or configuring components.

When the **secureMain lock** command is invoked with no other parameters, the permissions are tightened generally to 755. However, a number of directories and some files remain with **world write** permissions. When certain components that are commonly run using multiple user IDs are present in the installation, many more files have **world write** permissions.

When the **secureMain lock** command is invoked with the **-g common_group** parameter, the permissions are tightened generally to 775 and the directories and files have their group owner changed to **common_group** specified. There are no directories or files remaining that have **world write** permissions. Even when certain components that are commonly run using multiple user IDs are present in the installation, no files will have **world write** permissions. Additionally, the **common_group** value specified is written to a file and is used for all future **secureMain lock** invocations in this installation, unless the **-g** option is specified and the **common_group** is different from the previous value.

When the **secureMain lock** command is invoked with the **-t** *type_code* parameter, sections of the installation might be skipped when tightening permissions. Common directories, like `bin`, `config`, `registry`, and `logs`, and the files in them are always processed. Only directories and files specific to the specified **type_code** components are processed. The other component directory trees are skipped.

The **secureMain unlock** command is used to loosen permissions in an IBM Tivoli Monitoring 6.1 installation. The **secureMain unlock** command is typically not necessary, but can be run if desired. Run the command before installing or configuring components.

The **secureMain unlock** command does not return the installation to the permission state that it was in before running the **secureMain lock** command. It processes only the common directories, like `bin`, `config`, `registry`, and `logs`, and the files in them.

Examples

The following example locks the installation using the **itmgroup** common group:

```
secureMain -g itmgroup lock
```

The following example locks the base and `mq` component directories using the common group **itmgroup**:

```
secureMain -g itmgroup -t mq lock
```

Scenario with secureMain

The following scenario illustrates the use of the **secureMain** command:

1. Complete the following operations using **root** authorization:
   a. Install OS Agent.
   b. Configure OS Agent.
   c. List files with **world write** permissions, using the following command: `find . -perm -o+w -ls`
   d. Run the following command: `secureMain -g itmgroup -t ux lock`
   e. Install 32-bit Enterprise Svcs UI to get 32-bit Framework.
   f. Install MQ Agent.
   g. Run the following command: `secureMain -g itmgroup -t mq lock`
   h. List files with **world write** permissions, using the following command: `find . -perm -o+w -ls`
   i. Start OS Agent.
2. Complete the following operations using **mquser** authorization:
   a. Start MQ Agent for a queue manager.
   b. Start MQ Agent for a second queue manager.
   c. Stop MQ Agent for the first queue manager.
   d. Stop MQ Agent for the second queue manager.
3. Complete the following operations using **root** authorization:
   a. Stop OS Agent.
   b. List files with **world write** permissions, using the following command: `find . -perm -o+w -ls`

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 6, the upgrade toolkit upgrades to the Fix Pack 6 version of the agents.

For Fix Pack 6, you must use the following command to install support for Solaris computers:

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

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

Installing Java Web Start

The Java Web Start application lets you launch the Tivoli Enterprise Portal desktop client application without having to explicitly install the IBM Tivoli Monitoring version 6.1 installer on each system where you want to run the desktop client. After installing Java Web Start, you no longer have to manually update each Tivoli Enterprise Portal desktop client installation when you install additional support or products to the Tivoli Enterprise Portal Server because each Java Web Start client automatically downloads any new jar files and resources. The files to enable this application include a text file, a utility jar file, template JNLP file, and a digitally signed version of jsafe.zip (required if you are integrated with IBM Tivoli Enterprise Console) and can be downloaded from the OPAL Web site: http://www-18.lotus.com/wps/portal/topal.

Installing upgrades to monitoring agents

In an effort to improve quality within the OMEGAMON portfolio, IBM has provided additional focus on verification of OMEGAMON XE products and components running with IBM Tivoli Monitoring version 6.1 Fix Pack 6. Refer to the Planning Upgrades section of the following Web site for OMEGAMON XE maintenance levels **http://www-306.ibm.com/software/sysmgmt/products/support/IBMTivoliMonitoringV6.html**.

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

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

Understanding deployment options

For additional information about deployment issues, refer to the *IBM Tivoli Monitoring V6.1 Deployment Guide* found at the following URL in the Tivoli Open Process Automation Library (OPAL) Web site: http://www.ibm.com/software/tivoli/opal/?NavCode=1TW10TM4J.

Tivoli Widget Sample Utility

The Tivoli Widget Sample Utility is a Microsoft Windows tray application that provides a means to manage widgets on the desktop to display IBM Tivoli Monitoring data. It is a lightweight sample utility for viewing specific monitoring information in cases where an entire TEP Console installation might not be required. It also provides secure e-mail delivery mechanism to deploy widgets that have been configured for specific monitoring/display of data by a customer IT organization to its client work stations. Be aware that the Tivoli Widget Engine is a sample utility provided as-is.

The Tivoli Widget Sample README and Installation Instructions is found on the IBM Tivoli Monitoring Windows media.

IBM Tivoli Open Process Automation Library (OPAL)

The IBM Tivoli Open Process Automation Library (OPAL) is an online community of IBM and non-IBM developers. The library provides downloadable integrated extensions for IBM service management applications. The items in the library are provided by many parties, including IBM. See the following Web site: http://www-18.lotus.com/wps/portal/topal

Note: Each item in OPAL has an applicable end user license agreement that describes the terms and conditions under which a specific item might be used.

Chapter 5. Known limitations and workarounds

The following sections identify limitations that you might encounter during the use of this fix pack. Where available, workaround solutions are provided for the problems.

- "General installation and configuration issues"
  - "Installation"
  - "Configuration" on page 74
  - "IBM Tivoli Enterprise Console installation and configuration" on page 75
  - "Documentation of installation and configuration" on page 76
- "Remote deployment issues" on page 82
- "Tivoli Enterprise Monitoring Agent" on page 84
- "Tivoli Enterprise Monitoring Server" on page 85
  - "Tivoli Enterprise Monitoring Server on distributed platforms issues" on page 86
  - "Tivoli Enterprise Monitoring Server on z/OS systems issues" on page 89
- "Tivoli Enterprise Portal desktop and browser clients" on page 92
- "Tivoli Enterprise Portal Server" on page 93
- "Historical data collection issues" on page 97
  - "Summarization and Pruning Agent" on page 99
  - "Warehouse Proxy Agent" on page 101
- "Tivoli Universal Agent issues" on page 102
- "Globalization" on page 103
- "Online help" on page 104

APARs that require renewal of workarounds

The following APARs have workarounds that existed prior to Fix Pack 6, but have not been included in Fix Pack 6. After you install Fix Pack 6, you must reapply the workarounds. Contact IBM Software Support if your require assistance in reapplying the workarounds.

```
IY93196    ATTEMPTS TO START TEMS WHILE CMS PROCESS RUNNING CORRUPTS QA1
IY96372    UX AGENT RESTART FAILS. SU NOT IN PATH FOR INIT.D PROCESSES
IY97904    UPDATEAUTORUN.SH NEEDS TO HANDLE S390 MODE
IY97997    TEMS CONFIGURATION CREATES KSHXHUBS.XML FILE IN WRONG DIRECTORY
IZ00670    REMOVE SUPERFLOUS TACMD LOGGING FROM DYNARCH.SHL
IZ00676    ORACLE/SYBASE AGENTS NOT RESTARTING ON REBOOT.
IZ00684    CINFO -R OUTPUT WRONG WHEN LONG HOST IS IN RUNINFO
IZ03924    CANDLEAGENT KILLS NON-ITM PROCESSES IF RUNINFO PIDS ARE REUSED.
IZ04643    A SUBORDINATE PROCESSES LEFT IN RUNINFO AFTER UA SHUTDOWN
```

General installation and configuration issues

These limitations and workarounds are related to installation and configuration and include the following subsections:

- "Installation"
- "Configuration" on page 74
- "IBM Tivoli Enterprise Console installation and configuration" on page 75
- "Documentation of installation and configuration" on page 76

Installation

These limitations and workarounds are related to installation:

© Copyright IBM Corp. 2007

- **Limitation on UNIX-based and z/OS-based operating systems:** When you install application support for ITM 6.1, the installer does not account for case differences (uppercase and lowercase). In some cases, new, required files that the installer provides do not overwrite old files, because of case differences. As a result, the Tivoli Enterprise Monitoring Server might not detect and load the new file. For example, the installer might provide a new file kip.sql. If the old file that the installer must replace is named KIP.SQL, both files (kip.sql and KIP.SQL) exist on the computer after installation. OMEGAMON XE on z/OS, Version 3.1.0, and OMEGAMON XE for Mainframe Networks, Version 3.1.0, are among the products known to be affected by this limitation.

  Workaround: Prior to installing the IBM Tivoli Monitoring Fix Pack 4 and all subsequent IBM Tivoli Monitoring Fix Packs, you must perform these steps:

  1. Look for all **Kpp.ATR** and **Kpp.CAT** files (the installer only moves lowercase files to the upgraded Tivoli Enterprise Monitoring Server directory.)
  2. From the IBM Tivoli Monitoring home directory enter the following commands:

     ```
     find . -name "*.ATR"
     find . -name "*.CAT"
     ```
  3. Rename all occurrences of ***.ATR** and ***.CAT** (uppercase) found to ***.atr** and ***.cat** (lowercase).
  4. List all ***.cat** and ***.atr** files. The Fix Pack 6 upgrade only moves lowercase ***.cat** and ***.atr** files. Look for any ***.cat** and ***.atr** filenames that are mixed or uppercase; rename them to lower case.

     ```
     find . -name "*.ATR"
     find . -name "*.CAT"
     ```
  5. Install the Fix Pack 6.
- **Limitation:** After you upgrade the hub monitoring server to Fix Pack 6 a remote monitoring server is functioning normally, however, the icon for the server in the Tivoli Enterprise Portal is dimmed and the resource seems to be unavailable. The following RAS1 log message is a typical symptom of this problem:

  ```
  Endpoint unavailable: "ip.pipe:#9.99.999.99:1918", 1DE00006, 0
  ```

  Workaround: Add **KDS_NDSLISTEN=256** to **KBBENV** of the Tivoli Enterprise Monitoring Server to which these timeouts are reported. Be aware that the time on all systems must be time synchronized so that the heartbeat function works correctly.
- **Limitation:** The **-D** flags in a **cnp.sh** file are not preserved during an upgrade.

  Workaround: Reapply **-D** flags in the **cnp.sh** file in the upgraded environment. The **cnp.sh** file is located in the following path: *itm_home*/bin.
- **Limitation:** Custom settings that you applied to the **lnxenv** file are not preserved during an upgrade.

  Workaround: Choose one of the following solutions:

  – Copy the customized version of the **lnxenv** file to a temporary destination and restore after upgrade.

    OR

  – Reapply custom configuration to the **lnxenv** file in the upgraded environment.

  The file is located in the following path: *itm_home*/*architecture_identifier*/cq/bin.
- **Ensuring success of Java Runtime Environment (JRE) upgrades on Windows:** On Windows, to avoid JRE upgrade problems during install or upgrade to this fix pack, before launching the installation wizard or starting a silent install, you must first stop all applications that are using the JRE, so that the JRE is not busy and can be upgraded. The JRE is currently being used when there are running processes named **java.exe** or **javaw.exe**. Running processes are displayed in the Windows Task Manager.

  Workaround: If the fix pack install or upgrade hangs or terminates (and user interface panels disappear) during the upgrade of Java, restart the machine then start the fix pack installation again. Use the following information to further diagnose this Java JRE upgrade problem:

  – Search the Windows Registry for **HKLM\System\Control\Session Manager** and examine the values of the **PendingFileRenameOperations** variable name to see whether any pending renames are within the Java Home directory.

  - The default value for Java Home is **C:\Program Files\IBM\Java142\jre** and renaming during JRE upgrades typically occur in the **bin** or **lib** directories.
- **Limitation regarding the korn shell of newer Linux operating systems:** Upgrades fail for IBM Tivoli Monitoring components on the following Linux operating systems:
  - SUSE Linux Enterprise 10 (SLES 10)
  - RedHat Enterprise Linux 5 (RHEL 5)

  This problem is related to the implementation of the korn shell in those releases. You can replace the default korn shell with the korn shell used in the previous release, SLES 9 and RHEL 4 respectively. The previous shell is distributed in the **pdksh** package. You must perform a forced installation of the package, using the **force** option and the **nodeps** (no dependency) option. The following is an example command that installs the package on SLES10.

  ```
  rpm -Uhv pdksh-5.2.14-780.7.s390x.rpm --force --nodeps
  ```

  Note: If you wrote scripts in the korn shell for a SLES 10 or RHEL 5 operating system, moving to the older korn shell might affect those scripts.
- The Tivoli Enterprise Portal Server fails to run when Version 7.04.11 of Global Security Kit (GSKit) is installed. A version of GSKit must be available to enable the portal server. However, GSKit V7.04.11 is not currently recognized by IBM Tivoli Monitoring. You must install one of the valid versions of GSKit that are listed in the installation and setup guide, but you must be sure not to install Version 7.04.11. For example, you can install the version of GSKit that comes with IBM Tivoli Monitoring.
- During installation of a fix pack, you must not rename the directories of the depot of installation images. Otherwise, the commands you use to install new components fail and generate Java exceptions. These exceptions occur because the installer fails to find an installation package in a directory that has the expected naming convention.

  After your create a depot for agent deployment, you must not modify the directory structure of the depot:
  - Do not rename the directories in the depot where the installation images are located.
  - Do not create additional subdirectories

  The location of the depot directory in the monitoring server is as follows:
  - On Windows, the depot directory is *itm_home*\CMS\Depot.
  - On UNIX and Linux systems, the depot is *itm_home*/tables/TEMSServer_ms_TEMSName/depot.

