Tivoli. IBM Tivoli Monitoring

Version 6.1

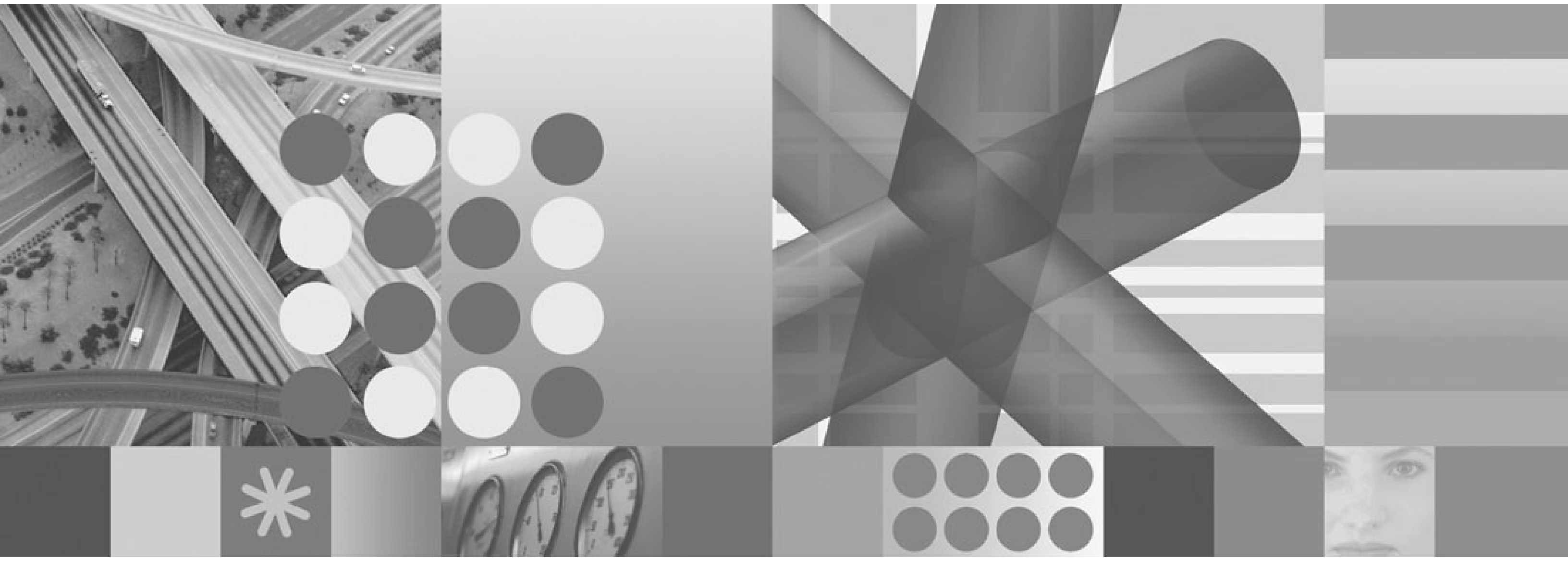
Fix Pack 7 Readme and Documentation Addendum

GI11-8885-00

Tivoli® IBM Tivoli Monitoring

IBM

Version 6.1



Fix Pack 7 Readme and Documentation Addendum

GI11-8885-00

Note

Before using this information and the product it supports, read the information in “Notices,” on page 131.

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

Contents

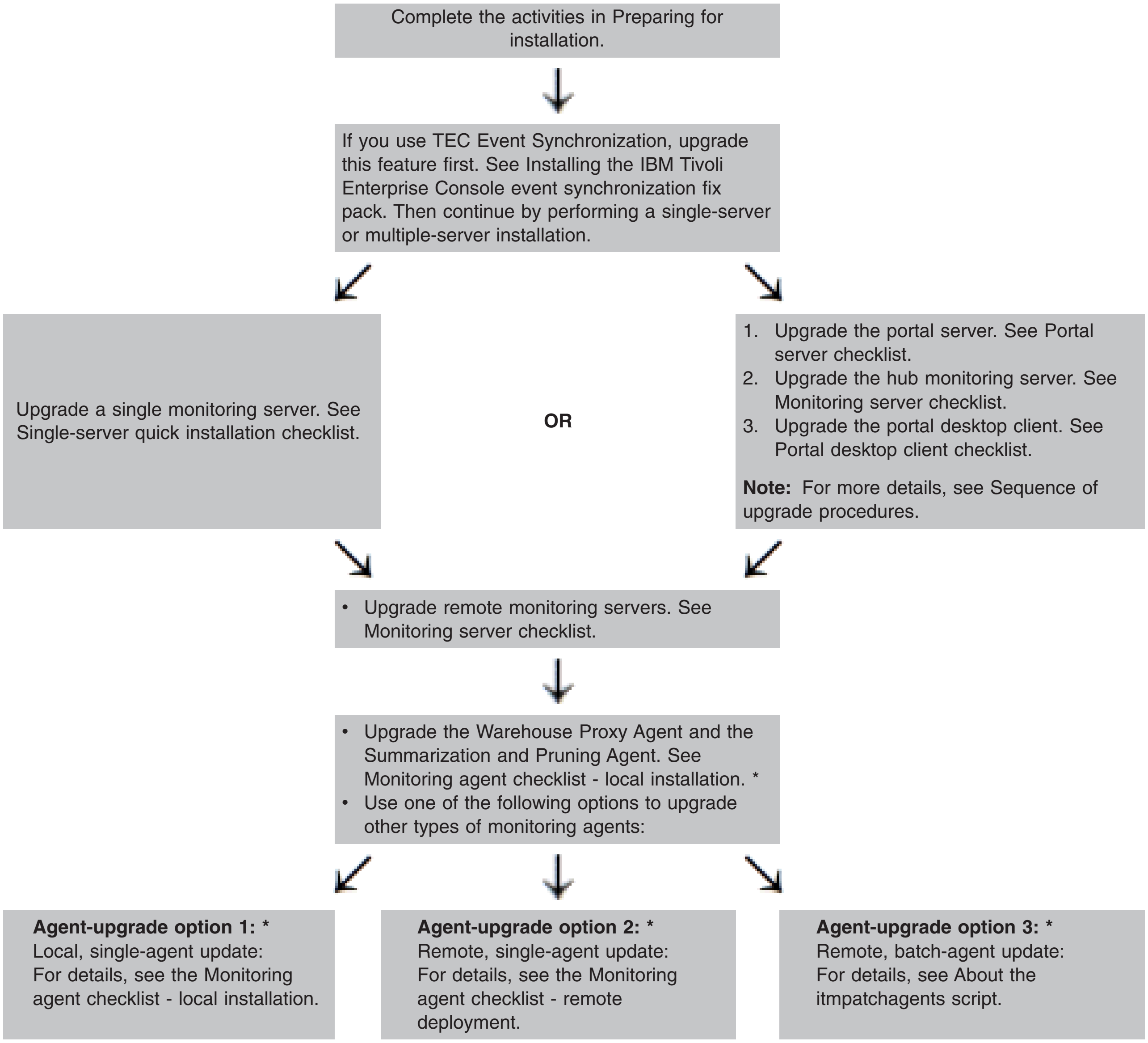
Figures

Tables

Chapter 1. Fix Pack 7 overview

Fix Pack 7 for IBM Tivoli Monitoring includes the fixes delivered in previous Version 6.1.0 fix packs plus additional fixes. This readme provides details about installing the fix pack and information about the changes that is makes to IBM Tivoli Monitoring. Chapter 6, “APARs addressed by Fix Pack 7,” on page 107 lists APARs that are fixed in Fix Pack 7 and in the interim fixes for Fix Pack 6.

The basic flow of the installation process to upgrade to Fix Pack 7 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 30. You must upgrade or install new components according to the sequence described in “Sequence of upgrade procedures” on page 13.



Complete the activities in Preparing for installation.

If you use TEC Event Synchronization, upgrade this feature first. See Installing the IBM Tivoli Enterprise Console event synchronization fix pack. Then continue by performing a single-server or multiple-server installation.

Upgrade a single monitoring server. See Single-server quick installation checklist.

OR

1. Upgrade the portal server. See Portal server checklist.
2. Upgrade the hub monitoring server. See Monitoring server checklist.
3. Upgrade the portal desktop client. See Portal desktop client checklist.

Note: For more details, see Sequence of upgrade procedures.

- Upgrade remote monitoring servers. See Monitoring server checklist.

- Upgrade the Warehouse Proxy Agent and the Summarization and Pruning Agent. See Monitoring agent checklist - local installation. *
- Use one of the following options to upgrade other types of monitoring agents:

Agent-upgrade option 1: *
Local, single-agent update:
For details, see the Monitoring agent checklist - local installation.

Agent-upgrade option 2: *
Remote, single-agent update:
For details, see the Monitoring agent checklist - remote deployment.

Agent-upgrade option 3: *
Remote, batch-agent update:
For details, see About the itmpatchagents script.

* Only the local agent-upgrade option (option 1) is valid for the monitoring agents that enable historical reporting.

Figure 1. Installation flow for upgrading a monitoring environment to Fix Pack 7

New in this fix pack

This section summarizes what is new in this fix pack:

- New operating system and database support.
- New Java Runtime Environment support for UNIX-based systems.

  Note: In response to APAR IZ04630, the product generates a message on the 64-bit AIX platform to explain how you can prevent out-of-memory conditions. See "Java out-of-memory errors on AIX" on page 80.
- Chapter 6, "APARs addressed by Fix Pack 7," on page 107 lists APARs that are fixed in Fix Pack 7 and in the interim fixes for Fix Pack 6.
- Improvements to reduce the size of and time of deployment for the Windows OS Agent (see APAR IZ03567).

  Note: *As a result of this change, for Windows deployment depots you must use the* **tacmd addBundles** *to update the Windows OS agent deployment bundle.* Also, the remote deployment of the Windows OS Agent no longer installs the Java 1.4.2 runtime environment on the target system, except for Windows 2000 targets in which case the JRE is still required for deployment. IBM Tivoli Monitoring application agents that require Java should include it as part of their deployment bundle. You should have the latest fix level of these agents (for example, Fix Pack 1 of "IBM Tivoli Monitoring for Databases") populated to your agent depot prior to a remote deployment.

About installation images

You can download the IBM Tivoli Monitoring, Fix Pack 7 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 7 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 7 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.

Note: An **MD5SUMS** checksum file is also available for download. You can use this file to confirm that a successful download has taken place.

Table 1. Fix Pack 7 file names

Category	Fix pack file name	Specific operating system (or application)
Windows®	6.1.0-TIV-ITM_TMV-Windows-FP0007.zip	Windows platforms

Table 1. Fix Pack 7 file names (continued)

UNIX®	6.1.0-TIV-ITM_TMV-AIX-FP0007.tar	UNIX platforms - AIX®
	6.1.0-TIV-ITM_TMV-HPUX-FP0007.tar	UNIX platforms - HP-UX Integrity, HP-UX native processors
	6.1.0-TIV-ITM_TMV-Solaris-FP0007.tar	UNIX platforms - Solaris
Linux®	6.1.0-TIV-ITM_TMV-LinuxIA64-LinuxX64-FP0007.tar	Linux on x86-64 and IA-64
	6.1.0-TIV-ITM_TMV-Linuxip-FP0007.tar	Linux on iSeries and on pSeries®
	6.1.0-TIV-ITM_TMV-Linuxz-FP0007.tar	Linux on zSeries®
	6.1.0-TIV-ITM_TMV-LinuxIA32-1-FP0007.tar[1]	Linux Intel® 32-bit platforms (Part 1 of 2)
	6.1.0-TIV-ITM_TMV-LinuxIA32-2-FP0007.tar[2]	Linux Intel 32-bit platforms (Part 2 of 2)
z/OS®	PTFs for the Tivoli Enterprise Monitoring Server on z/OS	z/OS
National languages other than English	6.1.0-TIV-ITM-LP-FP0007.tar	Language Pack - all platforms
	6.1.0-TIV-ITM-LP-FP0007.zip	Language Pack - Windows® platforms

Notes:

1. To upgrade all components except for Tivoli Enterprise Portal Server.
2. To upgrade a Tivoli Enterprise Portal Server.*

   * 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 on page 2:

- **Software prerequisites for installation of the language pack for Fix Pack 7:** Prerequisite software is required when you want to install the language pack for Fix Pack 7 (**6.1.0-TIV-ITM-LP-FP0007**):
  – IBM Tivoli Monitoring V6.1.0 (including Fix Pack 7)
  – IBM Tivoli Monitoring V6.1.0 FP4 Language Pack

    OR

    IBM Tivoli Monitoring 6.1-CER-Language Pack

  Note: The items that are listed in the preceding bulleted list must be installed before you install the language pack for Fix Pack 7.
- If you are running your monitoring server on a z/OS system, apply the z/OS Fix Pack 7 PTFs, available from IBM Software Support. See the “Monitoring server checklist” on page 34 for more information.
- If you are running OMEGAMON® XE products and plan to upgrade to IBM Tivoli® Monitoring version 6.1 Fix Pack 7, 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 12 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 25 for detailed installation procedures.

Supported operating systems

Fix Pack 7 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 7 is marked **New**.

For the latest OS support information, see http://www-1.ibm.com/support/docview.wss?rs=203 &uid=swg21067036.

Note: Shaded and unshaded rows are provided in the table as a visual cue to distinguish the different platforms.

Table 2. Supported Windows operating systems for IBM Tivoli Monitoring V6.1 Fix Pack 7 monitoring components

Operating system	OS monitoring agent[2]	Monitoring server	Portal client[1]	Portal server	WPA [3]	SPA[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)	X	X	X	X	X	X
Windows 2003 EE (64-bit)	X	X	X	X	X	X
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			
Windows 2008 (32-bit)	New[5]		New[6]			

Notes for Table 2:

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 12. 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. WPA stands for Warehouse Proxy Agent. SPA stands for 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, so that you are aware of any revisions regarding this platform.
5. For Windows 2008 monitoring agents, the remote installation of other agents using the **tacmd addSystem** command should not be used. Only local installation is supported.

CREATENODE? should be used? Only local installation (silent or GUI) is supported; that's the key issue.

6. Only the browser client is supported. The desktop client is not supported.

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

Note: Shaded and unshaded rows are provided in the table as a visual cue to distinguish the different platforms.

Table 3. Supported UNIX, i5/OS, and z/OS operating systems for IBM Tivoli Monitoring V6.1 Fix Pack 7 monitoring components [10]

Operating system	OS monitoring agent[1, 2]	Monitoring server	Portal client	Portal server	WPA [9]	SPA[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
AIX V6.1	New	New		New	New	New
Solaris Operating Environment V8 (SPARC)	X	X				X
Solaris V9 (SPARC)	X	X				X
Solaris V10 (SPARC)	X	X				X
Solaris V10 (x86-64) x86-64 refers to a 64-bit system running on AMD64/EM64t.	X	X				
Solaris Zones	X[4, 5]	X[4]				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]	X	X			X	X
HP-UX 11i v3 (B.11.31) on Integrity (IA64)	X	X			X	X
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				
z/OS 1.9[8]	X	X				

Notes for Table 3:

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 12. 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. 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. WPA stands for Warehouse Proxy Agent. SPA stands for Summarization and Pruning agent
10. During the installation of ITM 6.1 on UNIX-based systems, you might not see an option for a platform that is officially listed as supported. Refer to Technote 1303680 for information about installing the product on UNIX-based systems:http://www-1.ibm.com/support/docview.wss?uid=swg21303680

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

Note: Shaded and unshaded rows are provided in the table as a visual cue to distinguish the different platforms.