  If you rename directories or store backup versions of directories in the depot, the commands you use to deploy agents fail and generate Java exceptions. These exceptions occur because agent deployment code expects the directory tree to conform to a specific naming convention. Also the deployment code parses the directory structure for the newest numeric versions of components. If the code encounters non-numeric data, a Java process error is generated, for example, “can’t find suitable install package”.
- **Issue:** After you perform a silent installation of IBM Tivoli Monitoring on the zLinux operating system, the Workflow icon is greyed out in the toolbar of the Tivoli Enterprise Portal and the Workflow tool is not available. **Workaround:** Run the installation again, using the standard **install.sh** script, instead of silent installation. You must select the **9) Tivoli Enterprise Portal Server support** option during the installation process.
- If you upgrade Java, the installation program performs the upgrades and then ends without displaying any confirmation message. You must restart the component on which you installed the Java upgrade for the upgrade to take effect.
- Names for monitoring servers must be between 2 and 32 characters in length. For more information about naming conventions, refer to the *IBM Tivoli Monitoring: Installation and Setup Guide*.
- If you are performing a silent installation of application support on a zLinux system and you specify `ComponentSelectionPanel.tepdSelected="true"` in the **response.txt** file without having the desktop client installed, the installation program exits with an error that indicates the entire operation failed when actually only the desktop client portion failed.

To recover from this situation, rerun the silent installation and specify `ComponentSelectionPanel.tepdSelected="false"`.

- Fix pack installation fails on AIX V5.3 computers with file set **xlC.aix50.rte** at level 8.0.0.3.

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

Configuration

These limitations and workarounds are related to configuration:

- APAR IY93070 is introducing a new error message that is displayed in a Tivoli Enterprise Portal Server workspace data view when a query is sent to more than 200 managed systems.

  ```
  KFWITM217E Request error: Request to xxx nodes exceeds the limit of 200.
  Please specify a smaller distribution or increase the maximum.
  ```

  APAR IY93070 sets a default limit of 200 nodes for any single query for a workspace view. If the following conditions exist in the query for a workspace view, you must increase the **KFW_REPORT_NODE_LIMIT** environment variable for the Tivoli Enterprise Portal server environment variable as described below:

  – The query is assigned to a managed system list that contains more than 200 managed systems.

    OR

  – More than 200 managed systems are explicitly assigned to a query in any workspace view.

  Under these conditions, you must increase the following Tivoli Enterprise Portal server environment variable.

  `KFW_REPORT_NODE_LIMIT=`*`xxx`*

  where *xxx* is an integer that is equal to or greater than one of the following:

  – The number of managed systems defined in a managed system list.

    OR

  – Explicitly assigned to a query over 200 in a Tivoli Enterprise Portal workspace view.

  You must add the **KFW_REPORT_NODE_LIMIT** environment variable (or remove the comment marker (#) from the variable) in the following Tivoli Enterprise Portal Server environment files, and restart the portal server.

  – Windows systems: `\ibm\itm\cnps\kfwenv`

  – Linux or AIX systems: `/opt/IBM/config/cq.ini`

  After you change the **KFW_REPORT_NODE_LIMIT** variable, you might receive the following error:

  ```
  KFWITM217E Request error: SQL1_CreateAccessPlan failed, rc=1.
  ```

  Typically this problem is caused when too many explicitly defined managed systems are assigned to a query for a workspace view. The best practice for resolving this problem is as follows:

  1. Create a managed system list that specifies the explicitly defined managed systems.
  2. Remove the explicit assignments from the query.
  3. Assign the managed system list to the query.

  Alternatively, you can reduce the number of managed systems that you explicitly define in the query.

- **Custom settings for hot standby not preserved: Context:** On Linux and UNIX, a hub Tivoli Enterprise Monitoring Server can be configured to failover to a hot standby hub monitoring server, and a remote monitoring server can be configured to redirect to a hot standby hub monitoring server on failure of the primary hub monitoring server.

  Issue: If the hot standby monitoring server is configured with system name or IP address, and your goal is to unconfigure the hot standby, you must enter 'none' as the value during monitoring server reconfiguration.

- **Issue:** If you are upgrading to Fix Pack 6 from Fix Pack 4 or 5, specific custom settings that you might have made are not preserved. The specific settings, if any, and the affected *.ini files are as follows:
  - The **KBB_RAS1** setting for these *.ini files: hd.ini (Warehouse Proxy Agent), lz.ini (Linux OS AGent) ,ms.ini (monitoring server), ul.ini (UNIX Log Alert Agent), um.ini (Tivoli Universal Agent)
  - The **LOGSHOME** value in cj.ini (portal desktop client) and cq.ini (portal server)

  Workaround: You must manually restore the settings that you applied.
- **Hot standby with the Windows OS Agent:** As explained in APAR IY99214, if the NT Agent is configured with multiple protocols in a hot standby environment, applying Fix Pack 4, 5, or 6 could lead to a corrupt configuration with incorrect host names and ports. **Workaround:** Log on to the remote computer and use Manage Tivoli Monitoring Services to reconfigure the agent and correct the host names and ports where they have become corrupt.
- While you are configuring the Tivoli Enterprise Portal, you must enter a database user ID for the Tivoli Enterprise Portal Server database. On UNIX and Linux computers, you must not use the ID of the DB2 instance (for example, **db2inst1**) as the TEPS database user ID.

  If you use the DB2 instance ID, configuration of the Tivoli Enterprise Portal Server fails with an error that is similar to the following, "Cannot assign database control to *userid*." You then must run the configuration again, and provide a different value for the database user ID.
- **Selecting port numbers:** In a large monitoring environment, you need to generate sets of unique port numbers, because you cannot use the default port numbers repeatedly. System administrators typically use a formula to generate multiple unique numbers. However, a port conflict results if you use the following formula to generate a unique port number: **1918 + 4096(x)**, where x={1, 2, ..., 15}. On z/OS operating systems, the resulting port numbers cause the remote Tivoli Enterprise Monitoring Server on the z/OS operating system to start improperly. As a result, the agents cannot connect. This formula is also incorrect for distributed systems, although the specific error symptoms can vary. You must use an alternate method or formula to generate unique port numbers.
- On Windows, when the computer workload is so great that the Windows service cannot log its status, you see a message similar to the following:

  ```
  " (Friday, September 28, 2007, 05:04:47-{AE4}khdxsrvc.cpp,326,"serviceHandler") Service Interrogated!"
  ```

  You can ignore this service interrogation message. It reflects a temporary condition that resolves itself automatically.

IBM Tivoli Enterprise Console installation and configuration

These limitations and workarounds are related to documentation of the installation and configuration of IBM Tivoli Enterprise Console:

- **Limitation:** A problem can arise in the following context: Tivoli Enterprise Console integration is enabled on a hub monitoring server and Tivoli Enterprise Console event synchronization installed and configured on a TEC server. In this context, when you remove the acknowledgement for a pure situation, the associated event update forwarded to your TEC server results in the generation of an extraneous **TEC_ITM_OM_Situation_Sync_Error** event.

  Workaround: You can ignore this error event. The original event forwarded to your TEC server is correctly reopened.
- **Problem**: You might experience a problem when you use Fix Pack 6 to upgrade a hub Tivoli Enterprise Monitoring Server for which IBM Tivoli Enterprise Console (TEC) Integration is enabled. Custom configurations that you made to any Event Integration Facility (EIF) configuration file for an alternate destination TEC server might be deleted in error. This problem arises because the associated configuration file is deleted during an upgrade in some cases. The EIF configuration file (**om_tec.config**) for the default TEC server is not affected and all custom configurations are preserved in an upgrade.

  EIF configuration files are created for an alternate destination TEC server when a destination TEC server is specified in the **tecserver.txt** file and the hub Tivoli Enterprise Monitoring Server is restarted. The file is located as follows:

– **On UNIX and Linux systems:** *itm_home*/tables/*temsname*/TECLIB
– **On Windows systems:** *itm_home*\cms\TECLIB

You see the following message when this problem occurs:

```
cp: /opt/IBM/ITM/tables/temsname_old/TECLIB/directory is a directory (not copied).
 ERROR _ could not copy directory
```

where *temsname* is the name of the hub monitoring server and *directory* is any directory name.

Workaround: Choose one of the following solutions:

– Copy the EIF configuration files for the alternate destination TEC servers to a temporary destination and restore them to **TECLIB** after upgrade.

OR

– Reapply custom configurations to the configuration files when they are regenerated.

– **Issue:** You might encounter a problem with a configuration file after you perform a *second* silent installation (uninstallation and then reinstallation) of event synchronization for IBM Tivoli Enterprise Console. Specifically, the configuration file for situation timeouts (**sit_timeouts.conf**) is not recreated.
Workaround: You can manually create this file as follows:

1. Navigate to the **OM_TEC** directory of your installation of event synchronization on the IBM Tivoli Enterprise Console server:
   - **On Windows:** \Program Files\TME\TEC\OM_TEC\etc
   - **On UNIX and Linux:** /etc/TME/TEC/OM_TEC
2. Create a **sit_timeouts.conf** text file with the following content:

   ```
   DEFAULT_SIT_EXPIRE_TIME=59
   ```

"Closing sampled events in IBM Tivoli Enterprise Console" on page 61 provides more information on the **sit_timeouts.conf** file. Be aware that you can further modify this file to specify expiration timeouts for individual situation names. After you edit this file, the new expiration times can be dynamically loaded into the IBM Tivoli Enterprise Console rule base using the **sitconfig.sh refresh** command in $BINDIR/TME/TEC/OM_TEC/bin.

Documentation of installation and configuration

These limitations and workarounds are related to documentation of installation and configuration:

- The *IBM Tivoli Monitoring Command Reference* contains an incomplete description of the **tacmd createSit** command. This command also provides a **SitInfo** property:

  SitInfo

  Holds the EIF data for IBM Tivoli Enterprise Console. **SitInfo** is all or any one of the following separated by a semicolon (;). The **SitInfo** parameters must be enclosed in double quotes.

  – **Sev=***severity* can take values Critical or Warning or Minor or Harmless or Unknown.
  – **TFWD=[Y|N]**
  – **TDST=***n***1[,***n***2...,***n***5] TDST** can take up to five valid IBM Tivoli Enterprise Console destination server IDs. To find valid server IDs use the **tacmd listeventdest** command.

  ```
  -p SitInfo="SEV=Critical;TFWD=Y;TDST=100"
  ```

- Regarding APAR IY94954, confusing text was removed from sections regarding planning and pre-installation in the readme for Fix Pack 2. Clarification of many installation points has been added. Also, the installation methodology has been made consistent with the installation methodology for the basic product. This consistency has been achieved by use of an installation wizard instead of an approach based in the command-line interface. See "(*If you installed Fix Pack 3 or earlier*) Comparison of installation processes for former fix packs versus recent fix packs" on page 81 for a description of these changes.
- **Documenting how to set trace levels dynamically:** Information on this topic is provided in several of the problem determination guides for monitoring agents: "Setting trace levels dynamically using IBM

Tivoli Monitoring Service Console", For example, see http://publib.boulder.ibm.com/infocenter/tivihelp/v15r1/topic/com.ibm.omegamon.mn.doc/sc32-1926-00100.htm#rastrace.

This topic can be added to future editions of the basic *IBM Tivoli Monitoring Problem Determination Guide* because it applies to the product in general. The information can be augmented with the following instructions:

Disabling trace logging dynamically

Advanced users of IBM Tivoli Monitoring access the IBM Tivoli Monitoring Service Console to enable trace logging dynamically. A key benefit of this approach is as follows: When you set trace logging dynamically, your new settings take effect without a recycling of the Tivoli Enterprise Monitoring Server. The following instructions describe how to disable the settings that you apply.

Consider a scenario in which you apply the following setting for trace logging in the IBM Tivoli Monitoring Service Console: **KBB_RAS1=ERROR (UNIT:KRA ST ERR)**

This setting activates the following types of trace logging:

- **ERROR:** minimal trace logging for the IBM Tivoli Monitoring environment. This setting is the default level of tracing in IBM Tivoli Monitoring.
- **(UNIT:KRA ST ERR):** trace logging for requests to and answers from the Tivoli Enterprise Monitoring Server. The unit values **ST** and **ERR** indicate that you will be collecting state and error information for the agent framework component (**KRA**). This specification captures all rows of agent data that have passed filtering, including attribute names and values, request names, table names, and collection interval.

  Note: You might assume that you can disable the preceding setting by passing the general **KBB_RAS1=ERROR** setting (without a **UNIT** specified). This assumption is not correct because the general setting does not override any previous **UNIT** level settings. Instead you must use the following procedure.

To disable a setting for **UNIT** trace logging dynamically, you must explicitly reset that **UNIT** to the **ANY** value. For example, you can use the **KBB_RAS1=ERROR (UNIT:KRA ANY)** specification to reset the **KBB_RAS1=ERROR (UNIT:KRA ST ERR)** trace setting.

You can apply this specification dynamically by issuing the following command from the IBM Tivoli Monitoring Service Console:

```
RAS1 set ERROR (UNIT:KRA ANY)
```

- This item results from APAR IY94388. The tool used for license acceptance on the UNIX and Linux operating systems has changed. The new version of the tool eliminates some prompts during a command-line installation. The new version of the tool also uses the system NLS settings to automatically determine the language for license display. The new version has no impact for silent installations or remote deployment installations.

  Instructions like the following should be replaced in the installation guide:

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

  The following instruction should replace the preceding instructions:

  5. Type 1 to accept the agreement and press Enter.
- Current® documentation of the upgrade process for the OMEGAMON XE on z/OS monitoring agent needs to be updated. Specifically, *OMEGAMON XE on z/OS Planning and Configuration Guide, V4.1.0* needs to contain the information that is presented in "Sequencing the upgrade procedures" on page 12.
- Do not install and run IBM Tivoli Monitoring version 6.1 components (for example, the Tivoli Enterprise Monitoring Server or monitoring agents) using the same names as other IBM Tivoli Monitoring

components. This caution applies to releases of IBM Tivoli Monitoring version 350/360 and version 6.1 both to the Tivoli Enterprise Monitoring Server and monitoring agent components. This information originates from APAR OA18616.

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

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

Or in this example, if the test agent is reconfigured to point to a production Tivoli Enterprise Monitoring Server while the production agent was also running, problems with the monitoring server might occur. For example, a UNIX server named host01 is running a test agent named host01:KUX and a production agent also named host01:KUX. Each agent is configured to connect to its test or production Tivoli Enterprise Monitoring Server, RTEMS_TEST01 and RTEMS_PROD01 respectively. Test agent host01:KUX is mistakenly reconfigured to connect to a production Tivoli Enterprise Monitoring Server named RTEMS_PROD02 while the production agent host01:KUX is still running. The result is a situation where Tivoli Enterprise Monitoring Server issues can occur because there is more than one agent with the same name, each reporting through a different production monitoring server.

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

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

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

- This item addresses APAR IZ00597. The documentation needs to be augmented with description of the **secureMain** set of scripts that come with the product. The section “secureMain” on page 66 provides the description to be added to the next revision of the documentation. This information, and the entire section in which it is located (“Securing your Linux or UNIX IBM Tivoli Monitoring installation” on page 65) belongs in the *IBM Tivoli Monitoring Installation and Setup Guide*.
- **Ensuring display of historical data in the Tivoli Enterprise Portal:** Regarding APAR IY98582, the documentation of installation needs to be clarified as follows:

  Summary of the problem

  Data exists in the warehouse database. However, the graphical user interface of the Tivoli Enterprise Portal cannot display the data. This problem arises due to a problem with configuration.

  Location of the problem in the documentation

  The problem in the documentation is located in Chapter 6, ″Installing IBM Tivoli Monitoring″ of the *IBM Tivoli Monitoring Installation and Setup Guide* (Revised April 2007), GC32-9407-00. The document is located at the following URL: http://publib.boulder.ibm.com/infocenter/tivihelp/v15r1/index.jsp?toc=/com.ibm.itm.doc/toc.xml Specifically, Steps 22, 23, and 24 of the ″Windows: Installing the portal server″ procedure must be updated as described below.

  Updated content to fix the problem in the documentation

  The following replacement content helps the user avoid the problem in the portal of data not being displayed. Replace Step 22b and 23b with the content in the following box (the first sentence remains unchanged from the original procedure):

b. Gather the following information: data source name, database name, database administrator ID and password, warehouse user ID and password.
Note: The ID/password pair that you provide for the warehouse user must be the values that you declared in the configuration panel of the Warehouse Proxy Agent. That user ID becomes a prefix for the names of all tables that are created in the warehouse database. The Tivoli Enterprise Portal must find tables with this prefix in their name. If you declare a different user name now, the portal cannot find and display the historical data that is contained in the tables.

Replace Step 24b with the following content in the following box (the first sentence remains unchanged from the original procedure):

b. Gather the following information: the data source name, and the warehouse user ID and password.
Note: The ID/password pair that you provide for the warehouse user must be the values that you declared in the configuration panel of the Warehouse Proxy Agent. That user ID becomes a prefix for the names of all tables that are created in the warehouse database. The Tivoli Enterprise Portal must find tables with this prefix in their name. If you declare a different user name now, the portal cannot find and display the historical data that is contained in the tables.

- **Setting traces:** The following items provide previous missing information for the ″Setting traces″ section of the *IBM Tivoli Monitoring Problem Determination Guide*. The items are intended to completely replace the existing sections, which have the following headings.
  - Setting the trace option for the Tivoli Enterprise Portal Server trace
  - Setting the trace option for the Tivoli Enterprise Monitoring Server trace
  - Setting the trace option for the Agent Deploy tool

  You use trace parameters to configure trace logging in IBM Tivoli Monitoring. The following sections provide suggested trace parameters that increase the amount of trace log information that you gather.

  Note: When you set a high level of tracing, trace log files grow large quickly. Monitor the size of log files when you run the system with high levels of tracing. Otherwise, the log files can require an excessive amount of hard disk space.

  For more information about setting traces, see the *IBM Tivoli Monitoring: Problem Determination Guide*.

Alternative way to set tracing on Windows

On Windows, the Trace Parameters dialog box provides an alternative to manually edit the parameter file as described in this section. You access the dialog box as follows:

1. In the Manage Tivoli Monitoring Services window, right-click the row for a component to access the pop-up menu. For example, you can right-click the **Tivoli Enterprise Monitoring Server** row.
2. Select **Advanced > Edit Trace Parms**.
3. Select the tracing option that you want in the **Enter RAS1 Filters** pull-down menu.

Setting the trace option for the Tivoli Enterprise Portal Server trace

You perform these operations on the computer that hosts the component for which you are setting trace levels. You must navigate to the directory path (called *itm_home* in these examples) for your installation of IBM Tivoli Monitoring.

- For UNIX-based systems:
  1. Open the following file in a text editor:
     itm_home/config/cq.ini
  2. Change the **KBB_RAS1=** environment variable to match the following string:
     KBB_RAS1=ERROR(UNIT:KDY ALL)
- For Windows systems:
  1. Open the following file in a text editor:
     itm_home\bin\kfwenv
  2. Change the **KBB_RAS1=** environment variable to match the following string:
     KBB_RAS1=ERROR(UNIT:KDY ALL)

Setting the trace option for the Tivoli Enterprise Monitoring Server trace

You perform these operations on the computer that hosts the component for which you are setting trace levels. You must navigate to the directory path (called *itm_home* in these examples) for your installation of IBM Tivoli Monitoring.

– For UNIX-based systems:

1. Configure the first of two environment variables:
   a. Open the following file in a text editor:
      itm_home/config/*hostname*_ms_*TEMSid*.config

      where *itm_home* is the directory where IBM Tivoli Monitoring is installed, *hostname* is the name of the computer where you installed the product, and *TEMSid* is an ID for the monitoring server that is generated during installation.
   b. Change the **KBB_RAS1=** environment variable to match the following string:
      KBB_RAS1=ERROR(UNIT:KDY ALL)
2. Configure the second of two environment variables:
   a. Open the following file in a text editor:
      itm_home/bin/tacmd
   b. Change the **KBB_RAS1=** environment variable to match the following string:
      KBB_RAS1=ERROR(UNIT:KDY ALL)(UNIT:KUI ALL)
3. Recycle the Tivoli Enterprise Monitoring Server by ″restarting,″ or ″stop″ and then ″start″.

– For Windows systems:

1. Configure the first of two environment variables:
   a. Open the following file in a text editor:
      itm_home\CMS\KBBENV
   b. Change the **KBB_RAS1=** environment variable to match the following string:
      KBB_RAS1=ERROR(UNIT:KDY ALL)
2. Configure the second of two environment variables:
   a. Open the following file in a text editor:
      itm_home\bin\KUIENV
   b. Change the **KBB_RAS1=** environment variable to match the following string:
      KBB_RAS1=ERROR(UNIT:kdy ALL)

Setting the trace option for the Agent Deploy tool

You perform these operations on the computer that hosts the component for which you are setting trace levels. You must navigate to the directory path (called *itm_home* in these examples) for your installation of IBM Tivoli Monitoring.

– For UNIX-based systems:

1. Open the *itm_home*/config/<hostname>_ms_<TEMS id>.config file in a text editor and insert this trace log setting:
   KBB_RAS1=ERROR(UNIT:KDY ALL)
2. Open the *itm_home*/bin/tacmd file in a text editor and insert this trace log setting:
   KBB_RAS1=ERROR(UNIT:KDY ALL)(UNIT:KUI ALL)
3. On the Agent machine running the O/S Agent make the following changes:
   - For UNIX (other than Linux), open the *itm_home*/config/ux.ini file in a text editor and insert this trace log setting:
     KBB_RAS1=ERROR(UNIT:kdy ALL)(UNIT:kdd ALL)
   - For Linux, open the *itm_home*/config/lz.ini file in a text editor and insert this trace log setting:
     KBB_RAS1=ERROR(UNIT:kdy ALL)(UNIT:kdd ALL)

4. Recycle the O/S Agent on that computer.

– For Windows systems:
  1. Open the *itm_home*\CMS\KBBENV file in a text editor and insert this trace log setting:
     ```
     KBB_RAS1=ERROR(UNIT:KDY ALL)
     ```
  2. Open the *itm_home*\bin\KUIENV file in a text editor and insert this trace log setting:
     ```
     KBB_RAS1=ERROR(UNIT:kdy ALL)
     ```
  3. Recycle the monitoring server.
  4. On the Agent machine running the O/S Agent make the following changes:
     a. Open the *itm_home*\tmaitm6\KNTENV file in a text editor and insert this trace log setting:
        ```
        KBB_RAS1=ERROR(UNIT:kdy ALL)(UNIT:kdd ALL)
        ```
     b. Recycle the O/S Agent on that computer.

- Regarding APAR IY95361, the *IBM Tivoli Monitoring Installation and Setup Guide* needs to be updated with the following configuration information: You have the option to configure to Tivoli Enterprise Portal Server to use an external Internet Information Server (IIS) V6.0 web server. However, you must configure IBM Tivoli Monitoring to use a port other than **80**, the default port that IBM Tivoli Monitoring assigns. Otherwise problems might arise, such as socket pooling.
- Regarding APAR IY91951, background information and instructions should be provided to explain the differences between fix packs 1, 2 and 3 for IBM Tivoli Monitoring V6.1 and subsequent fix packs. See the following topic: "(*If you installed Fix Pack 3 or earlier*) Comparison of installation processes for former fix packs versus recent fix packs."

(*If you installed Fix Pack 3 or earlier*) Comparison of installation processes for former fix packs versus recent fix packs

You can directly upgrade from any previous IBM Tivoli Monitoring V6.1.0 Fix Pack to Fix Pack 6. After the upgrade you must use the component software from Fix Pack 6 for all subsequent updates that you make to your monitoring environment. In particular, you must not use the installation media from Fix Packs 1, 2, or 3. Otherwise, you might damage your environment. The information in this section addresses APAR IY91951.

Note: This section provides background information for customers who installed Fix Pack 3 or earlier only. These customers must account for differences between the installer that they used and the installer that is used for Fix Pack 4 and higher. If you have installed (or plan to install) Fix Pack 4 and higher only, you can disregard this section.

The IBM Tivoli Monitoring base and agent installer evolve over time to incorporate new functionality. With each new release, you must apply the versions and levels in correct sequence, as described in this section.

Two types of fix pack installation: Originally with the general availability (GA) version of IBM Tivoli Monitoring 6.1, an installer existed to install the products, including components that are provided in the base product CD, and a separate CD that contains software for specific types of monitoring agents.

Note: In all cases, each fix pack for IBM Tivoli Monitoring 6.1 includes the fixes provided in prior fix packs.

- **Policy for Fix Packs 1, 2, and 3:** You use the **itmpatch** command to install Fix Packs 1, 2, and 3. An installation of IBM Tivoli Monitoring 6.1 GA code was a prerequisite for installing these fix packs. These fix packs do not provide standalone installers.

  Note: If you upgrade Fix Packs 1, 2, or 3 (without moving to Fix Pack 4 or higher), you install the upgrade using the **itmpatch** command.

  The **itmpatch** tool can be used for limited availability (LA) fixes, which use a legacy patching format. These fixes typically contain a very small subset of affected files and platforms, whereas

the fix pack and interim fix formats are a refresh of the original media in its entirety. As a legacy patching tool in limited use, **itmpatch** has not been globalized in the IBM Tivoli Monitoring 6.2 release.

- **Policy for Fix Packs 4 and higher:** Starting in Fix Pack 4, the patches for IBM Tivoli Monitoring were replaced with a new installation or upgraded system. You install a new instance of IBM Tivoli Monitoring 6.1, if one does not already exist on the target computer. If IBM Tivoli Monitoring 6.1 already exists on the target computer, the installer updates only the components that need to be updated.

Specific guidelines: Follow these guidelines when you apply code to an IBM Tivoli Monitoring installation.

After you install a new fix pack, always use the installation software for that new fix pack when you want to install additional components for IBM Tivoli Monitoring.

You must never install a new component using software from a previous fix pack. For example, you must not do the following:

- Do not attempt to use a prior installation image to install monitoring agent software. Specifically, do not attempt to use the IBM Tivoli Monitoring 6.1 GA installer or any previous fix packs.
- Do not attempt to use a prior installation image to the integration component for IBM Tivoli Enterprise Console. Specifically, do not attempt to use the IBM Tivoli Monitoring 6.1 GA installer or any previous fix packs.

Understand the following scenario, which explains how older fix pack installers interact with the separate installers that exist for some monitoring agents.

The following scenario explains how fix pack installers interact with the separate installers that exist for some monitoring agents.

1. You install the GA version of IBM Tivoli Monitoring 6.1 and install only the OS agent.
2. You upgrade to Fix Pack 3 using the appropriate **itmpatch** installer mechanism used at Fix Pack 3 level.
3. Later, you upgrade to IBM Tivoli Monitoring 6.1 Fix Pack 4 using an installer
4. You now want to install the UNIX log agent. In this scenario, the only valid option is to use the IBM Tivoli Monitoring 6.1 Fix Pack 4 installer.

   Note: A version of the UNIX log agent is provided on the original installation media for the product. However, it is not valid to use the installer for the GA version of IBM Tivoli Monitoring 6.1 in this case.
5. You now want to install the IBM DB2 monitoring agent. This agent is distributed separately from the base installation media for IBM Tivoli Monitoring 6.1. Furthermore, the fix pack releases for this agent are provided at different times and on media that is distinct from the base installation media.

The rule that applies to the installation CD for the base product also applies to agent-related installation CD. After you upgrade to a new fix pack, you must use the CD from that new fix pack for any new agent installations or upgrades. You must not use prior installation media to install or upgrade additional components.

Notice the difference in media

- Upgrades from IBM Tivoli Monitoring 6.1 GA to Fix Packs 1, 2, and 3 are based on compressed files that the **itmpatch** tool references. For these fix packs, you are patching a GA installation of IBM Tivoli Monitoring 6.1.
- Installation of Fix Pack 4 and higher is based on an installation executable file (Windows) or a shell script (UNIX-based systems).