Table 4. Supported Linux operating systems for IBM Tivoli Monitoring V6.1 Fix Pack 7 monitoring components

Operating system	OS monitoring agent[1, 5]	Monitoring server	Portal client	Portal server	WPA [6]	SPA[6]
Asianux 2.0 for Intel 32	X	X	X	X	X	X
Asianux 2.0 for x86-64 x86-64 refers to a 64-bit system running on AMD64/EM64t.	X					
Asianux 2.0 on Itanium® 64	X					
Red Flag 4.1 for Intel 32-bit systems	X	X	X	X	X	X
Red Flag 5.0 for Intel 32-bit systems	X	X	X	X	X	X
RHEL[9] 2.1 Intel 32-bit systems	X					X
RHEL 3 on Intel 32-bit systems	X				X	X
RHEL 3 on zSeries 31-bit or 64-bit	X				X	X
RHEL 4 Intel 32-bit systems	X	X	X	X	X	X
RHEL 4 on x86-64 x86-64 refers to a 64-bit system running on AMD64/EM64t.	X					

Table 4. Supported Linux operating systems for IBM Tivoli Monitoring V6.1 Fix Pack 7 monitoring components (continued)

Operating system	OS monitoring agent[1, 5]	Monitoring server	Portal client	Portal server	WPA [6]	SPA[6]
RHEL 4 on Itanium 64-bit	X					
RHEL 4 on iSeries® and pSeries	X					
RHEL 4 on zSeries 31-bit or 64-bit	X	X[3]		X[3, 4]	X	X
RHEL 5 Intel 32-bit systems[7]	X[8]	X	X	X	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 or 64-bit[7]	X[8]	X[3]		X[3, 4]	X	X
SLES[9] 8 Intel 32-bit systems	X				X	X
SLES 8 for zSeries 31-bit or 64-bit	X				X	X
SLES 9 Intel 32-bit systems	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 or 64-bit	X	X[3]		X[3, 4]	X	X
SLES 10 Intel 32-bit systems	X[8]	X	X	X	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[9]	X[8]	X[3]		X[3, 4]	X	X

Notes for Table 4 on page 6:

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 12. 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 four 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. WPA stands for Warehouse Proxy Agent. SPA stands for Summarization and Pruning agent
7. This environment is supported only when operating system settings for SELinux Security and Firewall Security are set to disabled.
8. SLES refers to SUSE Linux Enterprise Server. RHEL refers to Redhat Enterprise Linux.
9. See Technote 1247529 for further information on support for this operating system: http://www-1.ibm.com/support/docview.wss?uid=swg21247529.

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 the Tivoli Platform and Database Support Matrix: http://www-1.ibm.com/support/docview.wss?rs=203&uid=swg21067036; refer to the "Database Support" tab in the spreadsheet that is provided.

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	—
Linux[5]	V8.1, with Fix Pack 10 or higher fix packs V8.2 with Fix Pack 3 or higher fix packs V9.1	—
Windows	V8.1, with Fix Pack 10 or higher fix packs V8.2 with Fix Pack 3 or higher fix packs V9.1[6] V9.5 **Attention:** On the 64-bit version of Windows 2003, you must install and use a 32-bit version of DB2 8 or DB2 9 on the portal server.	MS SQL 2000 EE SP3

Notes regarding Table 5:

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. However, support for the Tivoli Enterprise Portal Server on a 64-bit operating system is limited. See “Supported operating systems” on page 3 for full details. For example, the portal server is supported on zSeries servers that run the 64-bit Linux operating system. However, the portal server is not supported on xSeries (Intel-based architecture) servers that run the 64-bit Linux operating system. Also, refer to the limitations referenced in item 5 and item 6 in this list.
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.
6. As mentioned in APAR IZ15450, you must install this version of DB2 in 32-bit mode when the portal server runs on a 64-bit Windows operating system.

Table 6 on page 10 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 • AIX V6.1 • 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 9.	MS SQL 2000 EE, SP3 MS SQL 2005, only when the portal server runs on Windows.	Supported versions: • V9.2, 10g Release 1 • V9.2, 10g Release 2 • V9.2, 11g 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 regarding Table 6:

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 Fix Pack 2 for the Tivoli Data Warehouse. Use of DB2 V9 Fix Pack 2 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. See Technote 1240452 for further information on support for this application.

Chapter 2. Planning the installation of the fix pack

The information in this chapter helps you plan the installation of Fix Pack 7. The following table outlines the issues to consider as you plan the installation.

Table 7. Overall planning steps for Fix Pack 7

Goal	Where to find information
Determine which components must be upgraded.	"Determining which components need to be upgraded to Fix Pack 7"
Gather the information you need to perform the installation.	"Fix pack installation planning worksheets" on page 15
Learn how to preserve your customization.	"Preserving user customizations" on page 18
Understand how the autostart script works.	"Changes in the behavior of the autostart scripts on UNIX platforms" on page 21
Understand issues about the Windows versions of general availability (GA) CDs.	"Using the original versions of the IBM Tivoli Monitoring version 6.1 agent CDs for Windows platforms" on page 22

Determining which components need to be upgraded to Fix Pack 7

This section helps you determine on which components to install Fix Pack 7. 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
- "Sequence of upgrade procedures" on page 13

General guidelines for upgrading components

The following guidelines can help you plan deployment of Fix Pack 7:

- **Fix Pack 7 and monitoring servers.** It is a best practice to apply Fix Pack 7 to all monitoring servers in your environment. However, you can perform the upgrade over a period or several days. The older versions of the server are compatible with Fix Pack 7.
- **Fix Pack 7 and base monitoring agents.** The following points apply to base monitoring agents:
  - It is recommended that you upgrade base monitoring agents with Fix Pack 7.

    The more recent versions of the application monitoring agents are *compatible* with an IBM Tivoli Monitoring environment that you upgrade to Fix Pack 7. ("Base versus application monitoring agents" on page 12 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 7. See the last Note in this list.
  - Base monitoring agents that are upgraded to fix packs prior to Fix Pack 7 are supported by Fix Pack 7. See the last item in this list.
  - To learn whether Fix Pack 7 adds a required fix or feature to your base monitoring agents, review Chapter 6, "APARs addressed by Fix Pack 7," on page 107, including "Tivoli Enterprise Monitoring Agent APARs" on page 112 subsection.
  - The best practice is to upgrade all base monitoring agents to Fix Pack 7.
- **Fix Pack 7 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 7.
- **Fix Pack 7 and application monitoring agents.** "Base versus application monitoring agents" on page 12 explains the basic differences among agents.

- **Fix Pack 7 and the Warehouse Proxy Agent and the Summarization and Pruning Agent.** See “Historical data collection issues” on page 98.

Determining which components are present on a specific computer

In the “Fix pack installation planning worksheets” on page 15 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 a 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 7.
  2. Refer to the list while you are installing Fix Pack 7, to ensure that all components are upgraded.

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 7 upgrade described in this document.

Sequence of upgrade procedures

The installation sequence described here 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

The best practice (upgrade the hub Tivoli Enterprise Monitoring Server first; then upgrade the Tivoli Enterprise Portal Server; and then upgrade the remote Tivoli Enterprise Monitoring Server):

First: Hub Tivoli Enterprise Monitoring Server

Second: Tivoli Enterprise Portal Server

Third: Remote Tivoli Enterprise Monitoring Server

In an environment where the hub Tivoli Enterprise Monitoring Server and Tivoli Enterprise Portal Server are installed on the same distributed system, upgrade both in one upgrade session, as described in “Single-server quick installation checklist” on page 31.

In an environment where that the hub Tivoli Enterprise Monitoring Server and Tivoli Enterprise Portal Server are installed on different systems, upgrade the Tivoli Enterprise Portal Server soon after you upgrade the hub Tivoli Enterprise Monitoring Server. In environments that consist of at least one z/OS monitoring server or z/OS monitoring agent, the upgrade sequence remains the same, although the upgrade procedure requires additional planning and preparation, as described in this section.

Details regarding sequencing

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

Note: While IBM Tivoli Monitoring tolerates some components running with older versions of code, IBM recommends that you upgrade all of your IBM Tivoli Monitoring components to the same fix pack level.

Table 8. Sequence of fix pack upgrade activities

Component to upgrade	Details
1. **TEC Event Synchronization**	*TEC Event Synchronization users only.* See “Installing the IBM Tivoli Enterprise Console event synchronization fix pack” on page 54.
2. **Portal server**	Install Fix Pack 7 on the Tivoli Enterprise Portal Server, which runs only in a distributed computing environment or on a zLinux system. (Linux for zSeries is considered a distributed operating system, even though it runs in a mainframe environment. See “Supported operating systems” on page 3 for details regarding what components run on which operating systems.)

Table 8. Sequence of fix pack upgrade activities (continued)

Component to upgrade	Details
3. **Hub monitoring server**	• For a *distributed* hub monitoring server, apply Fix Pack 7 to the hub monitoring server. Follow the instructions that are provided in this readme. • For a *mainframe* hub monitoring server, apply the Program Temporary Fixes (PTFs) for Fix Pack 7 to the existing consolidated software inventory (CSI) for IBM Tivoli Monitoring, Version 6.1. A link to the PTFs is provided after this table. Be sure to follow any instructions provided in the ++HOLD text. See *z/OS Notes* following this table.
4. **Distributed remote monitoring servers**	Apply Fix Pack 7 to any remote monitoring servers that manage agents that you want to upgrade.
5. **Mainframe remote monitoring servers**	Apply the PTFs for Fix Pack 7 to the existing CSI for IBM Tivoli Monitoring, Version 6.1. Be sure to follow any instructions provided in the ++HOLD text. (You could have upgraded the remote monitoring server to Fix Pack 7 with the hub monitoring server in Step 2, if they exist in the same CSI.) See *z/OS Notes* following this table.
6. **Distributed agents**	Upgrade monitoring agents, including the Warehouse Proxy Agent and Summarization and Pruning agent that enable data warehousing with IBM Tivoli Data Warehouse. Consult the list of fixed APARs and other information in this readme to confirm which other agents that you want to upgrade. (You could have upgraded distributed agents to Fix Pack 7 when you upgraded the distributed monitoring server and portal server in Step 2, 3, or 4 above.) **Note:** Before you upgrade a monitoring agent, you must upgrade the monitoring server (remote or hub) to which the agent reports.
7. **Mainframe agents**	Apply the PTFs for Fix Pack 7 to the existing CSI for IBM Tivoli Monitoring, Version 6.1. Be sure to follow any instructions provided in the ++HOLD text. (You could have upgraded the agents with the mainframe monitoring server in Step 2 or 5 above, if they exist in the same CSI and the same runtime environment.) **Note:** Before you upgrade a monitoring agent, you must upgrade the monitoring server (remote or hub) to which the agent reports. The PTFs for Fix Pack 7 upgrades the basic services supporting the interactions between z/OS agents and monitoring server. See *z/OS Notes* following this table.
8. **Other components**	Install the fix pack for other components, as needed. For example, Fix Pack 7 provides a new language pack to resolve problems in non-English environments.

z/OS Notes:

1. You apply the PTFs for Fix Pack 7 to the mainframe components. A link to the PTFs is provided in *Platform Maintenance Tables*, Technote 7008514: http://www-1.ibm.com/support/docview.wss?rs=203&uid=swg27008514. Additional recommendations are provided in *Recommended Maintenance Service Levels for OMEGAMON XE products on ITM V6.x*, Technote 1290324: http://www-1.ibm.com/support/docview.wss?rs=2366&uid=swg21290324.
2. If a z/OS monitoring server (either a hub or a remote server) that you plan to upgrade has an OMEGAMON XE on z/OS monitoring agent running in its address space, complete the following tasks:
   a. Upgrade at one time all monitoring servers that are defined as sysplex proxies or that are eligible to serve as sysplex proxies. (A sysplex proxy monitoring server is a data consolidation point for sysplex monitoring.)
   b. Upgrade to V4.1.0 or higher any OMEGAMON XE on z/OS monitoring agents that are configured in the hub monitoring server, and in each of the remote monitoring servers you upgraded in Step 2a (that is, the proxy and proxy-eligible monitoring servers).
3. Check the Preventive Services Planning (PSP) bucket and apply current maintenance to any monitoring agents that remain at the V3.1.0 level after the monitoring server to which they connect is upgraded to the V6.1 Fix Pack 7 level.

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.

You perform some of the operations that are listed in Table 9 on page 16 in the Manage Tivoli Enterprise Monitoring Services window. Launch the window as follows:

- **On Windows:** Click the Windows **Start** button and select **Programs > IBM Tivoli Monitoring > Manage Tivoli Monitoring Services**.
- **On UNIX or Linux:**
  1. Use the following command to navigate to the **bin** directory: `cd itm_home/bin`.
  2. Run the following command: `./itmcmd manage [-h itm_home]` where *itm_home* is the optional specification for the product installation directory.

  See the *IBM Tivoli Monitoring Installation and Setup Guide* for detailed information on this command.

Table 9. 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 Services	“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 Services	“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 Services	“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 Services	“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 Services	“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 Services	“Monitoring server checklist” on page 34	
Host name of portal server: ______________________________ OS: __________________________	Monitoring server Portal desktop client Warehouse Proxy S&P Agent*	Manage Tivoli Enterprise Monitoring Services	“Portal server checklist” on page 37	

Table 9. Fix pack planning worksheet (continued)

<table>
<tr><td colspan="5"><b>IBM Tivoli Monitoring installation directory (CANDLEHOME environment variable):</b>
<b>Note:</b> This directory is referred to as <i>itm_home</i> in this document.</td></tr>
<tr><td colspan="5"><b>Fix pack installation directory (where you extract the fix pack files):</b>
<b>Note:</b> This directory is referred to as <i>patch_dir</i> in this document.</td></tr>
<tr><th>Host name: ____________________
Host operating system (OS): ______</th><th>Other components also installed on this computer (circle those that apply)</th><th>Where to obtain this information</th><th>When this information is used</th><th>Notes</th></tr>
<tr><td>Portal desktop client locations:
______________________________</td><td>Monitoring server
Portal server
Warehouse Proxy
S&P Agent*</td><td>Manage Tivoli Enterprise Monitoring Services</td><td>“Portal desktop client checklist” on page 40</td><td></td></tr>
<tr><td>Warehouse Proxy agent location:
______________________________</td><td>Monitoring server
Portal server
Portal desktop client
S&P Agent*</td><td>Manage Tivoli Enterprise Monitoring Services</td><td>“Monitoring agent checklist - local installation” on page 41</td><td></td></tr>
<tr><td>Warehouse S&P Agent* location:
______________________________</td><td>Monitoring server
Portal server
Portal desktop client
Warehouse Proxy</td><td>Manage Tivoli Enterprise Monitoring Services</td><td>“Monitoring agent checklist - local installation” on page 41</td><td></td></tr>
<tr><td>Agent types to update (product codes):
______________________________</td><td></td><td><b>tacmd listSystems</b></td><td>“Monitoring server checklist” on page 34
“Monitoring agent checklist - local installation” on page 41</td><td></td></tr>
<tr><td colspan="5">* Summarization and Pruning Agent</td></tr>
</table>

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. Also see the following related topic: “Overview of product behavior with custom configuration settings” on page 20.

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 *itm_home*\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 74 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.

- **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

The **Manage Scripts** feature in the Tivoli Enterprise Portal has a set of built-in scripts that manage 3270 terminal session navigation. These built-in functions persist after you install Fix Pack 7. However, you must save the custom scripts that you define for the navigation of 3270 terminal sessions. The *IBM Tivoli Monitoring User's Guide* describes this feature.