Remote deployment issues

These known problems and limitations are related to remote deployment.

- **Limitation:** If you use **tacmd updateAgent** from a Windows Tivoli Enterprise Monitoring Server to upgrade a UNIX OS monitoring agent running on AIX 5.2 from IBM Tivoli Monitoring 6.1 Fix Pack 5 level to Fix Pack 6 level, you may see one of the following messages:

  ```
  KUICUA099E: The updateAgent command did not complete because a system error occurred.
  An unexpected system error occurred while executing the updateAgent command.
  ```

  or

  ```
  KUICUA015E:  The updateAgent command did not complete because an error occurred. Refer to the
  following error returned from the server:
  The monitoring server encountered an error while updating the managed system type.
  The kuiras1.log file might provide more information about this error. If you
  require further assistance resolving the error, contact IBM Software Support.
  The file unix\axaix513.jar was not transferred to <target> from <depot>.
  A file on the agent bundle depot was not read because the file was not written to the target or
  there was a communication problem with the target system.
  ```

  Workaround: Access the AIX 5.2 system locally. Remove any remnants of the failed installation. Perform a local installation of the IBM Tivoli Monitoring 6.1 Fix Pack 6 UNIX OS monitoring agent.
- **Limitation:** An attempt to use **tacmd createNode** to deploy a UNIX OS monitoring agent to Solaris 10 target computer fails with the following message:

  ```
  KUICCN028E The silent response file for agent kux could not be found
  ```

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

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

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

If an entry in Add and Remove Programs does not exist and other monitoring agents are deployed to the target computer and then removed, the Windows monitoring agent can disappear after a second agent is removed from the remote computer.

- For 64-bit Windows computers, the installation stops indicating that there are missing .cab files.

  Locally install all of your monitoring agents. Due to a current restriction on 64-bit Windows computers, remote deployment cannot be used to update monitoring agents that are installed from a single CD. For example, the Tivoli Universal Agent and the Windows agent both are located on the same CD and there are four agents on the Database CD. To upgrade any agent on these CDs, you must do one of the following:

  – Physically take the CD to a remote computer and install it.
  – Copy the CD to the remote computer and install it.
  – Use a network drive that the remote computer can access for the installation.

  Uninstall the previous version of the agent before installing the new version. You must upgrade all of the agents on the CD at the same time from the local installation. If you need to install an agent from the CD at a later time, you must install the agent from the exact same location as you used for the original installation. Consider using a local copy of the CD or a network copy from the target computer and that it remain until all agents from that CD are removed. If you use a network copy, the mapped drive must remain at the same location for all installation of components from the mapped CD image.

- When attempting to install an application agent using Add Managed System from the Tivoli Enterprise Portal to a Windows OS computer, you might receive the following error message:

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

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

  1. Click **OK** on the error message window.
  2. Select the **Navigator update pending** button if it is displayed at the bottom of the Tivoli Enterprise Portal navigator.
  3. Verify that the new agent entry is displayed within the Tivoli Enterprise Portal navigator.
  4. Select the agent and browse through its workspaces to determine if it is communicating successfully and reporting data.

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

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

Tivoli Enterprise Monitoring Agent

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

- **UNIX OS monitoring agent running on an HP-UX system consumes CPU:**

  In a monitoring environment that includes a UNIX OS agent running on an HP-UX system, a **tacmd viewAgent** command run against other types of monitoring agents causes an error. For example, the following command run against the UNIX Log Alert (KUL) monitoring agent might fail:

  ```
  tacmd.exe viewAgent -m name:KUL
  ```

  The following message is generated:

  ```
  A Tivoli Enterprise Management Server error occurred while trying to complete the deployment request.
  The Tivoli Enterprise Management Server is not operational or not configured properly.
  Check the Tivoli Enterprise Management Server log for more details. Verify that the server is
  operational and configured properly.
  ```

  When you see this condition on the HP-UX system, an extra **kuxagent** process has been spawned by the original **kuxagent**, and it is consuming 99% of the CPU. If you kill the extra agent, another is spawned. After you kill the second extra agent, it is not respawned until you issue a **viewAgent** command again.

Note: The defect does *not* occur when the **viewAgent** command runs against the UNIX OS (KUX) monitoring agent, for example, if you run a command like the following:

```
tacmd viewagent -m name:KUX.
```

The defect has only been verified on HP-UX 11.11. It is not known if it occurs on other versions of HP-UX. The defect does NOT occur on other UNIX agent platforms, such as AIX and Solaris

- **Issue:** Regarding IY81984, when the UNIX OS Agent is running on an HP-UX 11i operating system, a core dump occurs in the following situation:
  1. You are successfully running the agent with the original release of IBM Tivoli Monitoring V6.1.0.
  2. You upgrade the Tivoli Enterprise Portal Server and Tivoli Enterprise Monitoring Server to Fix Pack 6, including the required restarting of the monitoring server during installation.
  3. After the restart operation, you see a core dump of the UNIX OS Agent.

  Workaround: Use Fix Pack 6 to upgrade the agent.
- For all OMEGAMON XE agents on z/OS that support sysplex-level tables, you are encouraged to specify history collection for all managed system in a sysplex, but collection actually takes place only on the current sysplex proxy-managed system. UADVISORS distributed to other systems will have no data to write (unless they become the sysplex proxy). The sysplex proxy functionality will move to another eligible Tivoli Enterprise Monitoring Server in this sysplex if the current sysplex proxy monitoring server is stopped or fails.

  Therefore, distribute the sysplex-level tables to all eligible managed systems, but only the current sysplex proxy system will record data.
- **Linux OS Agent only:** Data fails to be displayed in the User Login Information workspace. This problem arises when you install the agent on a 64-bit zLinux operating system, but run the agent in 32-bit mode. The workspace is unable to access user login data.
- When you run the **tacmd stopAgent** command to stop the agent or agents for the specific managed systems, you might see an error message similar to the following:

```
C:\>tacmd stopagent -t OR -n Primary:AMSNT105:NT
KUICKA006I: Are you sure you want to stop the OR agent(s) that manage testdb:AMS NT105:ORA?
   Enter Y for yes or N for no: Y
KUICKA007I: Stopping OR agent(s).
KUICKA009E: A problem occurred while stopping OR - refer to the following error returned
from the server:
The monitoring server encountered an error while stopping the managed system.
If the error information returned from the server is not sufficient to help you resolve
the error, contact IBM Software Support.

The command C:\data\E8\installITM\Batch\kincli  -stopagent -akor -itestdb did not start
or stop agent.

The command returned a return code. Call IBM Support.
```

  When remote commands are used extensively in the IBM Tivoli Monitoring environment, a specific default value in the Windows registry needs to be increased. Otherwise, heap leakage can occur and cause the system to run out of memory for the operation. The problem is registered by Microsoft at the following URL: http://support.microsoft.com/kb/184802/EN-US/. However, contact IBM Software Support for help in resolving this problem.

  Note: Do not attempt to alter the registry without first contacting IBM Software Support for assistance.

Tivoli Enterprise Monitoring Server

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

Tivoli Enterprise Monitoring Server on distributed platforms issues

- **Context:** IBM Tivoli Monitoring gives you the option to create a hot-standby hub Tivoli Enterprise Monitoring Server to provide failover support for the monitoring environment. You have the option to choose from several communications protocols, and you can specify up to three protocols to be used for communication. If the method you identify as Protocol 1 fails, Protocol 2 is used as a backup. If Protocol 2 fails, Protocol 3 is used as a backup.

  Problem: If your remote monitoring server runs on Windows, and has been configured with two protocols, on reconfiguring the monitoring server, the configuration dialog box automatically specifies that a third communication protocol will be configured. Unless you deselect the checkbox for the third protocol, or specify a third protocol, you cannot proceed with configuration to completion. After you have properly configured this, the next two dialogs are for specifying the hostname and port number for each protocol. The hostname or IP address of the second protocol to the hot standby monitoring server is incorrectly set to that of the primary hub monitoring server, not the hot standby monitoring server. Later, in a failover scenario, packets to be sent to the hot standby over the second protocol are actually sent to the failed primary hub.

  Workaround: Deselect the third protocol value if you do not want to establish it. Always check the host name and IP address settings in the configuration panels to insure that they target the hub monitoring server that you intend. Correct the values as needed.

- **Limitation:** An attempt to restart the Tivoli Enterprise Monitoring Server on Solaris fails, because of interference from a process that continues to run from the previous invocation of the Tivoli Enterprise Monitoring Server. It is normal for the running of the Tivoli Enterprise Monitoring Server to spawn the **kdsmain** process and the **cms** process. However in this problem scenario, the **kdsmain** process is killed after you stop the Tivoli Enterprise Monitoring Server, but the **cms** process continues to run.

  Workaround: Resolve the problem as follows:

  1. Issue the following command to confirm that the improper cms process is the source of the problem:

     ```
     ps -ef | grep cms
     ```

     In this case, the results of your search include the following string, which shows that the **cms** process continues to run: *itm_home*/sol603/ms/bin/cms start
  2. Kill the **cms** process, using the following command: `kill -9` *process_number*
  3. Issue the following command to restart the monitoring server: ./itmcmd server start *TEMS_name*

- In a Hot Standby environment, there are two hub monitoring servers. The configuration of each hub designates the other hub as the Hot Standby hub. At any given time, one of the two hub monitoring servers is operating as the hub. This server is referred to as the *Acting Hub*. The other hub monitoring server is in standby mode and is referred to as the *Standby Hub*.

  In IBM Tivoli Monitoring, version 6.1, you must not immediately restart the hub monitoring server that has failed. You must wait until all the remote monitoring servers and agents that were connected to the failed hub server successfully fail over to the standby hub. See the following sources to learn more about Hot Standby in IBM Tivoli Monitoring:

  – *IBM Tivoli Monitoring Installation and Setup Guide*
  – Check for recent articles in the IBM Tivoli Open Process Automation Library (OPAL) at the following Web address: http://www-18.lotus.com/wps/portal/topal. Keyword strings, such as "high availability," "hot standby," and a related issue, "clustering" lead you to any recent information.

- Regarding IY97997, on UNIX systems, the configuration process for the Tivoli Enterprise Monitoring Server places the SOAP access list in the following path in the IBM Tivoli Monitoring installation directory (referred to as the *itm_home* variable in this document):

  itm_home/tmaitm6/*operating_system*/ms/bin/HTML/kshxhubs.xml

  Issue: At run time, the Tivoli Enterprise Monitoring Server looks for the SOAP access list in a different path:

  itm_home/tables/*host_name*/HTML/kshxhubs.xml

As a result, the monitoring server does not detect a SOAP access list and adopts the default behavior of honoring SOAP requests for all userids on the system (assuming that security for the Tivoli Enterprise Monitoring Server is enabled).

Workaround: Create a link from *itm_home*/tables/*host_name*/HTML to *itm_home*/tmaitm6/*operating_system*/ms/bin/HTML/kshxhubs.xml. The configuration process continues to update the **kshxhubs.xml** file, and the Tivoli Enterprise Monitoring Server is able to read and honor the userid authorizations that the file contains.

- The *IBM Tivoli Monitoring Administrator's Guide* and *IBM Tivoli Monitoring Problem Determination Guide* can include the following configuration recommendation:

  Tuning the performance of SOAP transactions on AIX: On AIX systems, the default behavior for TCP connections is to allow delayed acknowledgements (**Ack** packets). When **tcp_nodelayack** is set to **0** (the default setting), TCP delays sending **Ack** packets by up to 200 ms. This allows the **Ack** to be combined with a response and minimizes system overhead. If you set the **tcp_nodelayack** parameter to **1** TCP immediately sends acknowledgement (Ack) packets to the sender. If you set **tcp_nodelayack** to **1** slightly more system overhead is generated, but much higher performance for network transfers results, when the sender is waiting for acknowledgement from the receiver. Measurements of communication between IBM Tivoli Monitoring components indicate that setting **tcp_nodelayack** to **1** can significantly improve performance.

  To make the parameter setting, access a user account that has **root** privileges and issue the following command:

  ```
  no -p -o tcp_nodelayack=1
  ```

  The following output is typical:

  ```
  Setting tcp_nodelayack to 1
  Setting tcp_nodelayack to 1 in nextboot file
  ```

  This is a dynamic change that takes effect immediately. The **-p** flag makes the change persistent, so that it is still in effect the next time you start the system.

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

  ```
  ulimit -a
  ```

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

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

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

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

  ```
  +45FFF5A0.0027
  +45FFF5A0.0027 ************
  +45FFF5A0.0027 ************ WARNING: UNABLE TO MAKE AN INTRA-PROCESS TCP
  ```

```
+45FFF5A0.0027 ************          CONNECTION USING THE LOOPBACK INTFC
+45FFF5A0.0027 ************          IF YOU ARE RUNNING FIREWALL SOFTWARE
+45FFF5A0.0027 ************          IT MAY REQUIRE A CONFIGURATION CHANGE
+45FFF5A0.0027 ************
+45FFF5A0.0027
+45FFF5A0.0027
+45FFF5A0.0027
```

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

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

- This item addresses APAR IY93701. Changes made in Fix Pack 3 for the Tivoli Enterprise Monitoring Server component caused problems for some users such that situations were not being started at the remote agents connected to a remote monitoring server. Fixes are available for the monitoring server on z/OS and on distributed platforms.
  - **On z/OS**: OA18854 has been created to PE PTF UA28536. The fix for this is to rebuild the Object Access List file at the remote monitoring server. To do this the client can delete: &rvhilev.RKDSDOBJ file, then open the Configuration Tool, and rebuild the RTE where the monitoring server is defined and submit this JCL. This job will rebuild only files that are not allocated.
  - **On Distributed Platforms:** To support this fix in the distributed environment, do the following.

    On Windows:

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

    On UNIX or Linux:

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

  For more information, see Technote 1250181 at http://www-1.ibm.com/support/docview.wss?uid=swg21250181 .
- Some products might have two .sql files when using Manage Tivoli Enterprise Monitoring Services to add application support to a Tivoli Enterprise Monitoring Server on a different computer.
  - Use k*pc*.sql, where *pc* is the two-character product code, if this is the first time that you are adding application support to that product.

– Use k*pc*_upg.sql, where *pc* is the two-character product code, if you are upgrading a product where you previously added application support.

The k*pc*.sql can contain delete statements that remove user customizations; therefore, you do not want to use it you have previously added application support and want to keep that configuration.

- In some instances where the hub Tivoli Enterprise Monitoring Server running on Linux on zSeries with Fix Pack 6, startup messages indicate that the monitoring server has timed out before it was able to start. However, the message might be generated in error. The monitoring server might have indeed started correctly with every service initialized. The message is misleading. Check the status of the monitoring server and if it is has started, ignore the error message. .\
- Be aware that the names used to configure the IP.UDP protocol on the Tivoli Enterprise Monitoring Server across platforms are inconsistent. On Linux or UNIX, IP.UDP is referred to as IP. In Windows and z/OS, it is named IP.UDP. However, IP.UDP and IP are the same protocol.

Tivoli Enterprise Monitoring Server on z/OS systems issues

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

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

  A circumvention for this error is to restart the hub monitoring server.
- In some instances, a remote Tivoli Enterprise Monitoring Server on z/OS is slow to acknowledge that it has been shut down using the `/p` command, even though monitoring agents running on the remote monitoring server acknowledge the shutdown immediately.

  Before assuming that the shutdown of a remote monitoring server on z/OS failed, check the status again after 15 minutes.
- When creating the jobs for batch mode installation the Runtime Environment *<myruntime>* (RTE *<myruntime>*), the following warning message is displayed:

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

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

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

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

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

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

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

After installation of application support, product-provided situations are not displayed in the Tivoli Enterprise Portal Situation editor or do not auto start. This problem occurs only with a z/OS hub monitoring server.

Explanation: The definitions of product-provided situations are installed on the hub Tivoli Enterprise Monitoring Server when application support for a product is installed. If the VSAM data sets in which the data is stored have filled up so that the data cannot be added, situations definitions might not be installed or the definitions might be incomplete.

If application support has been installed, check the `NonResSeedk`*`pp`*`.log` files in *`itm_home`*`\cnps\logs` for errors (where *pp* is the two-letter product code of a monitoring product for which you installed support). Any `SQL1_OpenRequest status=81` errors might indicate that you have a VSAM I/O error.

Workaround: If you see this error, check data sets whose names end in RKDS* to determine if they are out of space or have run out of extents. For example, *&rvhilev.&rte.&vsamfsv.RKSSSITF*, where *&rvhilev* is the VSAM runtime high-level qualifier, *&rte* is the RTE name, and *&vsamvsf* is the monitoring server EIB VSAM low-level qualifier.″ Refer to the TEMS started task to see a complete list of VSAM EIB files.

If the data sets are out of space:

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

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

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

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

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

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

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

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

Complete the following steps:

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

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

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

      Note: When you select a particular time period, by default, any time periods below the one you select is automatically selected too. For example, if you select to keep yearly summarized data, quarterly, monthly, weekly, daily, and hourly are selected too. You have the option to disable the time periods you do not want.
   e. In the **Pruning** section, select how you want to prune your data.
      1) Select the time period for the table to be pruned, Yearly, Quarterly, Monthly, and so on.
      2) Type the number of time periods in the next field.
      3) Select the pruning time period you wish. For example, if you want to prune hourly data when it becomes 30 days old, select **Hourly**, keep **30** and choose **Days** as the time period from the drop-down list.

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

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

Tivoli Enterprise Portal desktop and browser clients

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

Note: The information in this section supplements extensive troubleshooting information that is provided in the *IBM Tivoli Monitoring Problem Determination Guide*.

- **Connecting to portal servers of different versions**

  Tivoli Enterprise Portal V6.1.0 requires Java V1.4.2; Tivoli Enterprise Portal V6.2.0 requires Java V1.5. The desktop client must be at the same version as the portal server it connects to as does its Java version. This is also true for the browser client, but versioning is controlled at the portal server and upgraded automatically when you connect to a newer portal server.

  If you use the browser client and want to log on to a V6.1.0 portal server after having logged on to a V6.2.0 portal server, edit the applet.html file to enable the switch between the different Java versions. Otherwise, the V6.1.0 browser client will fail in its attempt to start with the wrong Java version (V1.5).

  Edit **applet.html** as follows:

  1. On the computer where the Tivoli Enterprise Portal Server V6.1.0 is installed, open applet.html in a text editor. On Windows, applet.html is in the *itm_home*\cnb branch. On operating systems such as Linux and AIX, it is in the *itm_home*/*platform*/cw branch, where *platform* is a string that represents the current type of operating system.
  2. Locate the **classid="clsid:1ACECAFE-0014-0002-0000-ABCDEFFEDCBA"** entry and change the last letter from "A" to "C" so that it reads: **classid="clsid:1ACECAFE-0014-0002-0000-ABCDEFFEDCBC"**
  3. Save and close applet.html. You can then open a new browser window and log on to the V6.1.0 portal server.
- You cannot delete a situation by clicking the **Delete** icon on the Situation Editor toolbar when you perform a **Create >New** or **Create >Another** function.

  To delete the situation, right-click on the situation name and select **Delete** or, with the situation selected, select **Delete** from the tool bar.
- This item addresses APAR IY90209. A policy does not function and returns a status code of 1145. Status code 1145 means that the Tivoli Enterprise Monitoring Server cannot find the situation's definition.

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

  Additionally, the situation definition is available to a policy only if the situation and policy have both been distributed to the same Tivoli Enterprise Monitoring Server. A policy and situation are not always directly distributed to a Tivoli Enterprise Monitoring Server, but are distributed to agents. The situation is

distributed to the Tivoli Enterprise Monitoring Server if the agent to which the situation is distributed is connected to that Tivoli Enterprise Monitoring Server. Ensure that the situation has the same distribution as the policy.

- In some instances when upgrading custom workspaces from OMEGAMON 350 to IBM Tivoli Monitoring V6.1 Fix Pack 6, depending on how the workspace was saved in OMEGAMON 350, the original default workspace might not be displayed for some users. The default workspace is still available under the list of workspaces returned under Enterprise Workspace.

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

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

Tivoli Enterprise Portal Server

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

- Regarding APAR IY97555, in large environments you might observe two symptoms when a Tivoli Enterprise Portal Server on AIX is started:
  - The system stops while initializing **KfwServices**. This happens when the **KFW_STARTJVM** environment variable setting in the `cq.ini` file is **N**. Other similar symptoms are possible.
  - The system goes into a loop when initializing **KfwServices**. This happens when the setting for the **KFW_STARTJVM** environment variable is **Y**.

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

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

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

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

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

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

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

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

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

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

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

```
dump -ov KfwServices
```

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

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

d. Change directories as indicated:

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

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

```
EXTSHM=ON
```

Save the edited `cq.ini` file.

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

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

   b. Issue the following commands:

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

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

```
EXTSHM=ON
export EXTSHM
```

Save the edit `userprofile` file.

3. Restart DB2 using these commands:

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

4. Restart the portal server using these commands:

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

- After upgrading to IBM Tivoli Monitoring Version 6.1 Fix Pack 6 from Fix Pack 2 or earlier, you might find that your operators are no longer able to see the severity of situations in Situation Event Consoles. This issue can be addressed by running the workspace migration utility to upgrade those workspaces on the system where Tivoli Enterprise Portal Server is installed. For information about running this utility, see “Portal server checklist” on page 37.
- You cannot use `tacmd configurePortalServer` command to determine available data sources for the Tivoli Enterprise Portal Server. The problem does not affect historical data collection.

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

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

1. Open the configuration file:
   - For Windows computers, open the *itm_home***cnps\kfwenv** configuration file.
   - For Linux and UNIX computers, open the *itm_home*/**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 portal server.

- You might see numerous errors in the Tivoli Enterprise Portal Server logs and the Tivoli Enterprise Portal Server might not shut down correctly when you send thousands of events more than the Tivoli Enterprise Portal Server was designed to handle.

  Use correct system design and load balancing to evenly distribute the load to the Tivoli Enterprise Portal Server.
- When your Tivoli Enterprise Portal Server is running on HP and you view custom workspaces after upgrading from OMEGAMON 350 to the current fix pack, 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.
- This item addresses APAR IY87195. If you install the Tivoli Enterprise Portal Server on a Microsoft SQL Server 2000 computer with the SQL authentication method set to ″mixed mode,″ you might receive internal security authentication rule errors stating that all SQL servers must use ″Windows only″ authentication. Use the following procedure to install the portal server with the Microsoft SQL Server 2000 in Windows Authentication only mode. A script for performing this action should be available from your IBM service representative.
  1. Temporarily configure the Microsoft SQL Server 2000 computer to use mixed mode authentication (for example, SQL Server and Windows authentication).
  2. Use the *IBM Tivoli Monitoring Installation and Setup Guide* to install the Tivoli Enterprise Portal Server.
  3. Stop the portal server through the Manage Tivoli Enterprise Monitoring Services utility.
  4. Reconfigure the Microsoft SQL Server to use Windows authentication only.
  5. Open the Control Panel and double-click **Administrative Tools**.
  6. Double-click on **Data Sources (ODBC)**.
  7. Select the **System DSN** tab.
  8. Select the ″teps″ data source and click **Configure**.
  9. Click **Next** until you receive the window that prompts you to designate how you want the Microsoft SQL Server to verify the authenticity of the login ID.
  10. Select **With Windows NT® authentication using the network login ID**.
  11. Click **Next** until the **Finish** button is displayed, and then click **Finish**.
  12. Click **OK** and close the ODBC Data Sources control panel.
  13. Open a Command Prompt window.
  14. Enter the following command:

      ```
      osql –E
      ```

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

      ```
      > use teps
      > go
      ```

16. At the prompt, enter the following commands:

```
> sp_changeobjectowner 'teps.KFWSEEDLEVEL', 'dbo'
> go
```

17. Repeat the command in step 16, replacing **KFWSEEDLEVEL** for each of the following table names:

```
KFWATTAC
KFWDBVER
KFWEDGE
KFWFOUNDODI
KFWHISTBEHAVIOR
KFWHISTDATA
KFWHISTSTAT
KFWJRNLLOGIN
KFWLAUNCH
KFWLOGIN
KFWMOBJ
KFWMOBJASSIGNED
KFWMOBJPROP
KFWNOTES
KFWPARMA
KFWPRESDEF
KFWPRESENTATION
KFWQUERY
KFWRANGES
KFWSEEDLEVEL
KFWSOUND
KFWTMPL
KFWTMPLSIT
KFWTMPLSTA
KFWTOPO
KFWTSIT
KFWUAXREF
KFWUSER
KFWUSERTOPO
KFWWORKPLACE
KFWWORKSPACE
KFWWORKSPACELINK
```

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

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

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

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

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

Historical data collection issues

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

- **Issue:** You might experience an abnormal end of task error (ABEND) in KPDMANE when you are collecting historical data for attribute groups from the OMEGAMON XE for z/OS agent (product code **M5**). This error might be caused by the default setting for collection of historical data, which is to collect data at the monitoring agent. **Workaround:** Change the settings for collection of historical data in the History Configuration dialog box of the Tivoli Enterprise Portal. Instead of the default settings, configure collection of historical data to occur at the Tivoli Enterprise Monitoring Server for all of the attribute groups of OMEGAMON XE for z/OS.
- The following update is required in Chapter 14 of the *IBM Tivoli Monitoring Installation and Setup Guide* for IBM Tivoli Monitoring, V610, which is titled "Tivoli Data Warehouse solution using Microsoft SQL Server". The "Step 1: Create the Tivoli Data Warehouse database" section must be updated with the following statement:

Give the warehouse user **public** and **db_owner** privileges to the Tivoli Data Warehouse database. **Note:** The warehouse user must have these two privileges *only*. Do not grant additional privileges.

- When there is a network connection problem on the remote server for Tivoli Data Warehouse, the **sy** log file for Summarization and Pruning might show the Java exception errors like below. No action is required other than resolving any network connection problems:

```
java.sql.SQLException: Io exception: The Network Adapter could not establish the connection
 at oracle.jdbc.driver.DatabaseError.throwSqlException(DatabaseError.java(Compiled Code))
 at oracle.jdbc.driver.DatabaseError.throwSqlException(DatabaseError.java:162)
 at oracle.jdbc.driver.DatabaseError.throwSqlException(DatabaseError.java:274)
 at oracle.jdbc.driver.T4CConnection.logon(T4CConnection.java:319)
 at oracle.jdbc.driver.PhysicalConnection.<init>(PhysicalConnection.java:344)
 at oracle.jdbc.driver.T4CConnection.<init>(T4CConnection.java:148)
 at oracle.jdbc.driver.T4CDriverExtension.getConnection(T4CDriverExtension.java:32)
 at oracle.jdbc.driver.OracleDriver.connect(OracleDriver.java:545)
 at java.sql.DriverManager.getConnection(DriverManager.java:539)
 at java.sql.DriverManager.getConnection(DriverManager.java:189)
 at com.tivoli.twh.ksy.db.WHDriverManager.getConnection(WHDriverManager.java:146)
 at com.tivoli.twh.ksy.agg.AggProduct.setupParameters(AggProduct.java(Compiled Code))
 at com.tivoli.twh.ksy.Enable.run(Enable.java(Compiled Code))
 at com.tivoli.twh.ksy.Enable.runMain(Enable.java(Compiled Code))
 at com.tivoli.twh.ksy.Enable.main(Enable.java(Compiled Code))
```

- The section in the *IBM Tivoli Monitoring Installation and Setup Guide* that describes "Configuring a Warehouse Proxy agent on Linux or AIX (JDBC connection)" requires the following statement regarding prerequisites:

Prerequisite: To enable configuration of the Warehouse Proxy agent, the X Window System (also known as the X11 GUI) must be available on the computer that hosts this agent.