You must not modify the following types of files because they are 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 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/*temsname*/*.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/*temsname*/KBBENV
- *itm_home*/config/.ConfigData/*hostname*_ms_*temsname*.config.

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

Overview of product behavior with custom configuration settings

This section provides an overview of product behavior regarding custom configuration settings.

Before you upgrade to Fix Pack 7

It is advisable to back up your IBM Tivoli Monitoring environment, especially if you have a more complicated environment. Most large companies have a standard process for preserving a backup image of all computer systems, including the IBM Tivoli Monitoring environment. If your company does not have a process or you do not want to use that process for the Fix Pack 7 upgrade process, use the procedure that is provided in “Backing up IBM Tivoli Monitoring” on page 28.

General operations

Several types of variables control the operation of IBM Tivoli Monitoring component. The basic types are as follows:

- **User-modified variables:** Users generate these settings while doing a configuration in UNIX or Windows, changing a value in the CLI or GUI configuration GUIs, and then saving the changes. These are user-modifiable variables, and are typically stored in initialization (`*.ini`) files on the disk using variables, like **key=$VAR1$**, which are then substituted with the value that the user specifies.
- **System variables:** The second type of setting is a variable for an internal component that you cannot configure through the common configuration tools. These variables are stored in `*.ini` files, in entries like **NUM_TIMES_TO_TRY=4**. No dynamic substitution takes place. This type of setting is static.

The following list describes persistence in several scenarios:

- During upgrade from one version of a component to another, the user-modified variables are always persisted with the installation values that are set through the configuration tools.
- If a user modifies these values by hand, for example *adding* a new value to the end of an existing **VR** value, that new value is not persisted.
- The static values for the system are typically not persisted because they are internal component variables, and not typically exposed to the user for configuration. These static variables are not documented. In most cases, they should not be changed. Changing these values without instructions from a technote or IBM Software Support could lead to unpredictable results. To ensure stability of the system, the default values are restored when you upgrade to a new component version level.

  Although these variables normally are not persisted, a variable that you add that does not already have a key is persisted. This type of value is usually created under the guidance of IBM Software Support.

Specific details

On Windows and UNIX, the parameters are preserved through the following distinct conventions:

For UNIX

An `*.ini` file has a single line that starts with `@preserved`. After that line keys are listed that are considered preserved in that file. Be aware that the `@preserved` line itself might not persist the merged file after an upgrade, but the line is always present after a fresh installation of the product.

For Windows

Both the `*.ini` file and the ENV file contain variables that are preserved.

- In the Windows `*.ini` file, all variables in the `[Override Local Settings]` section are preserved. Nothing outside this section is preserved.
- In the ENV file **variable=value**, the same information is kept, unless upgrading from a previous Candle release. In that case, no values are preserved. For example, ENV variables up to the following divider are preserved:

```
*****  ADDED BY CONFIGURATION PROGRAM: DO NOT EDIT BELOW THIS POINT! *****
```

Nothing after this line is preserved.

Keep notes about any changed static variables that you modify in response to instructions from technotes, IBM Software Support, and so on. After performing an upgrade, examine whether the values need to be reapplied.

Overriding configuration values

Advanced users can apply override values to component customization. This method ensures that values are retained during upgrade. You should test this method in your environment before applying it globally:

Overrriding configuration values on UNIX-based systems

To learn about overriding configuration values on UNIX-based systems, contact IBM Software Support.

Overrriding configuration values on Windows systems

1. Select the monitoring agent that you want to update in the Manage Tivoli Enterprise Monitoring Services window.
2. Right-click and select **Advanced > Edit Variables**.
3. Click **Add**.
4. Select **KDC_FAMILIES** from the pull-down list of variables. The `@Protocol@` value is displayed in the **Value** field.
5. Append `IP.PIPE SKIP:15` to the current value. The resulting string is `@Protocol@ IP.PIPE SKIP:15`.
6. Click **OK**.
7. Click **OK** again.

Changes in the behavior of the autostart scripts on UNIX platforms

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. “Sample output for the cinfo command (for UNIX or Linux)” on page 50 includes 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) are not preserved and are overwritten the next time that you configure an application, or install or upgrade an application.
2. Any changes made to the AutoRun.sh script are not preserved and are overwritten the next time you apply higher maintenance.

Using the original versions of the IBM Tivoli Monitoring version 6.1 agent CDs for Windows platforms

Do not install the CDs for IBM Tivoli Monitoring version 6.1 agent that were originally released for the Windows operating system into an IBM Tivoli Monitoring version 6.1 Fix Pack 7 environment. Do not use the CDs 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 7.

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 7 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 output for the KINCINFO command. See "Sample output for the kincinfo command (for 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 7 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 7 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 7 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 7 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. When 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 10 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 “Sequence of upgrade procedures” on page 13.

Table 10. Overall installation steps for Fix Pack 7

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 27
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 30
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 52

Notes:

1. Because of increases in the size of product components, support for Linux Intel platforms is split into two files. See Table 1 on page 2 for the fix pack file that you must use for upgrading the IBM Tivoli Monitoring components.
2. If your Warehouse Proxy agent or Summarization and Pruning agent are on computers other than the monitoring server or portal server, use the instructions in the “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 7 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 "Sequence of upgrade procedures" on page 13.
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 11.

Table 11. Installation and startup log file names and locations

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

While starting a component	• For the Tivoli Enterprise Portal:
	`itm_home\CNP\logs\kcjerror.log`
	`itm_home\CNP\logs\kcjras1.log`
	• For errors with distributed Tivoli Enterprise Monitoring Agents:
	`itm_home\TMAITM6\logs\hostname_pc_key.log`
	• For errors on the Tivoli Enterprise Portal Server, Tivoli Enterprise Monitoring Server, or warehouse proxy agent:
	`itm_home\logs\hostname_pc_key.log`
	where *hostname* is the hostname of the computer where the component is running, *pc* is the two-letter product code, and *key* is a hexadecimal identifier. Refer to the product code appendix in the *IBM Tivoli Monitoring: Installation and Setup Guide* for a list of product codes or to the output for the `kincinfo` command. See "Sample output for the kincinfo command (for 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.

(*Optional*) Disabling the forwarding of events to IBM Tivoli Enterprise Console

If event forwarding to IBM Tivoli Enterprise Console is enabled while you install a fix pack for IBM Tivoli Monitoring, you might see messages regarding the temporarily inactive status of the IBM Tivoli Monitoring environment. You have the option to disable event forwarding by reconfiguring the hub Tivoli Enterprise Monitoring Server in the Manage Tivoli Enterprise Monitoring Services window, as follows:

1. Right-click the row for the hub server.
2. Select **Reconfigure** in the pop-up menu. The **Tivoli Enterprise Monitoring Server Configuration** dialog box is displayed.
3. Deselect the **Tivoli Event Integration Facility** option and click **OK**. The **Hub TEMS configuration** dialog box is displayed.
4. Click **OK**. Your settings are applied, and event forwarding stops.

After installation of the fix pack, be sure to restore event forwarding by repeating these steps and *selecting* the **Tivoli Event Integration Facility** option. See *IBM Tivoli Monitoring Installation and Setup Guide* for complete information on the Tivoli Event Integration Facility.

Permissions

If you are installing the fix pack on Linux or UNIX computers, and you installed the IBM Tivoli Monitoring components (both the base monitoring components like the monitoring server and any monitoring agents) as a non-root user, you must perform the following steps to ensure that the user who installs the fix pack has the appropriate permissions:

Note: *ITMinstall_dir* is the installation location for IBM Tivoli Monitoring and *user_id* is the ID that was used to install the IBM Tivoli Monitoring components.

1. Log in to the computer as *user_id*.
2. Run the following command to change ownership of root owned files modified by **SetPerm** previously back to *user_id*:
   ```
   su - root -c "itm_home/bin/UnSetRoot user_id"
   ```
3. Install the fix pack on the computer, following the steps outlined in the checklists.
4. Run the following command to reset the file permissions and file ownership as required:
   ```
   su - root -c "itm_home/bin/SetPerm -a"
   ```

Daylight Savings Time Information

Annual Daylight Savings Time (DST) issues in the Fall season : 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. The document describes the potential side effects and the recommended corrective actions.

If you have not done so already, adapt your system and the product set to **daylight savings time** (DST) changes. 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.

The Java Runtime Environment that IBM Tivoli Monitoring uses may require timezone updates depending on your time zone and country. Details on which updates are available for IBM provided JREs got to the following URL: http://www-1.ibm.com/support/docview.wss?rs=3068&context=SSNVBF&uid=swg27008911

IBM Tivoli Monitoring version 6.1 Fix Pack 7 provides the following **tzdata** levels with the JRE update provided with this fix pack:

```
Linux or Unix IBM JRE Service Release 9:  tzdata2007f
Windows IBM JRE Service Release 8:        txdata2007c
```

For upgrade installs on Windows platforms, you must select the Upgrade IBM JAVA option in order for the installer to upgrade the Java software. If you do not choose the **Upgrade IBM JAVA** option and have not patched your current JRE using the JTZU utility referenced in the ″Urgent Actions..″ URL that is provided above, you might be missing needed DST updates. New installations since ITM Tivoli Monitoring version 6.1 Fix Pack 5 have the following JRE update:

```
FP5 Windows, Linux, and UNIX: tzdata2007a
FP6 Linux and Unix:           tzdata2007a
FP6 Windows:                  tzdata2007c
```

On UNIX-based platforms, Version 1.4.2 service release 9 (SR9) of the JRE is recommended because it has been confirmed to resolve numerous JRE-related PMRs.

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 of this procedure, you record the current configuration settings. In Step 9 on page 30, 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 on page 29.

   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 12. 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 15. 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 9
	2. Based on the platform of your local host computer, download and extract the required fix pack files to a temporary location on your computer. You can use the following space to write down the location of your patch directory. **Patch directory:** ________________________________

Table 12. Checklist for a new (non-upgrade) installation (continued)

✓	Installation step
	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 11 on page 26 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.) **Note:** If you install the fix pack in an language environment other than English, see "Software prerequisites for installation of the language pack" on page 3. The name of the installation image is **6.1.0-TIV-ITM-LP-FP0007**. 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*.

Limitation: 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

Use this checklist only if you have the following components installed on the same system:

- Tivoli Enterprise Monitoring Server

  Note: Only hub monitoring servers support SOAP servers.
- Tivoli Enterprise Portal Server
- Tivoli Enterprise Portal desktop client

Note: You can directly upgrade from any previous IBM Tivoli Monitoring V6.1.0 Fix Pack to Fix Pack 7. After the upgrade you must use the component software from Fix Pack 7 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 “Comparing installation processes for Fix Pack 3 (or earlier) and Fix Pack 7” on page 83.

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

✓	**Installation step**
	1. Gather information about the monitoring components in your environment. See “Fix pack installation planning worksheets” on page 15.
	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. On Windows, select from the list 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. . 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*.
	4. On Linux and UNIX computers, reapply application support on your local monitoring server. (The command line method is described here. Alternatively, you can use an installer to apply application support as described in the *IBM Tivoli Monitoring Installation and Setup Guide*; see the "Installing and enabling application support" section. 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 33 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`

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

✓	**Installation step**
	6. If the installation of this component fails, refer to the installation logs found in Table 11 on page 26 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 7. 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.) **Note:** If you install the fix pack in an language environment other than English, see "Software prerequisites for installation of the language pack" on page 3. The name of the installation image is **6.1.0-TIV-ITM-LP-FP0007**. 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 the components that 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 14. The process for updating a monitoring server on z/OS is shown in Table 15 on page 36.

Note: You can directly upgrade from any previous IBM Tivoli Monitoring V6.1.0 Fix Pack to Fix Pack 7. After the upgrade you must use the component software from Fix Pack 7 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 “Comparing installation processes for Fix Pack 3 (or earlier) and Fix Pack 7” on page 83.

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

✓	**Installation step**
	1. Gather information about the monitoring components in your environment. See “Fix pack installation planning worksheets” on page 15.
	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 14. 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 14. 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. (The following topic describes various options for installing application support: http://publib.boulder.ibm.com/infocenter/tivihelp/v15r1/topic/com.ibm.itm.doc_6.1/itm_install108.htm#agent_support 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 33 describes key parameters for the command. **Attention:** Do not reapply application support for any agent that is 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 7. 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.) **Note:** If you install the fix pack in an language environment other than English, see “Software prerequisites for installation of the language pack” on page 3. The name of the installation image is **6.1.0-TIV-ITM-LP-FP0007**. 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 11 on page 26 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 7 • “General guidelines for upgrading components” on page 11 • “Determining which components are present on a specific computer” on page 12 • “Sequence of upgrade procedures” on page 13

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

Table 15. Checklist for installing the fix pack on the 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 15.
	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 7. Select each of the levelset PTFs and install it using the typical z/OS SMP/E installation procedures.

Table 15. Checklist for installing the fix pack on the monitoring server on z/OS systems (continued)

✓	**Installation step**
	3. **Relink PTFs required for Fix Pack 7:** 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 7, 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 87.

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 7. After the upgrade you must use the component software from Fix Pack 7 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 "Comparing installation processes for Fix Pack 3 (or earlier) and Fix Pack 7" on page 83.

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

✓	**Installation step**
	1. Gather information about the monitoring components in your environment. See “Fix pack installation planning worksheets” on page 15.
	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. You must install application support. Specifically, you must respond as follows to a series of prompts from the installer:

- After you upgrade the Tivoli Enterprise Portal Server, the following prompt is displayed: `Do you want to install additional products or product support packages [ y or n; "n" is default ]?`

  You must respond **yes**.
- The list of available operating systems and component support categories is displayed. You must choose the number for the Tivoli Enterprise Portal Server support category and proceed to install the necessary application support packages.
- After you install the application support packages for the Tivoli Enterprise Portal Server, the following prompt is displayed: `Do you want to install additional products or product support packages [ y or n; "n" is default ]?`

  You must respond **yes**.
- The list of available operating systems and component support categories is displayed. You must choose the number for the Tivoli Enterprise Portal browser client support category and proceed to install the necessary application support packages.

b. On Windows computers, you must leave all of the items selected in the **Setup Type** window that is displayed during the installation process.

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.

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

✓	**Installation step**
	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 7. 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.) **Note:** If you install the fix pack in an language environment other than English, see “Software prerequisites for installation of the language pack” on page 3. The name of the installation image is **6.1.0-TIV-ITM-LP-FP0007**. 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 11 on page 26 for a description of installation problems.
	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 7” 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:
   - **On Windows:** *itm_home*`\cnps\WSFixupEventConsole` *server username password*
   - **On UNIX-based systems:** *itm_home*/bin/itmcmd execute cq ″WSFixupEventConsole.sh *server username password*″

   Note: The double quotation marks are required to correctly invoke this script.

   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 7. After the upgrade you must use the component software from Fix Pack 7 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 “Comparing installation processes for Fix Pack 3 (or earlier) and Fix Pack 7” on page 83.

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

✓	**Installation step**
	1. Gather information about the monitoring components in your environment. See “Fix pack installation planning worksheets” on page 15.
	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.

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

<table>
<tr><th>✓</th><th>Installation step</th></tr>
<tr><td colspan="2">**Notes:**
a. You must install application support. Specifically, you must respond as follows to a series of prompts from the installer:
• After you upgrade the Tivoli Enterprise Portal browser client, the following prompt is displayed: `Do you want to install additional products or product support packages [ y or n; "n" is default ]?`
You must respond **yes**.
• The list of available operating systems and component support categories is displayed. You must choose the number for the Tivoli Enterprise Portal browser client support category and proceed to install the necessary application support packages.
b. On Windows computers, you must leave all of the items selected in the **Setup Type** window that is displayed during the installation process.
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.</td></tr>
<tr><td></td><td>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 7. 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.)
Note: If you install the fix pack in an language environment other than English, see “Software prerequisites for installation of the language pack” on page 3.
The name of the installation image is **6.1.0-TIV-ITM-LP-FP0007**. 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*.</td></tr>
<tr><td></td><td>6. If the installation of this component failed refer to the installation logs found in Table 11 on page 26 for a description of installation problems.</td></tr>
<tr><td></td><td>7. Install the fix pack on the monitoring agents (local and remote).</td></tr>
</table>

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 7.
4. You can directly upgrade from any previous IBM Tivoli Monitoring V6.1.0 Fix Pack to Fix Pack 7. After the upgrade you must use the component software from Fix Pack 7 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 “Comparing installation processes for Fix Pack 3 (or earlier) and Fix Pack 7” on page 83.

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

✓	**Installation step**
	1. Gather information about the monitoring components in your environment. See “Fix pack installation planning worksheets” on page 15.
	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 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 7. 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.) **Note:** If you install the fix pack in an language environment other than English, see “Software prerequisites for installation of the language pack” on page 3. The name of the installation image is **6.1.0-TIV-ITM-LP-FP0007**. 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 11 on page 26 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.

Note: You can directly upgrade from any previous IBM Tivoli Monitoring V6.1.0 Fix Pack to Fix Pack 7. After the upgrade you must use the component software from Fix Pack 7 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 “Comparing installation processes for Fix Pack 3 (or earlier) and Fix Pack 7” on page 83.

Table 19. 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.

	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 `/fp7dir/aix`, the command to use is as follows:
	`tacmd addBundles -i /fp7dir/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:\fp7dir\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.

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

<table>
<tr><th>✓</th><th>Installation step</th></tr>
<tr><td></td><td>

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           06.10.07.00 Y
NM15.lab.ibm.com:LZ        LZ           06.10.07.00 Y
Primary:X3A30S8:NT         NT           06.10.07.00 Y
Primary:X3A30S13:NT        NT           06.10.07.00 Y
HUB_X3A30S13               EM           06.10.07.00 Y
apollo:KUX                 UX           06.10.07.00 Y
```

See the *IBM Tivoli Monitoring Command Reference* for additional command reference information.

</td></tr>
<tr><td></td><td>

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 45 for further information on the parameters.

</td></tr>
<tr><td colspan="2">

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.

</td></tr>
<tr><td></td><td>

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 7. 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.)
Note: If you install the fix pack in an language environment other than English, see “Software prerequisites for installation of the language pack” on page 3.

The name of the installation image is **6.1.0-TIV-ITM-LP-FP0007**. 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*.

</td></tr>
<tr><td></td><td>

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 11 on page 26 can also help you trace installation problems.

</td></tr>
</table>

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/*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 7," 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\061007000\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:

- 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

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
```

Adjusting timeouts for deployment operations

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*.

The `TIMEOUT` environment variable value that is specified in the Tivoli Enterprise Monitoring Server configuration file and the `TACMD_TIMEOUT` environment variable value are not related to the time that the **createnode** command waits for the installation of a managed system.

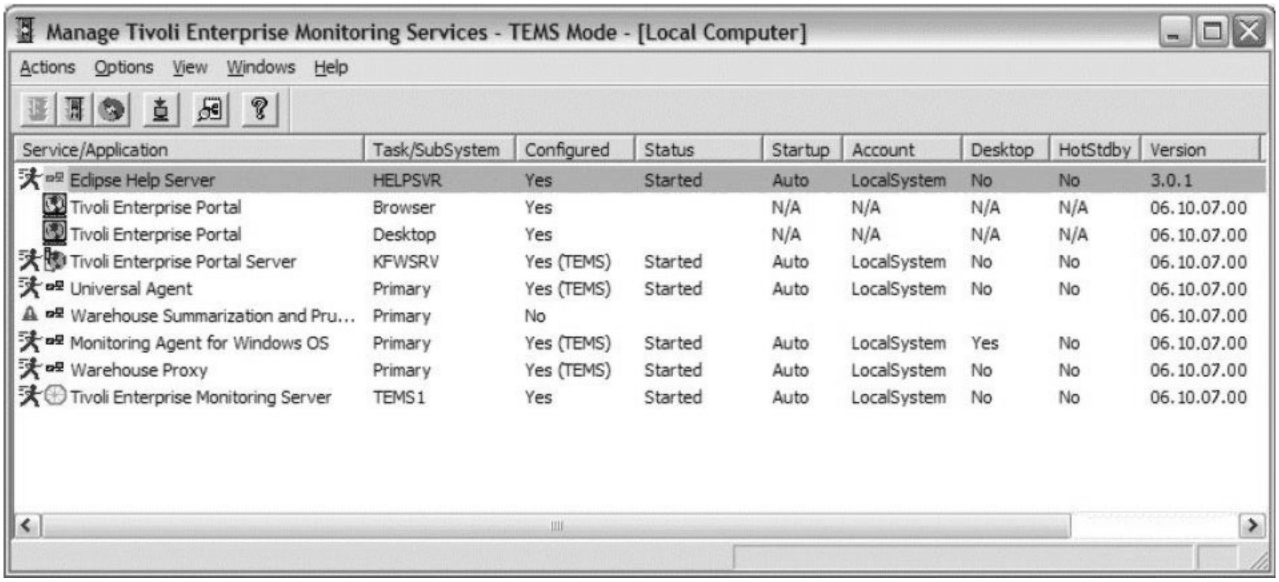
The **createnode** command uses a default timeout of 1800 seconds (30 minutes) to complete its operation. This timeout value may be changed by using the **-o TIMEOUT=***XXXX* option (where *XXXX* is seconds) when using the command.

The `TIMEOUT` environment variable value specified in the Tivoli Enterprise Monitoring Server configuration file is applied to the **updateAgent** and **addSystem** commands.

The `TACMD_TIMEOUT` environment variable value determines the amount of time, in minutes, that the CLI interface waits for the issued command to complete. If the `TACMD_TIMEOUT` value is less than the `TIMEOUT` values specified above and the `TACMD_TIMEOUT` value expires, the command under way continues, however, a command timeout message is displayed. Therefore it is important that the `TACMD_TIMEOUT` exceed either of the `TIMEOUT` values specified for the deployment operation.

Validating the components that you installed

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



Manage Tivoli Enterprise Monitoring Services - TEMS Mode - [Local Computer]
Actions
Options
View
Windows
Help

Service/Application	Task/SubSystem	Configured	Status	Startup	Account	Desktop	HotStdby	Version
Eclipse Help Server	HELPSVR	Yes	Started	Auto	LocalSystem	No	No	3.0.1
Tivoli Enterprise Portal	Browser	Yes		N/A	N/A	N/A	N/A	06.10.07.00
Tivoli Enterprise Portal	Desktop	Yes		N/A	N/A	N/A	N/A	06.10.07.00
Tivoli Enterprise Portal Server	KFWSRV	Yes (TEMS)	Started	Auto	LocalSystem	No	No	06.10.07.00
Universal Agent	Primary	Yes (TEMS)	Started	Auto	LocalSystem	No	No	06.10.07.00
Warehouse Summarization and Pru...	Primary	No						06.10.07.00
Monitoring Agent for Windows OS	Primary	Yes (TEMS)	Started	Auto	LocalSystem	Yes	No	06.10.07.00
Warehouse Proxy	Primary	Yes (TEMS)	Started	Auto	LocalSystem	No	No	06.10.07.00
Tivoli Enterprise Monitoring Server	TEMS1	Yes	Started	Auto	LocalSystem	No	No	06.10.07.00

Figure 2. Levels for all components following the installation of Fix Pack 7

You can also validate your installation by running one of the following cinfo commands:

- The `kincinfo` command on Windows. See "Sample output for the kincinfo command (for Windows)."
- The `cinfo` command on Linux or UNIX. See "Sample output for the cinfo command (for UNIX or Linux)" on page 50.

Sample output for the kincinfo command (for Windows)

Note: The example of `kincinfo` command output in this section shows components that are present in the example environment. If you do not have all of these components installed, your command output will not be identical to the sample output.

To run the `kincinfo` command, access 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 syntax.

Note: This command is global. You can enter the command from any directory path and generate output. In a typical installation, the command is located in the following directory: **C:\ibm\ITM\InstallITM**.

The following text block shows sample output of the **kincinfo** command to validate that all components have been installed. This command is described in "Validating the components that you installed" on page 46.

```
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: 06.10.07.00 Build: 200702230014

A4        i5/OS Support
          WINNT Version: 06.10.07.00 Build: 200702230014

A4        i5/OS Support
          WINNT Version: 06.10.07.00 Build: 200702230014

A4        i5/OS Support
          WINNT Version: 06.10.07.00 Build: 200702230014

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

CJ        Tivoli Enterprise Portal Desktop Client
          WINNT Version: 06.10.07.00 Build: 200705012123

CQ        Tivoli Enterprise Portal Server
          WINNT Version: 06.10.07.00 Build: 200705012135

CW        Tivoli Enterprise Portal Browser Client
          WINNT Version: 06.10.07.00 Build: 200705012123

GL        Tivoli Enterprise Monitoring Agent Framework
          WINNT Version: 06.10.07.00 Build: 200705012139

HD        Warehouse Proxy
          WINNT Version: 06.10.07.00 Build: 200705012139

IT        TEC GUI Integration
          WINNT Version: 06.10.07.00 Build: 200611010030

IT        TEC GUI Integration
          WINNT Version: 06.10.07.00 Build: 200611010031

IT        TEC GUI Integration
          WINNT Version: 06.10.07.00 Build: 200611010030

KF        IBM Eclipse Help Server
          WINNT Version: 06.10.07.00 Build: 200704171107

LZ        Linux OS Support
          WINNT Version: 06.10.07.00 Build: 200704301644

LZ        Linux OS Support
          WINNT Version: 06.10.07.00 Build: 200704301644

LZ        Linux OS Support
          WINNT Version: 06.10.07.00 Build: 200704301644

LZ        Linux OS Support
          WINNT Version: 06.10.07.00 Build: 200704301644

MS        Tivoli Enterprise Monitoring Server
          WINNT Version: 06.10.07.00 Build: 200705012139

NS        NLS Support
          WINNT Version: 03.50.03.00 Build: 200510061051

NT        Monitoring Agent for Windows OS
          WINNT Version: 06.10.07.00 Build: 200701160818

NT        Windows OS Support
          WINNT Version: 06.10.07.00 Build: 200701160818

NT        Windows OS Support
```

```
          WINNT Version: 06.10.07.00 Build: 200701160818

NT        Windows OS Support
          WINNT Version: 06.10.07.00 Build: 200701160818

NT        Windows OS Support
          WINNT Version: 06.10.07.00 Build: 200701160818

SY        Summarization and Pruning Agent
          WINNT Version: 06.10.07.00 Build: 200705012135

SY        Summarization and Pruning Agent
          WINNT Version: 06.10.07.00 Build: 200705012135

TM        IBM Tivoli Monitoring 5.x Endpoint Support
          WINNT Version: 06.10.07.00 Build: 200604051327

TM        IBM Tivoli Monitoring 5.x Endpoint Support
          WINNT Version: 06.10.07.00 Build: 200604051327

UI        Tivoli Enterprise Services User Interface
          WINNT Version: 06.10.07.00 Build: 200705012139

UL        UNIX Logs Support
          WINNT Version: 06.10.07.00 Build: 200701120847

UL        UNIX Logs Support
          WINNT Version: 06.10.07.00 Build: 200701120847

UL        UNIX Logs Support
          WINNT Version: 06.10.07.00 Build: 200701120847

UL        UNIX Logs Support
          WINNT Version: 06.10.07.00 Build: 200701120847

UM        Universal Agent
          WINNT Version: 06.10.07.00 Build: 200705012131

UM        Universal Agent Support
          WINNT Version: 06.10.07.00 Build: 200705012131

UM        Universal Agent Support
          WINNT Version: 06.10.07.00 Build: 200705012131

UM        Universal Agent Support
          WINNT Version: 06.10.07.00 Build: 200705012131

UM        Universal Agent Support
          WINNT Version: 06.10.07.00 Build: 200705012131

UX        UNIX OS Support
          WINNT Version: 06.10.07.00 Build: 200701161329

UX        UNIX OS Support
          WINNT Version: 06.10.07.00 Build: 200701161329

UX        UNIX OS Support
          WINNT Version: 06.10.07.00 Build: 200701161329

UX        UNIX OS Support
          WINNT Version: 06.10.07.00 Build: 200701161329

C:\ >
```

Sample output for the cinfo command (for UNIX or Linux)

Note: The example of `cinfo` command output in this section shows components that are present in the example environment. If you do not have all of these components installed, your command output will not be identical to the sample output.

Perform the following steps to run the `cinfo` command:

1. Access this path in a command prompt window: *itm_home*`/bin`.
2. Run this command: `./cinfo` .

The following text block shows sample output of the **cinfo** command, which is used on UNIX or Linux systems to validate that all components have been installed. This command is described in "Validating the components that you installed" on page 46. After you run the command, you choose one of four options on the CINFO menu shown, depending on your needs.

```
*********** Mon May  7 14:35:50 EDT 2007 ******************
User      : root         Group: root sys dasadm1 db2grp1 db2fgrp1
Host name : cvtlin01     Installer Lvl:06.10.07.00
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:06.10.07.00
CandleHome: /usr/IBM/ITM
***********************************************************
...Product inventory

a4      Monitoring Agent for i5/OS
         tms     Version: 06.10.07.00
         tpd     Version: 06.10.07.00
         tps     Version: 06.10.07.00
         tpw     Version: 06.10.07.00

ax      IBM Tivoli Monitoring Shared Libraries
         li6243  Version: 06.10.07.00

cj      Tivoli Enterprise Portal Desktop Client
         li6263  Version: 06.10.07.00

cq      Tivoli Enterprise Portal Server
         li6263  Version: 06.10.07.00

cw      Tivoli Enterprise Portal Browser Client
         li6263  Version: 06.10.07.00

hd      Warehouse Proxy
         li6243  Version: 06.10.07.00

it      TEC GUI Integration
         tpd     Version: 06.10.07.00
         tps     Version: 06.10.07.00
         tpw     Version: 06.10.07.00

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

```
kf      IBM Eclipse Help Server
         li6243  Version: 06.10.07.00

lz      Monitoring Agent for Linux OS
         li6263  Version: 06.10.07.00
         tms     Version: 06.10.07.00
         tpd     Version: 06.10.07.00
         tps     Version: 06.10.07.00
         tpw     Version: 06.10.07.00

ms      Tivoli Enterprise Monitoring Server
         li6243  Version: 06.10.07.00

nt      Monitoring Agent for Windows OS
         tms     Version: 06.10.07.00
         tpd     Version: 06.10.07.00
         tps     Version: 06.10.07.00
         tpw     Version: 06.10.07.00

sh      Tivoli Enterprise Monitoring SOAP Server
         li6243  Version: 06.10.07.00

sy      Summarization and Pruning Agent
         li6243  Version: 06.10.07.00
         tms     Version: 06.10.07.00

tm      Monitoring Agent for IBM Tivoli Monitoring 5.x Endpoint
         tms     Version: 06.10.07.00
         tps     Version: 06.10.07.00

uf      Universal Agent Framework
         li6243  Version: 06.10.07.00

ui      Tivoli Enterprise Services User Interface
         li6243  Version: 06.10.07.00

ul      Monitoring Agent for UNIX Logs
         li6243  Version: 06.10.07.00
         tms     Version: 06.10.07.00
         tpd     Version: 06.10.07.00
         tps     Version: 06.10.07.00
         tpw     Version: 06.10.07.00

um      Universal Agent
         li6243  Version: 06.10.07.00
         tms     Version: 06.10.07.00
         tpd     Version: 06.10.07.00
         tps     Version: 06.10.07.00
         tpw     Version: 06.10.07.00

ux      Monitoring Agent for UNIX OS
         tms     Version: 06.10.07.00
         tpd     Version: 06.10.07.00
         tps     Version: 06.10.07.00
         tpw     Version: 06.10.07.00

    -- 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 Object Management Architecture (OMA) objects was granted or changed, the authorities are 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 20. 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 10 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
	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 9.
	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. Save a copy of the configuration file **QAUTOTMP/KMSPARM(KBBENV)** to backup your current settings. After installation, compare the content of this file with new **QAUTOTMP/KMSPARM(KBBENV)** and apply the differences to **QAUTOTMP/KMSPARM(KBBENV)**.
	6. Use **GO OMA** option 3 to end the agent and then use F3 to exit the OMA Menu. Make sure that no other users are displaying the Tivoli Monitoring: i5/OS Agent panel.