In some cases, you might not have physical access to the host computer. You can run the **xhost +** command in the XTERM which allows every user who has access to such a host to connect to the display and run the following command in your terminal window to use an X terminal emulation program (such as Cygwin) that is running on another computer:

```
export DISPLAY=my_windows_pc_IP_addr:0.0
```

where *my_windows_pc_IP_addr* is the IP address of a computer that is running an X terminal (emulation) program.

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

  Go back to the history configuration panel and start the history group associated with this data. After the collection is started, you will no longer experience the SQL 3000 error.
- For monitoring agents on z/OS that use Tivoli Data Warehouse and capture configuration data in GENHIST files, there are instances when a persistent datastore delete request can corrupt a dataset.

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

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

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

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

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

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

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

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

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

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

  ```
  /F stcname,KPDCMD DEBUG OFF
  ```
- The Tivoli Enterprise Portal Server might record messages similar to these below. These messages can be ignored.

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

These messages can be ignored.

- If your workspace views display historical data across multiple pages, data is displayed only on the first page (and not displayed on subsequent pages).
- See “Ensuring display of historical data” on page 78 for information regarding APAR IY98582.

Summarization and Pruning Agent

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

- This item addresses APARs IZ00361 and IY99299. **Summarization and Pruning Agent updates:**

  The Summarization and Pruning Agent is updated with the following fixes and enhancements:

  – Incorrect timestamps generated on summarized tables
  – Incorrect date used for weekly summarized data
  – Scheduling tab defaulted to flexible rather than fixed
  – Aggregation stopped after first blackout period
  – Incorrect messages in the log when a blackout makes scheduling temporarily impossible
  – Multiple delete support for deleting blackout periods in configuration panel

  To enable flexible scheduling, variables are added to the appropriate environment variable files. The following files are modified:

  – **On Windows:** The **KSYENV** file (located under *itm_home*\TMAITM6 directory)
  – **One UNIX-based systems:** The **sy.ini** file (located under *itm_home*/config directory)

  The following variables have been added. See the descriptions of the variables later in this section.

  ```
  KSY_FIXED_SCHEDULE=Y
  KSY_EVERY_N_MINS=60
  KSY_BLACKOUT=
  ```

  Graphical user interface for the new variables

  When these variables are present, you can view and modify the values in the configuration panel for the Summarization and Pruning Agent. If you do not see the variables in the configuration panel, you can manually insert the variables into the **KSYENV** or **sy.ini** file. The next time you access the panel, the variables will be visible.

  You access the configuration panel through the Manage Tivoli Monitoring Services window. Specifically, you right-click the row for the Warehouse Summarization and Pruning Agent and select **Reconfigure** in the pop-up menu.

Note: A Java focus issue exists *on UNIX systems only*, when you use the Manage Tivoli Monitoring Services window to configure the Summarization and Pruning Agent. As a result, the number that you type in the minutes field of the **Flexible** section is not preserved if you click **Save** immediately. Avoid this problem as follows:

1. Type the minutes value that you want in the **Flexible** section.
2. Click another section of the user interface. The input focus is refreshed.
3. Click on the **Save** button. The minutes value is saved, along with your other settings.

Description of variables

- `KSY_FIXED_SCHEDULE` controls whether to run using the existing mechanism (`Y`) or the new flexible scheduling (`N`).
- `KSY_EVERY_N_MINS` controls the frequency to execute the Summarization and Pruning function and respecting the exception periods provided by `KSY_BLACKOUT`. This is only used when `KSY_FIXED_SCHEDULE=N`.
- `KSY_BLACKOUT` lists blackout periods where Summarization and Pruning function should not run in the format `HH:MM-HH:MM` with multiple values separated by a comma. This is only used when `KSY_FIXED_SCHEDULE=N`. For example, to block the Summarization and Pruning Agent from running between `00:00` and `01:59` and between `04:00` and `04:59` use the following:

  ```
  KSY_BLACKOUT=00:00-01:59,04:00-04:59
  ```

The number of worker threads should be adjusted between `N` to `2 * N` where N is the number of processors where summarization and pruning is running. This can be adjusted either through the configuration panel or through the configuration file by modifying the `KSY_MAX_WORKER_THREADS` property.

Each worker thread deletes `KSY_MAX_ROWS_PER_TRANSACTION` divided by `KSY_MAX_WORKER_THREADS` rows in each transaction. When you increase the number of worker threads, the `KSY_MAX_ROWS_PER_TRANSACTION` can be increased to improve the pruning performance. The transaction log size must be large enough to handle the maximum number of rows per transaction plus inserts from the Warehouse Proxy and any other activity.

In order to use the new log table pruning, the following variables need to be added to the configuration files:

```
KSY_WAREHOUSELOG_PRUNE=
KSY_WAREHOUSEAGGREGLOG_PRUNE=
```

Both are expected to be in the form *`number.unit`* where *`number`* is the number of units to keep the data in the database and *`unit`* is one of day, month or year. For example, to keep 14 days of data use `14.day` You can also use the graphical user interface to configure summarization and pruning in the Log Param tab to set the pruning value.

- IBM Tivoli Monitoring does not support multiple Summarization and Pruning Agents. When you have two Summarization and Pruning Agents configured against the same hub Tivoli Enterprise Monitoring Server and the same database, one of the Summarization and Pruning Agents is the backup of the other. After the Summarization and Pruning Agent upgrade installation, you need to make sure to stop the backup Summarization and Pruning Agent that must be configured to start manually. There might be issues if you have two Summarization and Pruning Agents running with the same configuration at the same time.
- Sometimes when the Summarization and Pruning Agent has been correctly configured using the Manage Tivoli Monitoring Services interface and seems to be running, it actually is not. No data is ever aggregated into the various ***_H**, ***_D**, ***_W**, ***_M**, ***_Q**, ***_Y** tables in the **WAREHOUS** database, and no ***sy_java*.log** file is created. Resolve this problem as follows:
  - For a hub Tivoli Enterprise Monitoring Server on UNIX or Linux run the following command locally:

    ```
    itmcmd support -t TEMS sy
    ```

    Then recycle the monitoring server using this command:

    ```
    itmcmd server stop/start TEMS
    ```

  - If the Tivoli Enterprise Portal Server is running on Windows, right-click on the portal server and select **Advanced > Add TEMS application support**, select "On a different computer" if the hub monitoring

server runs on a different system, and select **Summarization and Pruning Agent Support**. For more information, see Technote 1230920 at http://www-1.ibm.com/support/docview.wss?uid=swg21230920

- For the Warehouse Summarization and Pruning Agent, if you are using Microsoft SQL server, install the MS SQL 2005 JDBC driver. The Warehouse Summarization and Pruning agent might fail to run at the scheduled time on Windows computers because of a limitation of the number of tables it can retrieve. The MS SQL 2005 JDBC driver addresses this limitation. You can download the JDBC driver from the Microsoft Web site, http://msdn.microsoft.com/data/jdbc/default.aspx.
- On Windows 2000 computers, the Summarization and Pruning agent does not work after you upgrade from OMEGAMON to IBM Tivoli Monitoring.

  A restart of the system is required to reset your home directory for the Summarization and Pruning Agent.
- After you upgrade the Summarization and Pruning agent from Fix Pack 5 to Fix Pack 6, the **sy** log file might contain a message similar to the following:

  ```
  . . . Only limited VisiSecure functionality is enabled, If the product has a valid license make
  sure all licensing related jar files are in the CLASSPATH.
  ```

  This condition is harmless. You can ignore this message.

Warehouse Proxy Agent

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

- Regarding APAR IZ02460, the Warehouse Proxy Agent might fail when it is running on Windows with an Oracle warehouse database. The error message for this failure indicates an access violation. At the time of release Fix Pack 6, there is no fix or workaround for this problem. Contact IBM Software Support for additional information.
- On Windows systems, after you upgrade a Warehouse Proxy Agent or the Summarization and Pruning Agent, any startup behavior that you established, such as manual startup, is maintained. However, these two types of agent will automatically start up after upgrade. This is the default behavior of all agents and this behavior is based on an IBM Tivoli Monitoring design requirement. The agent resumes the configured or customized behavior for all agents, which is to start automatically after installation of the upgrade. (The one exception to this default behavior is the Summarization and Pruning Agent. That type of agent starts automatically only if you have previously configured it.)

  In the case of the ″manual startup″ behavior that you might have applied for any agents, you must manually stop an agent immediately after the upgrade installation, so that it resumes the non-default startup behavior that you want during the system reboot.

  Possible issue: IBM Tivoli Monitoring Fix Pack 5 introduced the option to install multiple Warehouse Proxy Agents. When you have multiple Warehouse Proxy Agents configured against the same hub Tivoli Enterprise Monitoring Server and the same database, one of the Warehouse Proxy Agents is the backup of the others. After the Warehouse Proxy Agent upgrade installation, you need to make sure to stop the backup Warehouse Proxy Agent, which must be configured to start manually. There might be issues if you have two or multiple Warehouse Proxy Agents running with the same configuration at the same time. For more information on this topic see the following technote:http://www-1.ibm.com/support/docview.wss?uid=swg21268675

  When there are multiple Warehouse Proxy Agents configured in the environment and there are Warehouse Proxy Agents are the slave Warehouse Proxy Agent as the failover or backup of the master Warehouse Proxy Agent, make sure that they are not running after IBM Tivoli Monitoring Fix Pack upgrade installation if they are configured as manual startup or are not preferred to be running.
- When configuring one or more warehouse proxy agents, connect all of them to the hub Tivoli Enterprise Monitoring Server, not to a remote monitoring server. Connecting a warehouse proxy to a remote monitoring server results in incorrect connections. For example, if the local location broker facility in the

remote monitoring server included a previously existing network address of a previously existing warehouse proxy agent, the monitoring agents connected to that remote monitoring server might try to send the data to this obsolete warehouse proxy.

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

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

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

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

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

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

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

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

Tivoli Universal Agent issues

These known problems and limitations are related to the Tivoli Universal Agent.

- On page 216 of the *IBM Tivoli Universal Agent V6.1 User's Guide*, in Table 33 ″“IBM Tivoli Universal Agent environment variables”, the second column of the KUMP_SNMP_TRAP_PORT row, the words “in addition to” should be replaced with “instead of” so that the cell reads as follows: *Specifies an installation specific trap destination port that the SNMP Data Provider must monitor instead of the standard trap listening port 162.*
- Some instances of the Tivoli Universal Agent do not start or appear as if they have not been upgraded after installing the fix pack.

  All instances of the Tivoli Universal Agent have been upgraded after you run the installation. You must manually restart those Tivoli Universal Agent instances that do not automatically restart or appear as if they have not been upgraded.
- After upgrading to Fix Pack 6 on a UNIX or Linux computer, some of your Tivoli Universal Agent instances that were installed remotely do not restart and you receive the following error:

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

  Upgrade the Tivoli Universal Agent to Fix Pack 6 and manually restart any Tivoli Universal Agent instances that did not restart.
- In some cases, the Tivoli Universal Agent console fails to launch from the Manage Tivoli Enterprise Services GUI on SUSE Linux Enterprise Server 10 computers. Start the console manually as follows:
  1. Using a command line interface, navigate to the **bin** directory in the installation path for IBM Tivoli Monitoring.
  2. Run the **./um_console** command.

- After upgrading the Tivoli Universal Agent with the fix pack, the correct version is not displayed. The agents have been upgraded as expected, however.

Globalization

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

- **Problem:** For multi-byte languages like Japanese, the help pane of the Situation Editor Condition panel displays unreadable text until a situation attribute is selected. At that time, the correct language help for that attribute is displayed. The unreadable text is redisplayed every time a situation is selected from the tree.

  Workaround: Navigate to the language-specific help directory and rename the **dlg_attrdefault.htm** file to some other name like **dlg_attrdefault.htm.bak**. For Japanese, the file is on the Tivoli Enterprise Portal Server machine in: *itm_home*\CNB\classes\candle\fw\resources\help\ja. Files for other languages are located in the help subdirectory that corresponds to the code name for their respective locale language. Changing the file name in the language-specific directory causes the English version of the help text to be displayed. After the code has been fixed, the language-specific file has to be renamed back to its original name to reverse this workaround.
- If you run the Tivoli Enterprise Portal client in a non-English locale, you must apply the fix pack for the language pack after you install Fix Pack 6. Otherwise, certain user interface strings are displayed in English instead of the default language. (This requirement also applies if you reconfigure any of the base components, such as the portal server.)

  The name of the installation image is **6.1.0-TIV-ITM-LP-FP0006**. This update to the language pack includes a fix regarding an expired certificate, which was identified in APAR IZ03654.

  For information about installing the language packs, see the “Installing the language packs” section of the *IBM Tivoli Monitoring Installation and Setup Guide*.
- In non-English environments, the agent help is not displayed in the help panel. You must run a **helpmerg** script to merge the missing help into your environment, as follows:
  1. Navigate to the directory where the script is located in *itm_home*, the installation path for IBM Tivoli Monitoring:
     - On Windows, go to *itm_home***\CNB\classes\candle**.
     - On UNIX, go to *itm_home***/bin**.
  2. Run the script:
     - On Windows, run **helpmerge.bat** from the command line.
     - On UNIX, run **./CandleExecute cq helpmerg.sh** from the command line.
- The i5/OS operator messages displayed in the Tivoli Enterprise Portal in Japanese are not displayed correctly. This problem occurs after you have installed the fix pack and applied the language pack. The installation program changes the value for the CCSID variable in the QAUTOMON file.

  To fix this problem, you can do the following.
  1. Open a profile of the user QAUTOMON using this command:

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

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

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

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

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

1. From a command line, change to the `jre/bin` directory:
   `cd ../../jre/bin directory`
2. Run the following command:
   `./JavaPluginControlPanel`
3. On the **Advanced** tab, type the following in the **Java Runtime Parameters** text box:
   `-Dibm.stream.nio=true`
4. Click **Apply**.

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

Online help

These known tips, problems, and workarounds are related to online help.