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

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

	10. 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`

Table 20. Checklist for remotely deploying the fix pack to an i5/OS agent (continued)

✓	Installation step

	11. 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)`

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

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 56
- "Important information for Windows users" on page 57
- "Installation instructions" on page 57
- "Modifying your rule base after installation" on page 61
- "Closing sampled events in IBM Tivoli Enterprise Console" on page 62
- "Verifying the installation of the event synchronization fix pack" on page 62
- "Uninstalling the IBM Tivoli Enterprise Console event synchronization" on page 63

Fix pack installations for the respective products must match, as stated in these examples:

- If you apply Fix Pack 7 to IBM Tivoli Enterprise Console event forwarding on IBM Tivoli Monitoring 6.1, then Fix Pack 7 must be applied to IBM Tivoli Enterprise Console Event Synchronization on the IBM Tivoli Enterprise Console server.
- If you apply Fix Pack 6 to IBM Tivoli Enterprise Console event forwarding on IBM Tivoli Monitoring 6.1, then Fix Pack 6 must be applied to IBM Tivoli Enterprise Console Event Synchronization 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 21.

Table 21. 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|7|0|1.0.0.7`, which indicates that Fix Pack 7 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 `1.0.0.7`, which indicates that Fix Pack 7 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|7|0|1.0.0.7`, which indicates that Fix Pack 7 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|7|0|1.0.0.7`, which indicates that Fix Pack 7 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 `1.0.7.0.DSP=1.0.0.7`, which indicates that Fix Pack 7 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:

- **Base:** The base IBM Tivoli Enterprise Console event synchronization available with the GA level of IBM Tivoli Monitoring, Version 6.1

  OR
- **Fix Pack 1:** IBM Tivoli Monitoring and IBM Tivoli Enterprise Console Event Synchronization Fix Pack 1

  OR
- **Fix Pack 3:** IBM Tivoli Monitoring and IBM Tivoli Enterprise Console Event Synchronization Fix Pack 3

  OR
- **Fix Pack 6:** IBM Tivoli Monitoring and IBM Tivoli Enterprise Console Event Synchronization Fix Pack 6

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 7 level.

- The prereqs for installing as an upgrade are Event Synch base (first sub-bullet) OR Event Synch FP1 (second sub-bullet) OR Event Synch FP3 (add third sub-bullet) OR Event Synch FP6 (add fourth sub-bullet).
- If you have IBM Tivoli Enterprise Console event synchronization installed on your computer already, first determine which version is installed (see Table 21 on page 55 for assistance). If the version installed is 1.0.0.7 (Fix Pack 7), you are at the current level. If the version installed is earlier than version 1.0.0.7, you can install the version that comes with Fix Pack 7.
- 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 6 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 (**setupwin32fp7.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 7: 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 (**setupwin32fp7.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" on page 58
- "Installing from the command line" on page 59
- "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 21 on page 55 for assistance). If the version ed is 1.0.0.7 (Fix Pack 7), you are at the current level. If the version installed is earlier than version 1.0.0.7, you can install the version that comes with Fix Pack 7.

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 **setupwin32fp7.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>fp7.bin
   ```

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

   ```
   setupAixfp7.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 22. 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.
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 23. 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:

   ```
   setupwin32fp7.exe -console
   ```

   On UNIX computers:

   ```
   setup<operating_system>fp7.bin -console
   ```

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

   ```
   setupAixfp7.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 22 on page 58 for explanation of the options) and press Enter to continue.
   - If you chose the manual update option, skip to Step 10 on page 60.
   - 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 changesto 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:

   ```
   setupwin32fp7.exe -options-template filename
   ```

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

   On UNIX computers:

   ```
   setupoperating_systemfp7.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:

   ```
   setupAixfp7.bin -options-template filename
   ```

2. Edit the output file to specify the **rbInstallTypePanel.rbInstallType** variable. Refer to Table 22 on page 58 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:

   ```
   setupwin32fp7.exe -options filename -silent
   ```

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

   On UNIX computers:

   ```
   setup<operating_system>fp7.bin -options filename -silent
   ```

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

   ```
   setupAixfp7.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 created in the directory defined by the %TEMP% environment variable. To determine where this directory is defined for the current command line window, run the following command:

```
echo %TEMP%
```

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

As mentioned in APAR IY96333, the closing of *sampled* events is managed as follows:

1. A situation event is forwarded to IBM Tivoli Enterprise Console that is associated with a *sampled* situation.
2. The situation event is subsequently closed in the event server.
3. Event Synchronization sends a request to IBM Tivoli Monitoring to acknowledge the situation with a specified timeout.
4. If the timeout period is completed and the acknowledgement of the situation expires, the acknowledgement expired update sent from IBM Tivoli Monitoring is used as a new situation event in IBM Tivoli Enterprise Console, and data from the original closed event is copied to the update event.
   - If the closed event expires from the cache, the new event will be missing data, because the update from IBM Tivoli Monitoring does not contain all the data from the original situation.
   - The new event does not contain the latest event data for the situation, but rather the event data that was reported when the situation first became true.
5. If the situation resets itself before the acknowledgement timeout period expires, the situation event remains closed in IBM Tivoli Enterprise Console.

Situation timeouts are set in the (**sit_timeouts.conf**) configuration file. This file is located on the event server. You can manage the configuration file as follows:

1. Modify the configuration settings:
   - You can change the default acknowledgement expiration time, which is 59 minutes.
   - You can set an expiration time for a single situations by inserting a line that adheres to the following syntax:

     ```
     situation_name=expire_time
     ```

     where *situation_name* is the literal name of the situation in IBM Tivoli Monitoring V6.1, and *expire_time* is the expiration time for acknowledgement, in minutes.
2. Run the **sitconfig.sh refresh** command to dynamically load the new settings into the IBM Tivoli Enterprise Console rule base. The path to the command is as follows: `$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 21 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 correctly 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 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.

Working with the Tivoli Enterprise Portal browser client

This topic describes how to update the Java Runtime Environment (JRE), which is required by the browser client, on computers where the JRE was not upgraded to Fix Pack 7 (in other words, systems that host no other components of IBM Tivoli Monitoring).

Updating the Java Runtime Environment (JRE) for the browser client

To upgrade to IBM Java, Version 1.4.2 SR8 (the version that Fix Pack 7 uses for Windows systems), perform the following procedure to install the recommended JRE for the browser client for the Tivoli Enterprise Portal:

1. On the Windows desktop where you want to run the browser client, click the Windows **Start** button, and select **Control Panel**.
2. Double-click the **Add or Remove Programs** icon to open the **Add or Remove Programs** window.
3. Select the icon for the IBM Java, Version 1.4.2 software.

   Note: If there is no IBM Java 1.4.2 icon in the **Add or Remove Programs** window, go to Step 5.
4. Click **Change/Remove** and follow the instructions on screen to uninstall the current version of the Java software.
5. Launch Internet Explorer.
6. Enter the standard URL for the portal, where *hostname* is the name of the computer that hosts the Tivoli Enterprise Portal Server:

   ```
   http://hostname:1920///cnp/client
   ```

   There is a delay as the new JRE, Version 1.4.2 SR8, executable is downloaded and installed on the computer. After the completion of installation the portal client launches automatically.

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 remain synchronized, 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.

Verifying a successful installation

This section describes quick methods to verifying that installation of the product was successful in a distributed environment, such as Windows, Linux, and UNIX.

Look for updated components in a master list of installed components

The **cinfo -i** command (**kincinfo -i** on Windows) generates a list of all installed product components, including version numbers. Consult this list to verify that the components that you installed are present. "Validating the components that you installed" on page 46 describes how to use this command and how to interpret the results that the command generates.

Look for updated components in the Tivoli Enterprise Portal

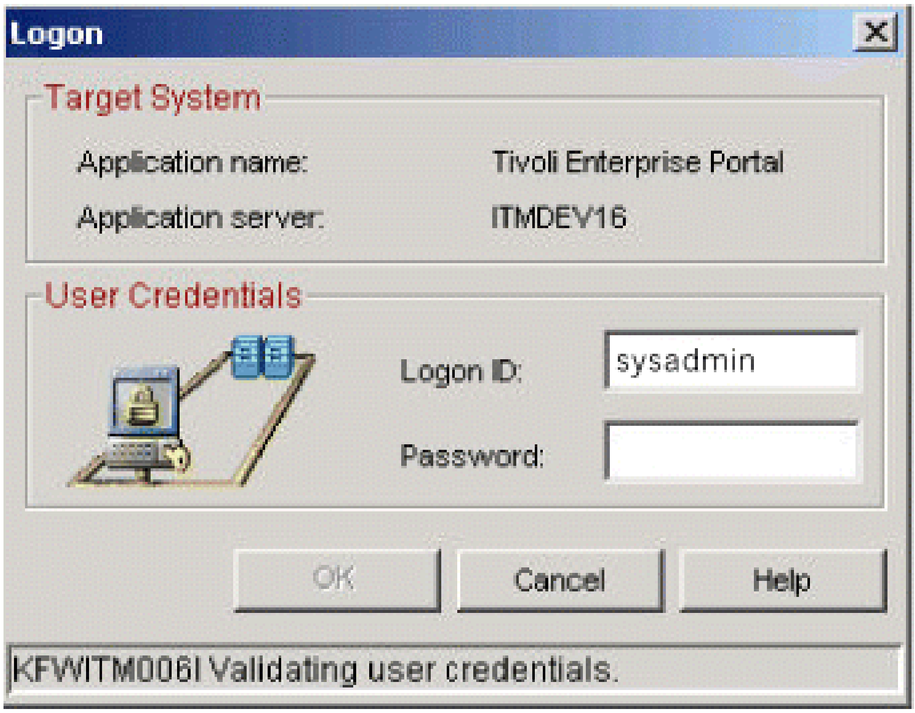
You can verify an installation by checking the portal as follows:

1. **Launch the Tivoli Enterprise Portal.**

   Access the Tivoli Enterprise Portal through the desktop client or the browser client, as described here:

   - **Desktop client:**

     a. In the Windows **Start** menu, select **Programs** > **IBM Tivoli Monitoring** > **Tivoli Enterprise Portal**. The login message is displayed.



Application name: Tivoli Enterprise Portal

Application server: ITMDEV16

Logon ID: sysadmin

Password:

KFWITM006I Validating user credentials.

Figure 3. Login prompt for the Tivoli Enterprise Portal

     b. Type the name (`sysadmin`) and password of the account that you created during installation.

     c. Click **OK**.

     OR

- **Browser client:**
  a. Start the Microsoft Internet Explorer browser.
  b. Type the following URL for the Tivoli Enterprise Portal into the **Address** field of the browser:
  ```
  http://systemname:1920///cnp/client
  ```
  where the *systemname* is the host name of the machine where the Tivoli Enterprise Portal is installed.
  c. Click **Yes** in response to any security prompts.
  d. In the login prompt, type the user name and password of the `sysadmin` account that you created during installation.
  e. Click **OK**.
  f. Click **Yes** to accept Java Security certificates for this browser session

2. **Verify that some of the default situations IBM Tivoli Monitoring are available.**
   a. In the Navigation tree (on the upper left side of the portal), expand the tree until you see the a monitoring agent that you have installed.
   b. To view the default situations, right-click the icon of this agent and select **Manage Situations** in the popup menu. A list of all available situations is displayed. This window displays the status of each situation and many other details.

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.

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 7, the upgrade toolkit upgrades to the Fix Pack 7 version of the agents.

For Fix Pack 7, 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

Using the Java Web Start application, you can 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 are not required 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, additional focus is placed on verification of OMEGAMON XE products and components running with IBM Tivoli Monitoring version 6.1 Fix Pack 7. 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, with some limitations:

- If you upgrade or add a base monitoring agent that reports to a Tivoli Enterprise Monitoring Server that runs on a z/OS system, you must ensure that the current catalog and attribute files for the product are transferred to that z/OS monitoring server. If the z/OS monitoring server is a remote monitoring server and reports to a hub monitoring server on z/OS, you must also transfer the files to the hub monitoring server. For more information see the *For distributed-based monitoring agents, add application support to the hub monitoring server* topic in Table 11. "Configuring the monitoring server for IBM Tivoli Monitoring products" in the *IBM Tivoli Monitoring Installation and Setup Guide*, Version 6.1.
- In general, you can follow the guidelines for sequencing upgrades that is provided in Table 8 on page 13.

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 Tivoli Enterprise Portal Console installation might not be required. It also provides secure e-mail delivery mechanism to deploy widgets that have been configured for specific monitoring or display of data by a customer IT organization to its client workstations. 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 OPAL Web site at 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

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

- “Installation”
- “Configuration” on page 75
- “IBM Tivoli Enterprise Console installation and configuration” on page 78
- “Documentation of installation and configuration” on page 79

See the following topics for additional information regarding installation and configuration issues:

- “Supported operating systems” on page 3
- “Supported databases for Tivoli Enterprise Portal Server and Tivoli Data Warehouse” on page 9

Installation

These limitations and workarounds are related to installation:

- **Limitation for UNIX-based systems:** During the installation of IBM Tivoli Monitoring 6.1 on UNIX-based systems, you might not see an option for a platform that is officially listed as supported. **Workaround:** Refer to Technote 1303680 for information about installing the product on UNIX-based systems: http://www-1.ibm.com/support/docview.wss?uid=swg21303680

- **Limitation for the Database monitoring agents:** Remote deployment of a Database monitoring agent might fail in a 64-bit Windows environment. **Workaround:** Perform a local installation on the target computer.

- **Limitation:** Remote configuration of deployed DB2 agents fails under specific conditions. The **tacmd addSystem** command does not complete successfully when you are deploying Fix Pack 1 for the DB2 Agent to a Windows endpoint which has an installed version of DB2 9.1.

  Workaround: See the options described in Technote 1304437. http://www-1.ibm.com/support/docview.wss?rs=2366&uid=swg21304437

- **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 for installation on Windows:** On Windows systems, the installation of IBM Tivoli Monitoring might freeze during installation of the required Java Runtime Environment (JRE). Silent install or remote deployment of a monitoring agent might also freeze or fail due to timeout error, because the JRE installation is not completed.

  The failure of the installation of the JRE to complete can be determined as follows:

  – For IBM Tivoli Monitoring silent install or remote deploy, the install process does not complete or times out.

  – For IBM Tivoli Monitoring installation using the UI, a message similar to the following is displayed and remains visible: `Installing IBM Java2 Runtime Environment 1.4.2, please wait.`

  Workaround: Perform the following steps:

  1. End the non-responding Java Run-time Environment (JRE) installer in the Windows Task Manager:
     – **For remote deploy:** look for **ibmjava142.exe** in the Processes view of Windows Task Manager, and end the process.
     – **For IBM Tivoli Monitoring installation using the UI, or attended silent install:** look for ″InstallShield - IBM Java Run-time Environment″ (or similar) in the Applications view of Windows Task Manager, and end the application.
  2. Wait for the monitoring agent installation to complete. After the installation completes, the agent is installed but not configured.
  3. Check Windows Task Manager, Processes view, for another **IDriver** process that might still be running. If you find such a process, end the process.
  4. Verify that the desired IBM Tivoli Monitoring components have been installed.
  5. Check the default JRE directory (`C:\Program Files\IBM\Java142`) to see whether the JRE code has been installed. Test the JRE by running the command: `C:\Progra~1\IBM\Java142\JRE\bin\ java -version`. If this command successfully returns Java version information, you know that the JRE is successfully installed.
  6. Respond as follows:
     – If the JRE and product components are successfully installed, no action is necessary.
     – If the JRE is not successfully installed, run the JRE installer directly from the installation media using one of the following options:

- **Local Install:** Run this executable:

  ```
  INSTALL_MEDIA\WINDOWS\InIBMJRE\ibm-java2-jre-142-SR8.exe
  ```

- **Remote deployment:** Run this executable:

  itm_home`\TMAITM6\agentdepot\`*productcode*`>\`*version*`\InIBMJRE\ibmjava142.exe`

If the JRE installation fails again, contact IBM Software Support for further assistance.

7. Reboot the Windows computer before using IBM Tivoli Monitoring.

- **Limitation for remote deployment and silent installation:** A silent installation terminates if product files are locked. This behavior ensures that the installer does not overwrite product files that are currently running. The best practice is to shut down all components, including monitoring servers, portal server, and portal clients before you perform any product upgrade.

  This limitation only affects silent installation. Installation through the installation wizard is not affected.

  Workaround: Use the following method to resolve the problem:

  1. Search the installation log for instances of the **CheckLockedFiles** string. Locked files are listed at these places.

     Locked files are files that might need to be upgraded during an installation, and because they are in use (locked) the silent install terminates.
  2. Identify the process that is locking the files.
  3. Stop the process.
  4. Prevent file locking by modifying the response file for installation file. This step is required when a silent installation has terminated.
     a. Open the response file in a text editor. In many cases, the file in which you make this modification is named **silent.txt**. On Windows, the file to modify is the **NT_Silent_Install.txt** file that is located on the monitoring server.
     b. Add the following line to the `[INSTALLATION SECTION]` area of your silent install response file:

     ```
     Locked Files=continue
     ```

     If you apply any other value or assign no value for this parameter, silent installations fail when locked files exist.
     c. Reboot the computer. (This step is mandatory.)
  5. Run the silent installation again.

- (*AIX only*) **Limitation:** The Tivoli Enterprise Monitoring Server fails to start after you install application support for z/OS components on and AIX system. This problem is seen in the following scenario:
  – You are working with a monitoring server that is hosted on an AIX system.
  – You installed Fix Pack 6 and then upgrade to Fix Pack 7 on the AIX system.
  – You install the z/OS product support package and OMEGAMON XE support for the z/OS interim fix 5 (IF5)
  – After installation, you might need to install application support on the hub monitoring server with 'm5' (Example: `itmcmd support -S` *hub_name* `m5`) and rebuild the portal server presentation (Example: `run itmcmd config -A cq` again).

  You can detect the problem as follows:
  – The monitoring server that is hosted on AIX fails to start.
  – The log file for the monitoring server includes messages that are similar to the following:

  ```
  +47FA8425.0000       Target: aix51
  (47FA8425.0001-6:kglcbbio.c,790,"open") Open failed for 'RKCPDEFW.DB', errno= 2, retrying
  ```

  Workaround: Copy two **RKCPDEFW*** files from **orig** folder to the following path:

  `../tables/`*hostname*

where *hostname* is the name of the AIX system that hosts the monitoring server. The following is an example command for this workaround. The target system is an AIX host that is named **server05** and the product has been installed into the default installation path:

```
cp ./ITM/tables/PLACEHOLDER/orig/RKCPDEFW* ./ITM/tables/server05
```

- **Limitation:** 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.

- **Limitation on UNIX-based and z/OS-based operating systems:** When you install application support for IBM Tivoli Monitoring 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 7 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 7.

- **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`.

- 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/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".

- **Limitation:** 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 the **xlC.aix50.rte** file set 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

This section specific limitations and workarounds for configuration of the product:

- **Problem:** The Tivoli Monitoring Services Discovery Library adapter (DLA) fails at startup on UNIX when the UNIX environment is not correctly configured. You see an error like the following, after you run the **KfwTmsDLA** command: `libjsig.so not found`.

  Workaround: Prior to using the **KfwTmsDLA** command, configure the UNIX environment as follows:

  1. Access the `/opt/IBM/ITM/config` directory path.
  2. Run this utility:

     ```
     . ./cq.config
     ```

3. Access the `/opt/IBM/ITM/arch/cq/bin` directory path, where *arch* is the identifier for the specific architecture of your operating system.
4. Run this utility:

   ```
   . ./pathsetup.sh
   ```

- **Limitation:** IBM Tivoli Monitoring depends on the time being roughly synchronized in the monitoring environment. Clock differences, such as those that can arise with the timekeeping of the VMware guest operating system, might generate the following symptoms:
  - Situations do not fire at the correct time.
  - Agents are displayed with offline status.
  - Warehouse data is not collected as expected.

  Workaround: Address these symptoms by referring to the recommendations in the following sources:

- "Heartbeat issues when running IBM Tivoli Monitoring v6.x on a Linux guest using VMWare": http://publib.boulder.ibm.com/infocenter/tivihelp/v15r1/index.jsp?topic=/com.ibm.itm.doc/pdg_itm6297.htm
- "VMware Time Sync and Windows Time Service":http://kb.vmware.com/selfservice/microsites/search.do?cmd=displayKC&docType=kc&externalId=1318&sliceId=2&docTypeID=DT_KB_1_1&dialogID=56893670&stateId=0%200%2056889717

- 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 7 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. For related information, see "Overview of product behavior with custom configuration settings" on page 20.

- **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 Enterprise 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 portal server 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 7 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 62 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:

- **Limitation on 64-bit AIX operating systems:** When you uninstall the product on a 64-bit AIX operating systems, you see the following message:

  ```
  uninstall.sh warning:  Purging /opt/itmfp7, continuing ...
  rmitab: 0481-211 Cannot update /etc/inittabhREgaa; errno is 28.
  ```

  Workaround: Ignore this message. (This information should be added to the next release of the *IBM Tivoli Monitoring Problem Determination Guide*, Version 6.1.)
- The following tip should be added to the documentation for IBM Tivoli Monitoring:

  To ensure the integrity of data that you collect, persistent data store maintenance procedures must be installed and operational. Otherwise, the data sets can become incorrect or full over a period of time. See the *IBM Tivoli Monitoring Administrator's Guide* for information about the persistent data store facility.
- **Problem:** The documentation of the **-i** parameter of the **tacmd editEventDest** command must be updated. You use this parameter to specify the ID of the server whose definition you want to edit. The documentation incorrectly states that zero (0) is a valid value for the **-i** flag. Actually, zero (0) is an incorrect value because it represents the default destination server definition, which cannot be edited by this command.

  Workaround: The following workarounds are available:
  - You can specify any *other* server ID, from 1 to 999.
  - You can edit the default destination server information manually by editing the **om_tec.config** file.

  The following updated parameter description should replace the original parameter description of the **tacmd editEventDest** command in all documentation:

  ```
  -i|--id|–serverID  Specifies the Server Destination ID of the event destination server
  definition to modify on the server. The value must be an integer between 1 and 999, inclusive.
  ```
- The following updates should be added to the next revision of the following IBM Tivoli Monitoring problem determination guides:
  - *IBM Tivoli Monitoring Problem Determination Guide*, Version 6.1, GC32-9458-00 (September 2006)
  - *IBM Tivoli Monitoring Problem Determination Guide*, Version 6.1, GC32-9458-00 (Revised May 2007)
  - *IBM Tivoli Monitoring Problem Determination Guide*, Version 6.2, GC32-9458-01

Table 24. Configuration updates for IBM Tivoli Monitoring problem determination guides

Documentation problem	Solution
Refer to Table 18. *Resolutions for agent deploy operations that TIMEOUT*. The Resolution for the “KDY0014E message” problem has an error. The syntax of the path name for a UNIX configuration file is incorrect, and the path name for another relevant file is missing.	Update the ″UNIX-based systems″ section in the Resolution column to state the following: “**On UNIX-based systems:** *installation_dir*/config/*host_name*_ms_*Tivoli Enterprise Monitoring Server_ID*.config and *installation_dir*/config/ms.ini”
Refer to Table 18. Resolutions for agent deploy operations that TIMEOUT. The Resolution for the “A system error occurs when running a tacmd command” problem has an error. The variable specification "(TIMEOUT=30)" is wrong and redundant.	Delete variable specification "(TIMEOUT=30)". The correct specification is provided later in the same section. **Note:** This problem appears in the Version 6.1 documents that are listed above, but not the Version 6.2 document.
Refer to Table 18. Resolutions for agent deploy operations that TIMEOUT. Backward slashes are used in UNIX and Linux path names.	Use forward slashes in UNIX and Linux path names.

Table 24. Configuration updates for IBM Tivoli Monitoring problem determination guides (continued)

Documentation problem	Solution
The following incorrect file name is specified: *hostname*_ms_*hostname*.config This incorrect file name appears twice in the Problem Determination Guides for Version 6.1 of the product and once in the Problem Determination Guide for Version 6.2. For example, see the "Setting the trace option for the IBM Tivoli Monitoring event forwarding" section.	Replace the incorrect file name with the following name and definition: "*hostname*_ms_*temsname*.config, where *temsID* is the name that you assign to the Tivoli Enterprise Monitoring Server during installation." For the sake of consistency, the following additional references to this configuration file should be given the same sample name (*hostname*_ms_*temsname*.config): • *host_name*_ms_*Tivoli Enterprise Monitoring Server_ID*.config • *hostname*_ms_*temsname*.config
The documentation describes how to modify the version of the configuration file (*hostname*_ms_*temsID*.config) that is currently in use. However, the documentation fails to describe the option to make the same configuration changes in the ms.ini initialization file.	First, resolve the naming problem that is described in the preceding row of this table. Then add the following statement in each place that the document mentions modifying the *hostname*_ms_*temsID*.config file: "Unlike the settings in the *hostname*_ms_*temsID*.config file, the settings in the ms.ini file persist after you reconfigure the Tivoli Enterprise Monitoring Server. If you want your changes to the configuration settings to persist, you must also apply these changes to the ms.ini file, which is located in this path: *installation_dir*/config/ms.ini. That way, the changes persist even after you reconfigure the monitoring server."

- Regarding APAR IZ04630, the following updated information should be added to the next version of the *Installation and configuration troubleshooting* chapter of the *IBM Tivoli Monitoring Problem Determination Guide*:

  Problem: In a 64-bit AIX environment, you might see a warning message as you work with IBM Tivoli Monitoring.

  ```
  **************************** WARNING ******************************
  You are currently running with data limits not set to unlimited.
  You may experience out of memory(OOM) conditions. In the event of an
  OOM error, please increase the data limit value. You may use
  "ulimit -d unlimited" to set data limit as unlimited.
  *******************************************************************
  ```

  Explanation: This problem arises because the product uses the following new Java service release on this platform: IBM AIX Java 2 Technology Edition, Version 1.4.2, SR9. This message is printed to the terminal every time the AIX 64-bit Java Run-Time Environment (JRE) is initialized. The message might be displayed during installation of IBM Tivoli Monitoring, and when you run the **itmcmd** and **tacmd** commands. Unlimited data size is required by the JRE to collect diagnostic data in the event of a JRE failure.

  Workaround: Ignore the message or run the **ulimit -d unlimited** command to avoid the message.

- Regarding APAR IZ01185, the following updated information belongs in the "Reference" chapter of the *IBM Tivoli Monitoring User's Guide*. The specific location for the update is the "Managed Systems attributes" topic in the "Attributes" section:

  For the Navigator Physical view Enterprise item and for custom Navigator view items that have the `*HUB_` or `*ALL_CMS` managed system list assigned, you can also create situations or queries with these monitoring server attributes.

  Note regarding queries: An attempt to distribute a query to any other type of component (such as a remote Tivoli Enterprise Monitoring Server) fails. You see the following message in the view for the managed system status query:

```
KFWITM217E - Request Error :   SLQ1_CreateRequest Failed , RC=5
```

All managed system status queries must be distributed to the hub, so you must either explicitly define the query result source, or the node to which you assign the query must have `*HUB` in its list of assigned systems.

- 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 “Comparing installation processes for Fix Pack 3 (or earlier) and Fix Pack 7” on page 83 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 "Sequence of upgrade procedures" on page 13.

- 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 68 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 67), 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. 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.

- 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.

  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: “Comparing installation processes for Fix Pack 3 (or earlier) and Fix Pack 7.”

Comparing installation processes for Fix Pack 3 (or earlier) and Fix Pack 7

You can directly upgrade from any previous IBM Tivoli Monitoring V6.1.0 Fix Pack to Fix Pack 7. After the upgrade you must use the component software from Fix Pack 7 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 was used 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 in IBM Tivoli Monitoring.

- **Limitation:** Remote deployment to the Windows 2008 operating system fails. **Workaround:** Manually install monitoring components on the Windows 2008 operating system. Remote deployment is not supported.
- **Limitation:** Deployment of version 6.2 agents from a Version 6.1 deployment depot is not supported. **Workaround:** Deploy version 6.2 agents from a version 6.2 depot.
- 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.

- **Limitation:** 64-bit attributes are not supported. For example, on a computer with physical memory that is greater or equal to 2 GB, the Memory workspace shows zero (0) or Unknown values for attributes such as Available Bytes and Commit Limit (Bytes). **Workaround:** None.

- **Limitation for the Windows OS Agent on the Windows 2008 operating system:** The Tivoli Enterprise Portal fails to display specific operating system metrics for Windows 2008.

  Explanation: Windows Counters are unique identifiers that the operating system uses to track system activity. IBM Tivoli Monitoring references these counters to provide monitoring data for the Windows OS Agent. Some of the counters that are used in Windows 2008 differ from the counters used in previous versions of Windows.

  Workaround: None. At this time, the software for IBM Tivoli Monitoring, Version 6.1, does not capture the data that is associated with these new counters.

- **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 7, 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 7 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 errorreturned
  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.

- **Problem with the i5/OS monitoring agent:** When you shut down the agent a message is logged indicating an abnormal shutdown. **Workaround:** You can ignore this message. To eliminate this message, you have the option to do the following:
  1. Open the QAUTOTMP/KMSPARM(KBBENV) file in a text editor.
  2. Insert an asterisk (*) at the beginning of the following two lines to comment them out:

     ```
     KBB_RAS1_LOG=(QAUTOTMP/KA4AGENT01 QAUTOTMP/KA4AGENT02
     QAUTOTMP/KA4AGENT03) \
     INVENTORY=QAUTOTMP/KA4RAS.INV LIMIT=5 PRESERVE=1
     ```

     The resulting lines would look like the following:

     ```
     *KBB_RAS1_LOG=(QAUTOTMP/KA4AGENT01 QAUTOTMP/KA4AGENT02
     QAUTOTMP/KA4AGENT03) \
     *INVENTORY=QAUTOTMP/KA4RAS.INV LIMIT=5 PRESERVE=1
     ```
  3. Recycle the agent. A spool file is created under the QAUTOMON user. You can discard the trace data in the spool file, unless IBM Software Support asks you keep the data.

Tivoli Enterprise Monitoring Server

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

Tivoli Enterprise Monitoring Server on distributed platforms issues

- **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 clear 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 dialog boxes 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: Clear 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 ensure 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 starttemsname`

- 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.

- 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. **Workaround:** Modify the corresponding ***.ini** file, which preserves the value when you run the **itmcmd config** command again.

- 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.

- **Limitation regarding firewall or anti-virus settings:** When you are installing a fix pack on the Tivoli Enterprise Monitoring Server on Windows, the installation can enter an endless loop, and the Manage Tivoli Monitoring Services status windows indicates that the monitoring server is in the ″Start Pending″ state.

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

  Workaround: 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 platforms**: 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 runtime environment 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.

- In some cases where the hub Tivoli Enterprise Monitoring Server is running on Linux on zSeries with Fix Pack 7, 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

- The following issue was reported during development of Interim Fix 5 for Fix Pack 6:

  After a z/OS hub Tivoli Enterprise Monitoring Server is stopped and restarted quickly, the agents reporting to a remote Tivoli Enterprise Monitoring Server that has been running may not come on line. **Workaround:** After the z/OS hub monitoring server is stopped, wait for the remote monitoring server's heart interval (3 minutes by default) to elapse before restarting 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 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 start automatically. 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 name of the runtime environment, 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 JCL suffix for the runtime environment) 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 is 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*.

- The following clarifications should be added to the documentation:

The following statement belongs in the *IBM Tivoli Monitoring Problem Determination Guide*, Version 6.1.0:

Limitation on AMD 64-bit environments that run Windows 2003: The Desktop client fails to launch in the following scenario:

1. You uninstall IBM Tivoli Monitoring.
2. You reinstall the Tivoli Enterprise Portal Server. (In this step, you might also install monitoring agents.)
3. In a separate installation operation, you install the Desktop client without configuring the Tivoli Enterprise Portal Server.

In this scenario, the Desktop Client fails to run because configuration of the portal server is required in Step 3. This configuration step is required even though you have already installed and configured the portal server in Step 2.

Workaround: Install the Desktop Client again, accepting the option to configure the Tivoli Enterprise Portal Server. Supply the correct configuration values for your environment.

An update is needed in the *IBM Tivoli Monitoring Installation and Setup Guide*, Version 6.1.0. Specifically, the “Windows: Installing the desktop client” topic in the should be updated. The following paragraph should be added between steps 10 and 11: “On all Windows computers, when the desktop client is installed on the same host as the portal server but as part of a separate installation, the portal server must be reconfigured during installation of the client.”

- **Limitation:** A problem arises when you create a query and add new attributes to the query. The column heading for the new attributes in the Specification tab fails to display the function (*fx*) icon and you are not able to specify functions for the attribute. **Workaround:** Save and reopen the newly created query. The icon is displayed for the new attributes.

- **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.

- 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 7, 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 theTivoli 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`.

  See Technote 1258694, http://www-1.ibm.com/support/docview.wss?uid=swg21258694, for more information about this workaround.

  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 7 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.

- 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 "IBM Tivoli Data Warehouse solution using Microsoft SQL Server". The "Step 1: Create the IBM Tivoli Data Warehouse database" section must be updated with the following statement:

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

- The **sy** log file for Summarization and Pruning might show the Java exception when you restart the Warehouse Proxy Agent while the remote server for IBM Tivoli Data Warehouse is down or not available on the network. errors like the following. No action is required other than resolving any network connection problems. The following excerpt shows a typical Java exception:

```
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.

- 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 83 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 Enterprise 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 Enterprise 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 Enterprise 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 these commands:

    ```
    itmcmd server stop TEMS
    itmcmd server 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. Learn more about the JDBC driver at the following Microsoft Web page: http://msdn.microsoft.com/en-us/library/ms378749.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, the **sy** log file might contain a message similar to the following harmless message, which you can ignore: `. . . Only limited VisiSecure functionality is enabled, If the product has a valid license make sure all licensing related jar files are in the CLASSPATH.`

Warehouse Proxy Agent

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

- 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 7 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 7 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 Tivoli 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 the fix pack. 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.)

  Note: If you install the fix pack in an language environment other than English, see "Software prerequisites for installation of the language pack" on page 3.

  The name of the installation image is **6.1.0-TIV-ITM-LP-FP0007**. 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*.

- 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/*platform*/cw/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 7

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 7. Fixed APARs are categorized as follows:

Note: Unless otherwise stated, the fixed APARs in this section were fixed for the first time in Fix Pack 7. The lists include fixed APARs from the interim fixes for Fix Pack 6. In these cases, the APAR description mentions the specific interim fix in which the APAR was first fixed, to help you plan and prioritize installation. *All the interim fixes for Fix Pack 6 are included in Fix Pack 7.*

- "Documentation APARs"
- "Installation component APARs"
- "Event synchronization APARs" on page 111
- "Tivoli Enterprise Monitoring Agent APARs" on page 112
- "Tivoli Enterprise Monitoring Server APARs" on page 113
- "Tivoli Enterprise Portal APARs" on page 120
- "Tivoli Enterprise Portal Server APARs" on page 121
- "IBM Tivoli Data Warehouse APARs" on page 123
- APARs addressed for specific monitoring agents.
  - "i5/OS monitoring agent APARs" on page 128
  - "Linux OS monitoring agent APARs" on page 128
  - "UNIX Logs monitoring agent APARs" on page 129
  - "Tivoli Universal Agent APARs" on page 125
  - "Windows OS monitoring agent APARs" on page 129
  - "UNIX OS monitoring agent APARs" on page 130

Updates to this list, if any become necessary, are provided in Technote 1303093 at the following Internet address: http://www-1.ibm.com/support/docview.wss?uid=swg21303093. 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, 1303093, 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 7" on page 11.

Installation component APARs

The following installation APAR fixes are delivered in Fix Pack 7:

- Table 25 lists the APAR fixes that are provided in Fix Pack 7.
- Table 26 on page 108 lists the APAR fixes that are included in Fix Pack 7 and were originally fixed in the interim fixes for Fix Pack 6. *All the interim fixes for Fix Pack 6 are included in Fix Pack 7.*

Table 25. Installation component APARs that are fixed in Fix Pack 7

APAR Number	Symptom, as described in the APAR database
IY89723	The SetPerm script located in the /bin folder produces errors when selecting the first two options after installing the OS agent on Solaris 9/10.

Table 25. Installation component APARs that are fixed in Fix Pack 7 (continued)

APAR Number	Symptom, as described in the APAR database
IY89862	SetPerm command failed when TEMS Security validate is requested and an underscore ″_″ exists in the TEMS name. For example hub_mytems. Fix changed the search so the name could be isolated completely.
IY94408	Can not install MQ monitoring agent for Tandem on newer systems which have JRE 1.5 installed. Additional issues came up after initial problem was resolved. These resolutions are included in these changes.
IY97997	″itmcmd config -S -t <TEMSNAME>″ and ″itmcmd manage″ create the SOAP access list ,kshxbubs.xml, in ″$CANDLEHOME/tmaitm6/<PLAT>/ms/bin/HTML″ instead of in ″$CANDLEHOME/tables/<TEMSNAME>/HTML″ where the TEMS attempts to locate it.
IZ02405	The itmcmd history command does not produce history files in a Tandem environment and displays a LIB error.
IZ04630	Various PMRs have been opened against problems caused by the JRE. This APAR updates the JRE from service release 1.1 to service release 9.
IZ07022	The itm agent /etc/inittab entry on an AIX machine is delayed for an extended period of time when the network is disconnected.
IZ07144	When the TEPS agent was started, a file migrate-env.sh was left in whatever was the current directory
IZ09503	Upgrade fails when upgrading on Suse 10 or RedHat 5. Which is caused by these platforms using a new version of Korn shell, called ksh93r
IZ09571	**Problem Summary:** The CandleHistory command doesn't work for Oracle or Sybase with instance info. It gives back an error that it cannot continue
IZ13729	Welcome screen presented during upgrade is confusing to the customers.

Table 26. Installation component APARs originally fixed in the interim fixes for Fix Pack 6.

APAR Number	Symptom, as described in the APAR database
Tivoli Distributed Installer APARs	
IY83136	During a fresh install of IBM Tivoli Monitoring 6.1 on an HPUX PA-RISC1 machine, the install fails during the GSKit installation phase. **Note:** This APAR was first resolved in the following interim fix (IF) for Fix Pack 6: `6.1.0.6-TIV-ITM-IF0003`.
IY88061	An error may occur when trying to view agent trace logs using Manage Tivoli Monitoring Services. This error has been isolated to agent instances that have been created from a template agent. **Note:** This APAR was first resolved in the following interim fix (IF) for Fix Pack 6: `6.1.0.6-TIV-ITM-IF0003`.
IY88877	The intent of the Program Folders parameter in the silent install file is Unclear and is confused with the computer group that was created. **Note:** This APAR was first resolved in the following interim fix (IF) for Fix Pack 6: `6.1.0.6-TIV-ITM-IF0003`.
IY88972	Files laid down by itmpatch when run as root were owned by the builder server user rather than by the appropriate install user. **Note:** This APAR was first resolved in the following interim fix (IF) for Fix Pack 6: `6.1.0.6-TIV-ITM-IF0003`.
IY89013	If hostname is greater than 8 characters, the output of cinfo -r is badly aligned, the fields are not aligned with the title of the field. **Note:** This APAR was first resolved in the following interim fix (IF) for Fix Pack 6: `6.1.0.6-TIV-ITM-IF0003`.
IY89098	When running UnSetRoot to restore non-root ownership of files owned by root (as set by SetPerm), the file kbbacf1 is missed. **Note:** This APAR was first resolved in the following interim fix (IF) for Fix Pack 6: `6.1.0.6-TIV-ITM-IF0003`.
IY91620	During a configuration, the config tool was attempting to load jars for reference. Those jar files, if on a disk with a symbolic link, were not being followed during the find comment to attempt to locate them. **Note:** This APAR was first resolved in the following interim fix (IF) for Fix Pack 6: `6.1.0.6-TIV-ITM-IF0003`.

Table 26. Installation component APARs originally fixed in the interim fixes for Fix Pack 6. (continued)

APAR Number	Symptom, as described in the APAR database
IY93196	If the TEMS is started when it is already running this can cause corruption to the TEMS tables. There is already code to prevent this from happening, but when one of the two TEMS processes is terminated (either ″cms start″ or ″kdsmain″) the current code allows the TEMS to be started which then causes multiple ″cms start″ or ″kdsmain″ processes to be started which can then cause corruption. **Note:** This APAR was first resolved in the following interim fix (IF) for Fix Pack 6: `6.1.0.6-TIV-ITM-IF0001`.
IY93322	When configuring a TEMS as a ″Hub″ with a hot standby setup, only the primary hub information is written to the \CMS\glb_site.txt file, the hot standby information is missing. **Note:** This APAR was first resolved in the following interim fix (IF) for Fix Pack 6: `6.1.0.6-TIV-ITM-IF0003`.
IY95415	InstallPresentation failed. Checking cq.config shows LIBPATH/SHLIB_PATH/LD_LIBRARY_PATH with DB2V8 path not DB2 V9. Running db2check.sh instance - will not return the correct path to the DB2 V9 instance. **Note:** This APAR was first resolved in the following interim fix (IF) for Fix Pack 6: `6.1.0.6-TIV-ITM-IF0003`.
IY95546	Tivoli Enterprise Portal Server connections not created properly if using DB2 9.x. **Note:** This APAR was first resolved in the following interim fix (IF) for Fix Pack 6: `6.1.0.6-TIV-ITM-IF0003`.
IY95816	Busy Java or GSKit files cause the corresponding install to either loop, hang, or force a reboot. The problem seems to appear on servers loaded with Java Apps or servers that contain Websphere or DB2 V9. This problem seems to occur more on Windows 2003 based servers than on Windows 2000 based servers. **Note:** This APAR was first resolved in the following interim fix (IF) for Fix Pack 6: `6.1.0.6-TIV-ITM-IF0003`.
IY96353	AutoRunAgents.sh run on Solaris machines doesn't properly link startup files with a soft link. **Note:** This APAR was first resolved in the following interim fix (IF) for Fix Pack 6: `6.1.0.6-TIV-ITM-IF0003`.
IY96372	When some HP machines boot up, the directory where su resides sometimes isn't included in the path.. which means that when su is called, it fails. **Note:** This APAR was first resolved in the following interim fix (IF) for Fix Pack 6: `6.1.0.6-TIV-ITM-IF0003`.
IY96450	Tivoli Enterprise Portal Desktop will not start, no trace is put out. Customer must edit CNP.BAT to clean up the trace information on the -Dkjr.trace.params= parameter. The error is caused by unpaired quotes that cause parameters to be ignored. **Note:** This APAR was first resolved in the following interim fix (IF) for Fix Pack 6: `6.1.0.6-TIV-ITM-IF0003`.
IY97093	If the UA agent starts before Tivoli Enterprise Portal Server does on some Windows machines, port 1920 is used and is unavailable for portal server to use, and the portal server startup fails. **Note:** This APAR was first resolved in the following interim fix (IF) for Fix Pack 6: `6.1.0.6-TIV-ITM-IF0003`. There are no code changes for this APAR, this is a documentation solution: When a computer connection is established, the client side of the connection uses a port number. Unless a client program explicitly requests a specific port number, the port number used is an ephemeral port number. Ephemeral ports are temporary ports assigned by a machine's IP stack and are assigned from a designated range of ports for this purpose. When the connection terminates, the ephemeral port is available for reuse. It is sometimes desirable to change which port numbers are used for the ephemeral port range. The user can use a larger range so that more simultaneous connections are possible and can shift the range to the higher numbered ports. The higher numbered ports should be used as ephemeral ports because they are less likely to be used as port numbers for system services. Well-known service ports have traditionally been assigned to lower port numbers. For instance, the portal server uses port 1920. It is recommended that you begin the ephemeral port range at port 4096 or higher. **Note:** This APAR was first resolved in the following interim fix (IF) for Fix Pack 6: `6.1.0.6-TIV-ITM-IF0003`.