- The *IBM Tivoli Monitoring User's Guide* describes how to write Expert Advice topics for the situations that you modify or create. However, the document needs to include mention of the `TEP_TARGET` option. This option enables the user to create an HTML hyperlink in an Expert Advice topic that launches the target page in a browser window outside of Tivoli Enterprise Portal. The `TEP_TARGET` option is also available for use in HTML files accessed by relative URL reference in a Tivoli Enterprise Portal browser view.

  The current documentation should be augmented with the **Note** that is displayed in the following steps:

  1. You can add formatting conventions, using standard HTML tagging, as in these examples:
     `<b>bold</b> and <i>italics</i>.`
  2. You can also add hyperlinks, as in this example:
     `<a href "http://www.ibm.com">IBM</a>`

     Click **Preview** to check that your coding is correct.

     Note: Add the `TEP_TARGET=external` attribute to a hyperlink to cause the page to be displayed in a browser window outside of the Tivoli Enterprise Portal, as in the following example:
     `<a href "http://www.ibm.com" TEP_TARGET=external>IBM</a>`

- This item addresses APAR IY88830. 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:

     itm_home\cnb\classes\candle\fw\resources\help\lang\

     UNIX computers:

     itm_home/cnb/classes/candle/fw/resources/help/lang

3. Rename **contents.htm** to **contents.bak**.
4. Rename **contents_dhtml.htm** to **contents.htm**.

If the *itm_home*\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 are enabled.

- The hover help is missing for the Time attribute in the **Local Time** and **Global Time** attribute groups. These are the descriptions:
  - **Time** in the **Local Time** attribute group: The time of the data sampling, corrected for local time zone and daylight saving time, formatted as HHMMSS. For example, 170700 is 5:07 PM.
  - **Time** in the **Global Time** attribute group: The time at the hub Tivoli Enterprise Monitoring Server when the data was sampled, formatted as **HHMMSS**. For example, **153000** is 3:30 PM.

Chapter 6. APARs addressed by Fix Pack 6

The list of fixed APARs below represents all APARs that were known to be fixed at the time of general availability (GA) for Fix Pack 6. Fixed APARs are categorized as follows:

Note: The lists include 70 fixed APARs from the interim fixes for Fix Pack 5.

- "Documentation APARs"
- "Installation component APARs"
- "Event Synchronization APARs" on page 108
- "Tivoli Enterprise Monitoring Agent APARs" on page 108
- "Tivoli Enterprise Monitoring Server APARs" on page 109
- "Tivoli Enterprise Portal APARs" on page 111
- "Tivoli Enterprise Portal Server APARs" on page 111
- "Tivoli Data Warehouse APARs" on page 112
- "Tivoli Universal Agent APARs" on page 113
- "i5/OS monitoring agent APARs" on page 114
- "Linux OS monitoring agent APARs" on page 114
- "UNIX OS monitoring agent APARs" on page 114
- "Windows OS monitoring agent APARs" on page 115

Updates to this list, if any become necessary, are provided in Technote 1266108 at the following Internet address:

http://www-1.ibm.com/support/docview.wss?uid=swg21266108

Instead of the Internet address, you can search for this Technote at the Tivoli Support Web site: http://www.ibm.com/support/us/. For example, you can search for the ID number of the technote, 1266108, or search for the version identifier of the fix pack itself, **6.1.0.6-TIV-ITM**. The technote should be relatively easy to locate in the resulting search hits.

Documentation APARs

The documentation updates for APAR IY91951 are provided in "Determining which components need to be upgraded to Fix Pack 6" on page 11.

Installation component APARs

The following APARs are addressed in Fix Pack 6:

APAR Number	Symptom
Tivoli Distributed Installer APARs	
IY98007	If the **HKLM\System\CurrentControlSet\Control\Session Manager** key value **PendingFileRenameOperations** was set and the list contained rename operations, IBM Tivoli Monitoring would say a reboot was pending and abort the install. The code was changed to include a review of the rename operations and if they did not involve IBM Tivoli Monitoring 6.1 files (in the **HOME** directory) we ignore the rename operations and perform the install. This problem only occurs in Windows operating systems.
IY99337	When an Agent (Remote or Local) had an Override Local Settings, the values were preserved during the upgrade from GA, Fix Pack 1, Fix Pack 2, Fix Pack 3 or Fix Pack 4 to Fix Pack 5, however the agent was not reconfigured after the values were added. This caused the agent to revert to default settings. This appeared to the customer as loss of customization.

© Copyright IBM Corp. 2007

APAR Number	Symptom
Other installation APARs	
IY93070	Additional documentation was provided. See “Configuring large monitoring environments” on page 74.
IY98598	ENABLE DEPLOYMENT WHEN DUPLICATE LOCAL HOSTNAMES EXIST
IY94388	OMEGAMON MESSAGING V6 INSTALL ISSUE - X11
IY98374	X LIBRARIES NEEDED TO INSTALL AMD OPTERON AGENT CODE
IZ00550	SECUREMAIN LOCKS AIX513 KUD ON AIX 64 BIT IF BOTH INSTALLED
IZ00597	NEED BETTER DOCUMENTATION FOR SECURELOCK
IZ00699	secureMain lock breaks MQ agent and tacmd
IZ04686	IF THE PARTITION.TXT FILE IS CUSTOMIZED BY THE ADMINISTRATOR,
IY90449	UPGRADE PACKAGING OF FP4 TO INCLUDE NEWEST IBM JRE TO CORRECT
IY96713	REMOTE DEPLOY OF AGENTS VIA TERMINAL SERVICES SERVERS
IY91583	ITM 6.1 FP03 PROBLEM WITH ″TACMD CONFIGURESYSTEM″ COMMAND FAILS
IZ02755	REMOTE DEPLOY: SEVERAL MEMORY OVERWRITES THAT CAN
IY88736	INSTALLATION OF WINDOWS OS AGENT CREATES %SYSTEMROOT%\PSAPI.DLL
IY96268	TACMD LOGIN FAILS WHEN GSKIT INSTALLED IN NON DEFAULT PATH.

Event Synchronization APARs

The following APARs are addressed in Fix Pack 6 regarding event synchronization between IBM Tivoli Monitoring and IBM Tivoli Enterprise Console:

APAR Number	Symptom
IY89788	THE TEST.CMD CAN GET PARSE FAILURE ON RESPONSES
IY90371	TEC_ITM_OM_SITUATION_SYNC_ERROR EVENT OCCURS WITH WRONG MSG.
IY91119	OMEGAMON.RLS USES DROP_RECEIVED_EVENT WITHOUT COMMIT_SET
IY91935	OMEGAMON.RLS CRASHES TEC IF A TEC_START IS PROCESSED
IY95029	SUF CAN’T TELL IF THE LISTENER ON A PORT IS A TEMS
IY96333	TEC CAN CLOSE SAMPLED ITM EVENTS
IZ01585	IF THE NAMES OF THE BAROC AND RLS FILES ARE CHANGED IN THE RULE BASE, EVENTSYNCH INSTALLERS WILL FAIL

Tivoli Enterprise Monitoring Agent APARs

The following APARs are addressed in Fix Pack 6:

APAR Number	Symptom
IZ02246	A Segmentation Fault might occur if entries are being placed or removed from the locale Object linked-list at the same time that a locale object on that linked-list is being validated. This also affects the Tivoli Enterprise Monitoring Server.
IY87701	Agent parses reflex substitutions incorrectly. It is not possible to add a suffix to variable without intervening blanks.

APAR Number	Symptom

IY96423	Situation action commands containing internationalized data do not work properly when the command executes at the agents. If a double quote character is used in the command, the agent might not format the command properly. When the situation is distributed to more than one agent, the agents might not receive the command at all. In some cases, the command might not stop executing when the situation is stopped.
	
	Additional Information: The following problems have NOT yet been addressed by this fix. The fix delivered in 6.1.0.5-TIV-ITM-IF0003 base fix pack was not updated to include these corrections.
	1. Situation reflex commands executed at the agent and having internationalized data that also contains the percent character (%) are not properly formatted. The following situation action command fails at the agent:
	`cmd opt %use service &{NT_Services.Display_Name} %count "%some utf8 data"`
	2. There must be a space character following the substitution parameters. If a space is not added after the substitution parameter, the resulting command might not be formatted properly. In this example, when a space character is not added before the double quote character, an extra ″ is added in error.
	`echo Process "path &{NT_Process.Binary_Path} name &{NT_Process.Process_Name}"`

IY95964	The krarloff history conversion utility was not being provided for HP NonStop Kernel systems. The utility is documented in the section: *Converting history files to delimited flat files on HP NonStop Kernel Systems* in the online IBM Tivoli Monitoring Administrator's Guide Version 6.1.0, but failed to provide the file for installation in `$CANDLEHOME/tmaitm6/ta6046/bin` for **HP H06.xx** Integrity NonStop platforms and `$CANDLEHOME/tmaitm6/tv6256/bin` for **HP G06.xx** NonStop Operating System platforms.
IY98649	The UNIX OS Agent consumes high CPU after a network glitch. This effects all v610 Tivoli Enterprise Monitoring Server and Tivoli Enterprise Monitoring Agent platforms except z/OS and Win32.
IY99106	FP5 TEMA INITIALIZATION FAILS: CONNECTION REFUSED
IZ07221	HISTORY DATA CORRUPTION ON AGENT.AGENT ON BOX W/ MULTIPLE CPU
IZ07224	FP5 TEMA INITIALIZATION FAILS: CONNECTION REFUSED

Tivoli Enterprise Monitoring Server APARs

The following APARs are addressed in Fix Pack 6:

APAR Number	Symptom
IZ02230	A hub Tivoli Enterprise Monitoring Server begins looping during processing, and stops working, as a result of nodelist entries that become corrupted. The problem typically arises with DB2 or SYSPLEX agents.
IY95811	When a remote Tivoli Enterprise Monitoring Server is shutdown, its OFFLINE heartbeat communication is missed by the Hub Tivoli Enterprise Monitoring Server. Consequently, the remote Tivoli Enterprise Monitoring Server status at the Hub continues to show ONLINE until its heartbeat interval expires. As a result, it can take up to 6 minutes for the remote Tivoli Enterprise Monitoring Server to change to OFFLINE at the hub following shutdown.
IY97601	If a situation formula includes functions such as *COUNT, *SUM, *AVG, *MIN, *MAX, (which are evaluated at the Tivoli Enterprise Monitoring Server), Reflex actions set to execute at the agent are executed despite the fact that the situation criteria are not true.
IY99897	Agents go online/offline continuously under high situation load.

APAR Number	Symptom
IZ00879	Due to a subscript specification error, the Data Server Catalog Cache Manager does not properly detect when a page has been exhausted and allows access beyond the page boundary causing an access violation exception.
IZ02246	A Segmentation Fault might occur if entries are being placed or removed from the locale Object linked-list at the same time that a locale object on that linked-list is being validated. This also affects the Tivoli Enterprise Monitoring Agent.
IZ02647	If an FTO configured HUB Tivoli Enterprise Monitoring Server is left up without starting the Mirror Tivoli Enterprise Monitoring Server, KQM eventually shutdown the HUB.
IZ02661	Tivoli Enterprise Monitoring Server abends in module khdxcl1 as a result of the KHD client passing null parameters to the KHD_ExportHistory RPC call. This fix requires patching both the Tivoli Enterprise Monitoring Server and Warehouse Proxy Agent components. See IY99862.
IZ03829	The following symptoms could occur, primarily in environments with OMEGAMON v350/360 agents. Agent on-line status keeps changing and the Tivoli Enterprise Monitoring Server logs contain the following message: `kdcc1sr.c,869,"rpc__sar") Remote call failure: 1C010003`
IY91246	The Situation Editor indicates targets (distribution endpoints) that are already included in the Custom MSL that a node has been explicitly added to, giving the impression that the CUSTOM MSL was not updated.
IY97535	HUB or remote Tivoli Enterprise Monitoring Server that are starting up consume too much CPU time and memory when a significant number of node list and access list records are being processed. **Additional Information:** To realize full benefit of the changes, the HUB and remote Tivoli Enterprise Monitoring Server should apply this fix.
IY98663	A Tivoli Enterprise Portal Server that is restarted might receive only status change records instead of records for all nodes. This results in a partial list of nodes in the recycled Tivoli Enterprise Portal Server.
IY98791	Tivoli Enterprise Monitoring Server instability when 'tacmd updateAgent' is used.
IY98908	Tivoli Enterprise Monitoring Server crashes when 'tacmd updateAgent' is used on a heavily loaded system.
IY99087	Tivoli Enterprise Monitoring Server crashes when 'tacmd updateAgent' is used in a large production environment.
IY99721	Tivoli Enterprise Monitoring Server crashes when 'tacmd updateAgent' is used in a large production environment.
IZ00413	The 'tacmd updateAgent' hangs in a large production environment.
IY93337	Tivoli Enterprise Monitoring Server goes offline when: 1. A policy has just been added. 2. A situation with take action that's set to execute at Tivoli Enterprise Monitoring Server every interval has just been added. 3. Soon after Tivoli Enterprise Monitoring Server is restarted, and there is at least one policy or situation fitting condition 1 & 2 above. Tivoli Enterprise Monitoring Server does not crash. Its process is still running, but it's no longer responding to requests.
IY93795	The LCLTMSTMP value for Situation Start and Stop events in TSITSTSH always report the time at PST/PDT regardless of the time zone of the Tivoli Enterprise Monitoring Server.

APAR Number	Symptom
IY96158	If DUPER is activated on the Tivoli Enterprise Monitoring Server through CMS_DUPER=YES and if a situation contains a predicate whose length exceeds 100 bytes, the Tivoli Enterprise Monitoring Server exits during initialization when situations are being assessed for duperization. Turning on (COMP:IBIFACE ALL) tracing reveals the situation that is being processed when the error is encountered.
IY82122	REPORT REQUESTS FAIL WHEN REQUESTED TO TOO MANAY MANAGED
IY95642	TACMD EDITSIT COMMAND HANGS WHEN SPECIFYING MORE THAN 69 HOSTS
IZ02087	AE IZ02083 FIX COMPLETION TACMD EXPORT WORKSPACES DOES NOT
IY90672	ITM6.1 KCJ196 OVERLY SENSITIVE CHECKBOX
IY94868	RESTORE ORIGINAL WORKSPACE MENU CHOICE REMAINS ENABLED EVEN
IY98398	DISPLAY ITEM VALUES HAVING JAPANESE CHARACTERS UNREADABLE
IY99702	DELETING MANAGED SYSTEM WITH SUBNODES FAILS AFTER FP5
IZ01301	CAN'T CLOSE PURE EVENTS WITH NOTES
IY98731	AGENTS COMING ON-LINE AT RTEMS DO NOT GO ON-LINE AT HUB.
IZ00010	UNIX OS AGENT CONSUMES HIGH CPU AFTER NETWORK GLITCH.
IY92356	EVENTS FAILING WITH REAL PARSING_FAILED LINE 1: VALUE DOES NOT MATCH TYPE REAL
IY91080	TEC EVENTS FORWARDED WITH # CHARACTER
IZ07219	HISTORY DATA CORRUPTION ON AGENT.AGENT ON BOX W/ MULTIPLE CPU

Tivoli Enterprise Portal APARs

The following APARs are addressed in Fix Pack 6:

APAR Number	Symptom
IY87499	Tivoli Enterprise Portal workspace table view thresholding is incorrect when the Tivoli Enterprise Portal client is run on a Windows computer that has hyper-threading active. The problem only occurs on Windows computers capable of hyper-threaded multiple CPU configurations.
IY96298	The user editor only displays a maximum of 100 installed applications. In addition, the application selection trees in the situation and query editor dialogs also only display 100 installed applications. Customers who have a large number of custom Tivoli Universal Agent applications might experience this problem if the number of custom UA applications plus the number of installed IRA-based applications is greater than 100.

Tivoli Enterprise Portal Server APARs

The following APARs are addressed in Fix Pack 6:

APAR Number	Symptom
IZ02878	During installation of the IF3 fix pack on AIX Tivoli Enterprise Portal Server with the Oracle Warehouse Database configured, the InstallPresentation.sh script appears to hang.
IZ03654	Starting September 1, 2007 running the IBM Tivoli Monitoring V6.1 browser client might prompt the user to accept an expired certificate. **Additional Information:** Customers running their Tivoli Enterprise Portal client in non-English locales should also apply the language pack that comes with Fix Pack 6.

APAR Number	Symptom
IY96347	When accessing warehouse data using JDBC, the scaling of decimal data is not taken into account and significant zeros are lost. Only when the data is greater than 100 does it begin to be displayed but with an incorrect scaling factor applied.
IY99020	In large environments, these symptoms might arise: 1. Events are out-of-sync between two Tivoli Enterprise Portal servers connected to same hub Tivoli Enterprise Monitoring Server. 2. Node status information as reflected in physical navigator does not match current state in INODESTS. 3. Events on a single managed object are different in two navigators on same Tivoli Enterprise Portal client. **Note:** There is a related IY98663 that manifests similar symptoms. See the Known Problems and Workarounds section below for details.
IY99088	Occasionally, the connection between the Tivoli Enterprise Portal Server and a remote DB2 warehouse database is reset. When this occurs, the Tivoli Enterprise Portal Server does not reconnect to the remote DB2 server. Tivoli Data Warehouse requests work fine shortly after starting Tivoli Enterprise Portal Server. After waiting a couple of days, many, but not all, Tivoli Data Warehouse views show the -30081 error.
IY86013	CHANGES TO TEP TRACE LEVELS ARE NOT EFFECTIVE ON JAPANESE BOXES
IY98067	BROWSER CLIENT CORE DUMPS WHEN ACCESSING THE SITUATION EDITOR.
IY91949	ITM 6.1 FP3, TEPS DOESN'T STORE WS LINKS WITHOUT THE USERID IN
IY92654	TEP PROBLEMS WHEN BROWSING WEB WITH HTTP PROXY SERVER ENABLED.
IY94745	TEP_TARGET=EXTERNAL SWITCH DOESN'T WORK THE SAME WAY FOR A WEB
IZ01792	RACE CONDITION CAUSES PERFORMWORK TIMEOUT ERROR

Tivoli Data Warehouse APARs

The following APARs are addressed in Fix Pack 6:

APAR Number	Symptom
IZ00361	Provide ability to prune the warehouseaggreglog and warehouselog. See "Summarization and pruning updates" on page 99 for instructions on enabling the updated code for this feature.
IY99299	The summarization and pruning agent is very slow in pruning data. See "Summarization and pruning updates" on page 99 for instructions on enabling the updated code for this feature.
IY99862	Tivoli Enterprise Monitoring Server abends in module khdxcl1 as a result of the KHD client passing null parameters to the KHD_ExportHistory RPC call. This fix requires patching both the Tivoli Enterprise Monitoring Server and Warehouse proxy components. See IZ02661.
IZ01655	The Warehouse Proxy code considers NULL padded data to be incorrect data but did not provide any checks or correction to this problem, blindly inserting the data into the database. This can result in failures to insert data into the database, errors during the Summarization and Pruning Agent or the display of strange characters in the Tivoli Enterprise Portal client.
IY93067	Summarization and Pruning Agent fails with java.lang.NullPointerException at com.tivoli.twh.ksy.agg.AggProduct.getVacationFromCandleTimestamp (AggProduct.java(Compiled Code))

APAR Number	Symptom
IZ00354	The Warehouse.LG0 file grows without bounds. Additional Information: The same data that was written to the Agent Operations file (Warehouse.LG0) can be found in the WAREHOUSELOG table within the warehouse. For example you can issue the following SQL statement to get the equivalent information formerly found in the Agent Operations file: `select ORIGINNODE,OBJECT, EXPORTTIME, ROWSINSERTED, ERRORMSG, WPSYSNAME from WAREHOUSELOG order by EXPORTTIME desc` This show the inserts performed by the Warehouse Proxy Agent with the most recent inserts sorted to be at the top of the list.
IZ00357	Some columns of type string shows up in the database with null characters at the end. When the database datatype is CHAR or NCHAR, the string should be space padded and should not contain null characters.
IZ00361	The WAREHOUSELOG and WAREHOUSEAGGREGLOG tables grow without bounds and require manual pruning to clean them up.
IY96376	HISTORY DATA CORRUPTION ON AGENT.AGENT ON BOX W/ MULTIPLE CPU
IY97589	BUG IN KFA HISTORICAL WRITER CAUSES HISTORY CORRUPTION.
IZ01917	S&P NOT ABLE TO SUMMARIZE TABLES WHICH CONTAINS GERMAN CHARS

Tivoli Universal Agent APARs

The following APARs are addressed in Fix Pack 6:

APAR Number	Symptom
IY92754	There is a problem with using the SCRIPT data provider when the script output is larger than 4096 bytes. It occurs whenever SCRIPT data provider experiences a failure trying to read STDERR. A UA trace log message appears that reads `"kumplscr.c,2097,"KUMP_LaunchScript") No stderr data read, possible noise on socket, errno = 0"` When this case occurs the subsequent attribute values are skewed and results are incorrect due to a loss of a partial data row. One or more of the attribute values could be incorrect.
IY95773	UA has signed integer limit of 32767, which causes no SNMP data to appear in Tivoli Enterprise Portal if UA is configured to use an alternate port number greater than 32767.
IY97733	UA computer's CPU usage hit 100%, and /opt filesystem filled due to runaway log file growth.
IZ00895	When Remote Deploy is used to push a Tivoli Universal Agent metafile to a remote UNIX system, a special non-interactive flag is passed to the um_console shell script. When the um_console script calls the Tivoli Universal Agent **kumpcon** program with empty input, the logic that waits/retries for console input gets into an infinite loop. As a result, the metafile cannot be successfully imported.
IY94600	When monitoring a large number of files using the FILE data provider, it is possible to have data rows received from one monitored file appear in another monitored file's report or table on a Tivoli Enterprise Portal workspace.

APAR Number	Symptom
IY96550	The omission of some SNMP traps from the UA's SNMP Trap Emitter is likely to happen when there are bursts of multiple trap emits at the same time, where same time is a lapse of 1 to N secs. It is unpredictable as to how many trap emits are lost, and it is not possible to specify how many concurrent trap emits are required to constitute the ″burst″ phenomenon. Both the customer experience and the L3 recreate environments produced ″burst″ of as many as 200+ trap emits in a 3 seconds time span, resulting in loss of SNMP trap emits. A typical customer experience of this problem is N number of IBM Tivoli Monitoring situations firing as true, where each true event triggers a SNMP trap to be emitted. Yet, when reviewing the SNMP traps received by customer's SNMP Manager there are less than N traps that were received. Some of the triggered trap emits failed to actually emit, thus they were never received. This problem is not restricted to any specific platforms.
IY93100	ITM 6.1 FP0004 KUMPSEND ALWAYS RETURN RC=0
IY95401	SPECIFYING AN INCORRECT LIST IN ″UM_CONSOLE LOADLIST...″
IY96688	WHEN IMPORTING MDL THAT WAS VALIDATED, GETS ERROR
IY96997	DERIVED ATTRIBUTE VALUE INCORRECT WHEN USING HIDDEN ATTRIBUTE
IY97274	SECURITY SCAN & SOCK/API DPS :DP-DCH PIPE BRKS, UA CONSUMES CPU
IY98702	NUMERIC ATTRS W/ SPACE/BLANK VALUE & CLEARVALUES DISPLAYS LARGE
IZ00454	UA:UNIX- NO DATA AFTER DELETED FILE RECREATED, IOLOCK BLOCKED

i5/OS monitoring agent APARs

The following APARs are addressed in Fix Pack 6:

APAR Number	Symptom
IY96974	OS400 OS AGENT DOES NOT STOP AND HANGS THE SYSTEM WHEN ENDSYS O
IY99792	QGYOLJOB (OPEN JOB LIST API) CALL USED IN I5/OS MONITORING

Linux OS monitoring agent APARs

The following APARs are addressed in Fix Pack 6:

APAR Number	Symptom
IZ00191	COMMAND LINE ATTRIBUTE ISN'T LISTED AT DISPLAY ITEM.
IZ00842	ABNORMAL SHUTDOWN OF LINUX OS AGENT - CRASHES WHILE
IZ00994	USER TO SYSTEM CPU PERCENTAGE NOT CORRECT.

UNIX OS monitoring agent APARs

The following APARs are addressed in Fix Pack 6:

APAR Number	Symptom
IY96272	IBM Tivoli Monitoring, version 6.1.0 of the UNIX OS agent currently limits the number of the process ID to be within a range of 0-999999. **Additional Information:** This results in limiting the value assigned to a situation associated with the process ID to a maximum value of 999999. For example, if the process ID is 1626243, the situation editor does not allow you to fill in this value. It displays in red and the situation cannot be saved.

APAR Number	Symptom
IY94878	IBM Tivoli Monitoring UNIX OS agent goes offline on AIX computers, when running at IBM Tivoli Monitoring Version 6.1.0 Fix Pack 3 (6.1.0-TIV-ITM-FP0003) or later.
IY95942	On some HP-UX systems, the IP address displays as 0.0.0.0 for Network Interface Cards that are bound to a Valid IP address.
IY94446	IBM Tivoli Monitoring HP-UX agent reports negative cpu values for user, busy and idle attributes when the numbers of cpu's are more than 32. **Additional Information:** You must set the environment variable KBB_HPUX_VMSTAT=TRUE to make the agent use the vmstat -n command to poll metrics for CPU data.
IY95495	Situation of file information does not fire. **Additional Information:** Situations associated with UNIX OS agent User_File attributes do not fire, when running at IBM Tivoli Monitoring Version 6.1.0 Fix Pack 4 (6.1.0-TIV-ITM-FP0004) or later.
IY93133	The summarized query for network data fails with ″SQL0802N Arithmetic overflow or other arithmetic exception occurred″ error message.
IY97367	KUX AGENT CRASHES WHEN IOSTAT SENDS DUPLICATE LINE FOR A DISK
IY97834	″PROCESSES FOR USER ID″ DOESN'T RESTRICT THE LIST OF PROCESSES
IY98240	ACTIVE VIRTUAL MEMORY VALUE INCORRECTLY REPORTED FOR HPUX
IY99555	ON SOLARIS, THE ITM UNIX O/S AGENT FILESYSTEM % USAGE REPORTED
IZ00355	PROBLEM DESCRIPTION: ITM 6.1 UNIX AGENT ON HP-UX MACHINES
IZ00800	AIX %SPACEUSED AND %INODES DATA IS NOT CORRECT
IZ00854	POST FP05, ″DISK USAGE″ WORKSPACE SHOWS THE FOLLOWING:
IZ01111	THE SIZES OF FILES MORE THAN 2 GB ARE DISPLAYED AS A NEGATIVE
IZ01748	UNIX OS FILE INFORMATION WORKSPACE INCORRECTLY SHOWS FILE ACCES

Windows OS monitoring agent APARs

The following APARs are addressed in Fix Pack 6:

APAR Number	Symptom
IY96470	Fix Pack 4 required that the Windows OS monitoring agent have Java 1.4.2 to be installed.
IY94797	WINDOWS OS AGENT HANDLE LEAK
IY98502	MONITORED LOGS DATA APPEARS TO BE CORRUPTED

Appendix. Notices

This information was developed for products and services offered in the U.S.A. IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785 U.S.A.

For license inquiries regarding double-byte (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

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

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law:

INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION ″AS IS″ WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement might not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

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.

© Copyright IBM Corp. 2007

Such information may be available, subject to appropriate terms and conditions, including in some cases payment of a fee.

The licensed program described in this document and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement or any equivalent agreement between us.

Trademarks

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

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

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

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

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

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

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

Index

E

event synchronization
  installing from the command line 58
  installing using silent install 60
  installing with the wizard 57
  removing 62
  uninstalling 62

R

removing
  event synchronization 62

U

uninstalling
  event synchronization 62

© Copyright IBM Corp. 2007

Printed in USA

GI11-8125-00