Table 26. Installation component APARs originally fixed in the interim fixes for Fix Pack 6. (continued)

APAR Number	Symptom, as described in the APAR database
IY97280	Oracle agent fails to start when the instance names end similarly. If the name of the instances are for example TEST & ATEST, starting TEST first and then ATEST it appears that they start successfully. If you start ATEST first and then try to start TEST, TEST remains OFFLINE. **Note:** This APAR was first resolved in the following interim fix (IF) for Fix Pack 6: `6.1.0.6-TIV-ITM-IF0003`.
IY97318	During the start and stop of some agents (specifically MQ), temporary files are not removed from the /tmp directory and you are prompted to allow them to be removed. **Note:** This APAR was first resolved in the following interim fix (IF) for Fix Pack 6: `6.1.0.6-TIV-ITM-IF0003`.
IY97554	ITM Install loops 100% cpu while installing either Java or GSKit. The loop will complete and the file will be updated if the read-only flag is reset on the setup.iss file. **Note:** This APAR was first resolved in the following interim fix (IF) for Fix Pack 6: `6.1.0.6-TIV-ITM-IF0003`.
IY97819	When GSKit or Java existed in a location not recognized by IBM Tivoli Monitoring 6.1, the install would fail. If the installed GSKit was at a higher release than the GSKit needed, the upgrade of GSKit would fail or change the location of GSKit, causing other products to fail. **Note:** This APAR was first resolved in the following interim fix (IF) for Fix Pack 6: `6.1.0.6-TIV-ITM-IF0003`.
IY97903	On a Solaris 10 system with multiple zones defined, IBM Tivoli Monitoring install attempts to install GSKit into in the global zone and all local-zones. **Note:** This APAR was first resolved in the following interim fix (IF) for Fix Pack 6: `6.1.0.6-TIV-ITM-IF0003`.
IY97904	When you install a zLinux 64 bit machine using 32 bit mode, and later it starts up under 64 bit mode during boot, the auto-start routines don't run, since its in the wrong mode, 32, not 64. **Note:** This APAR was first resolved in the following interim fix (IF) for Fix Pack 6: `6.1.0.6-TIV-ITM-IF0001`.
IY98134	Windows install continues when the PATH environment variable has exceeded the maximum length allowed by Windows, which leads to unpredictable results. **Note:** This APAR was first resolved in the following interim fix (IF) for Fix Pack 6: `6.1.0.6-TIV-ITM-IF0003`.
IZ00468	Three agents (YN, YJ, HT) didn't properly stop, they are killed using -9, rather than a warning SIG -15. **Note:** This APAR was first resolved in the following interim fix (IF) for Fix Pack 6: `6.1.0.6-TIV-ITM-IF0003`.
IZ00670	The candle_installation.log file become filled with extraneous digup msgs caused by an embedded tacmd call that caused the tracing. **Note:** This APAR was first resolved in the following interim fix (IF) for Fix Pack 6: `6.1.0.6-TIV-ITM-IF0003`.
IZ00676	Oracle/Sybase configuration files created with long hostname which results in UpdateAutoRun.sh not processing them which means that the agents don't restart when the machine is rebooted. **Note:** This APAR was first resolved in the following interim fix (IF) for Fix Pack 6: `6.1.0.6-TIV-ITM-IF0001`.
IZ00684	The Oracle and Sybase agents put entries into the RunInfo table using an fully qualified domain name, for example, `foobar.company.com`. For these entries when customer runs **cinfo -r** there is no Owner or Start information. **Note:** This APAR was first resolved in the following interim fix (IF) for Fix Pack 6: `6.1.0.6-TIV-ITM-IF0003`.
IZ01406	Multiple consecutive blank lines in an ini file caused an agent not to start. **Note:** This APAR was first resolved in the following interim fix (IF) for Fix Pack 6: `6.1.0.6-TIV-ITM-IF0003`.
IZ01751	The IBM Tivoli Monitoring installation on an HP-UX server caused a PeopleSoft application problem because it incorrectly changed the permissions of an HP-UX OS library, namely (/usr/lib/libCsup_v2.2). **Note:** This APAR was first resolved in the following interim fix (IF) for Fix Pack 6: `6.1.0.6-TIV-ITM-IF0003`.
IZ02078	When installing IBM Tivoli Monitoring and GSKit, there are flags set by GSKit that indicate a reboot is required. Often these flags are set for reasons that do not require a reboot before the IBM Tivoli Monitoring install. **Note:** This APAR was first resolved in the following interim fix (IF) for Fix Pack 6: `6.1.0.6-TIV-ITM-IF0003`.

Table 26. Installation component APARs originally fixed in the interim fixes for Fix Pack 6. (continued)

APAR Number	Symptom, as described in the APAR database
IZ03557	After customer installs platform CD and LA fixes, they return to the Platform CD to install a non-selected component. After install ANY component that had a LA fix applied will disappear. Only occurs on Windows platforms. **Note:** This APAR was first resolved in the following interim fix (IF) for Fix Pack 6: `6.1.0.6-TIV-ITM-IF0003`.
IZ03723	Customer copies Install MEDIA (CD) to local directory that contains a space. Runs setup.exe from the Windows directory of the MEDIA and after GSKit is installed but before the License Agreement displays, the install just disappears, no logs are written. This occurs where long file names are supported, but short 8.3 filename equivalents are not supported. **Note:** This APAR was first resolved in the following interim fix (IF) for Fix Pack 6: `6.1.0.6-TIV-ITM-IF0003`.
IZ03809	During an upgrade to IBM Tivoli Monitoring 6.1 from 04R1M4 with the CMS installed, the CMS service remains on the user's machine and may block the new TEMS from starting. The CMS service in the Windows Services window remains after an upgrade from 04R1 to IBM Tivoli Monitoring 6.1 or 6.2. This can cause a problem on some user's machine if it ties up resources barring the newly installed TEMS from running. **Note:** This APAR was first resolved in the following interim fix (IF) for Fix Pack 6: `6.1.0.6-TIV-ITM-IF0003`.
IZ03924	On UNIX/Linux machines, if a monitoring agent, portal server, or monitoring server process is started, and then it stops for some reason, and the operating system reuses the process id that the dead process was started on. IBM Tivoli Monitoring might detect that the dead process continues to run. Consequently, IBM Tivoli Monitoring might stop the process, even though the process ID number now corresponds to a separate software application. **Note:** This APAR was first resolved in the following interim fix (IF) for Fix Pack 6: `6.1.0.6-TIV-ITM-IF0001`.
IZ04429	During an upgrade to IBM Tivoli Monitoring 6.1 and when the TEMS framework is selected for upgrade, the Back button on the ″TEPS Desktop and Browser Signon ID and Password″ install dialog does not work. **Note:** This APAR was first resolved in the following interim fix (IF) for Fix Pack 6: `6.1.0.6-TIV-ITM-IF0003`.
IZ04643	If you stop multi-instance agents, such as Universal Agent, the sub-processes stops properly, but the tracking file (RunInfo) is not updated properly. This shows an agent running when you execute ″cinfo -r″, when in fact the agent is no longer running. **Note:** This APAR was first resolved in the following interim fix (IF) for Fix Pack 6: `6.1.0.6-TIV-ITM-IF0001`.
IZ05110	**runGSkit** fails to recognize GSKit 7.0.4.11 as an acceptable version that does not require the installation of the IBM Tivoli Monitoring supplied version **Note:** This APAR was first resolved in the following interim fix (IF) for Fix Pack 6: `6.1.0.6-TIV-ITM-IF0003`.
IZ07026	The IBM Tivoli Monitoring UNIX command **SetPerm** does not execute properly on Linux AMD 64 machines. **Note:** This APAR was first resolved in the following interim fix (IF) for Fix Pack 6: `6.1.0.6-TIV-ITM-IF0003`.
IZ07528	Some directories are not getting cleaned up in the /tmp dir and later users of different permissions are having problems. **Note:** This APAR was first resolved in the following interim fix (IF) for Fix Pack 6: `6.1.0.6-TIV-ITM-IF0003`.
IZ08466	On Linux systems where multiple versions of GSKit are detected, GSKit installation may detect the earliest version of the GSKit product instead of the latest installed version, thus GSKit installation is attempted when it should not be. **Note:** This APAR was first resolved in the following interim fix (IF) for Fix Pack 6: `6.1.0.6-TIV-ITM-IF0003`.

Event synchronization APARs

The following APARs are addressed in Fix Pack 7 regarding event synchronization between IBM Tivoli Monitoring and IBM Tivoli Enterprise Console:

APAR Number	Symptom, as described in the APAR database
IY86073	The Situation Update Forwarder discards situation updates with a display item containing a comma, logging an error message.

APAR Number	Symptom, as described in the APAR database
IY90868	″link_table″ slot missing from kib.baroc file
IY95008	The ITM_KKA_EVENT_DISTRIBUTION_BY_STATUS_BASE variable has 2 slots with the same name.
IZ02775	If the HTTPS (SOAP) port has been customized for a TEMS as something other than the default of ″3661″, the SUF will not be able to synchronize events with the TEMS.
IZ02879	Situation event data shows up with '~' (tilde).
IZ03902	When using the TEC Event Viewer in the Tivoli Enterprise Portal, selecting Dynamic Filter may result in the following error message, if the TEC database is an Oracle database and there are 1000+ systems below the currently selected Navigator item in the Tivoli Enterprise Portal. `ECO2044E: The RDBMS can not be reached.` No events are displayed by the event viewer when the error occurs.
IZ04292	The SUF fails to synchronize events containing Japanese (non-UTF8) characters in the display item.

Tivoli Enterprise Monitoring Agent APARs

The following installation APAR fixes are delivered in Fix Pack 7:

- Table 27 lists the APAR fixes that are provided in Fix Pack 7.
- Table 28 lists the APAR fixes that are included in Fix Pack 7 and were originally fixed in the interim fixes for Fix Pack 6. *All the interim fixes for Fix Pack 6 are included in Fix Pack 7.*

Table 27. Tivoli Enterprise Monitoring Agent APARs that are fixed in Fix Pack 7

APAR Number	Symptom, as described in the APAR database
IY93399	Data returned as results of queries to CICS agents configured with subnodes that have similar names are not complete. For example, if the CICS agent contains subnodes named CI308 and CI308W, just the data from the subnode CI308W is returned by the query; no data from subnode CI308 will be present.
IZ00591	Situations created for tables defined as being a PureEvent type, distributed and associated to a specific subnode, becomes true when the condition is satisfied by any subnode of the same agent.
IZ02165	A Take Action command executed twice.
IZ11504	WINDOWS HANDLE leak in KDSMAIN while reflex actions.
IZ13788	The KDE GATEWAY freezes with flood of agents.
IZ16659	ITM WINDOWS OS AGENT DOES NOT START ON WINDOWS SERVER 2008 IBM Tivoli Monitoring Windows OS Agent fails to start on Microsoft Windows Server 2008 operating systems due to problems loading several dll's. Problem symptoms: 1. Memory dumps during agent startup. 2. Error Message ″The service did not respond to the start or control request in a timely fashion." 3. Agents installed on Windows Server 2008 are not displayed under ″Windows System″ node like other Windows OS agents.

Table 28. Tivoli Enterprise Monitoring Agent APARs originally fixed in the interim fixes for Fix Pack 6.

APAR Number	Symptom, as described in the APAR database
IY79060	The 'HISTORICAL SUMMARIZED AVAILABILITY' workspace view shows negative numbers. **Note:** This APAR was first resolved in the following interim fix (IF) for Fix Pack 6: `6.1.0.6-TIV-ITM-IF0005`.

Table 28. Tivoli Enterprise Monitoring Agent APARs originally fixed in the interim fixes for Fix Pack 6. (continued)

APAR Number	Symptom, as described in the APAR database
IZ10691	SNA setup hangs with locking embrace. Intra-process SNA pipes that are created to prevent deadly embraces when SNA conversations are attempted back to the originating process do not carry the correct port. Since the port number is wrong, the SNA interface is attempting to start a real SNA conversation (with itself) rather than the correct behavior which is utilization of the loopback pipe. The real SNA conversation setup hangs with a locking embrace and the remote monitoring server will basically be unusable. This error can be exposed any time a REMOTE TEMS has SNA configured, and the REMOTE starts before the HUB. This can happen even when SNA is not the preferred protocol. This was also fixed in the TEMS via APAR IZ10689. **Note:** This APAR was first resolved in the following interim fix (IF) for Fix Pack 6: `6.1.0.6-TIV-ITM-IF0001`.
IZ10795	Subnodes may fail to return to ON-LINE state after a TEMS recycle. The TEMS Node list (TNODELST) and node status (INODESTS) tables can also become corrupted. **Note:** This APAR was first resolved in the following interim fix (IF) for Fix Pack 6: `6.1.0.6-TIV-ITM-IF0001`.
IZ11498	A netstat display of active connections shows sockets associated with the TEMS (http daemon) process on port 1920 in the CLOSE_WAIT state. This results when the http daemon is operating in 'header mode' and receives a disconnect from the session partner. The socket pair remain in CLOSE_WAIT until the TEMS process terminates. . **Note:** This APAR was first resolved in the following interim fix (IF) for Fix Pack 6: `6.1.0.6-TIV-ITM-IF0002`.
IZ11535	Message 1DE00070=KDE1_STC_BADPIPEHANDLE will be seen in the RKLVLOG immediately prior to the ABEND. There's a very small timing window that opens when a connection is broken, and the pipe listener thread is processing an event list containing the disconnected ASD. **Note:** This APAR was first resolved in the following interim fix (IF) for Fix Pack 6: `6.1.0.6-TIV-ITM-IF0002`.
IZ11550	KDEB_SocketMonitorWait() loops if it is awoken from select() and one of these conditions is true: (1) EWOULDBLOCK is presented on the subsequent receive(). (2) A NO DATA indication is presented on the subsequent receive().**Note:** This APAR was first resolved in the following interim fix (IF) for Fix Pack 6: `6.1.0.6-TIV-ITM-IF0002`.
IZ11557	Segmentation fault in pthread_mutex_init when an IP.PIPEconnection receives an inbound DISCONNECT notification while the connection is still in setup (XID exchange in-progress). The fault is due to the unconditional use of the CCB pointer in KDEP1_AttachChannel. This fault is typically preceeded by the following RAS1 log message: `Status 1DE0000B=KDE1_STC_DISCONNECTED=32: Broken pipe` **Note:** This APAR was first resolved in the following interim fix (IF) for Fix Pack 6: `6.1.0.6-TIV-ITM-IF0002`.
IZ12126	ITM6.1 Agents may fail to restart some situations after the agent has reconnected to it's TEMS. This applies only to agents on distributed platforms, not to z/OS agents. **Note:** This APAR was first resolved in the following interim fix (IF) for Fix Pack 6: `6.1.0.6-TIV-ITM-IF0005`.

Tivoli Enterprise Monitoring Server APARs

The following Tivoli Enterprise Monitoring Server APAR fixes are delivered in Fix Pack 7:

- Table 29 lists the APAR fixes that are provided in Fix Pack 7.
- Table 30 on page 116 lists the APAR fixes that are included in Fix Pack 7 and were originally fixed in the interim fixes for Fix Pack 6. *All the interim fixes for Fix Pack 6 are included in Fix Pack 7.*

Table 29. Tivoli Enterprise Monitoring Server APARs that are fixed in Fix Pack 7

APAR Number	Symptom, as described in the APAR database
IY86005	Use of relative paths with the tacmd addBundles, tacmd listBundles, or tacmd removeBundles commands fails. Specifically, the use of a period (".") in the path causes problems, as the path will be mangled internally such that the bundles will not be found at the path specified by the user.

Table 29. Tivoli Enterprise Monitoring Server APARs that are fixed in Fix Pack 7 (continued)

APAR Number	Symptom, as described in the APAR database
IY89278	After updating an endpoint, the agentdepot directory not cleaned up.
IY91192	Executing tacmd viewAgent against a universal agent subnode with a non-standard product code (e.g. *NOT* UA or UM) causes the TEMS to crash Executing tacmd viewAgent against a universal agent subnode with a non-standard product code (e.g. *NOT* UA or UM) causes the deployment controller module on the TEMS to crash when the deployment controller attempts to execute the GETCONFIG query.
IY91527	The product provided situation MS_OFFLINE would not fire for nodes that were OFFLINE when the TEMS started and didn't come online. For example, if a HUB is restarted and a node does not come online the MS_OFFLINE situation will not fire. However if the HUB is restarted and the node does come online but then doesn't heartbeat or is stopped, the situation WILL fire.
IY93640	KRARLOFF.EXE did not run on the i5/OS agent on AS400 systems.
IY94519	The following message: (45B81EA7.0006-AA0: ko4tobje.cpp,2296,″ibTable: : find_string″) No records in cache table <22CAB18>, should only be displayed if STATE level error recording is requested.
IY95449	tacmd createnode could fail over non standard SSH node.
IY96019	SOAP requests with double quotes within the <item> were not being issued because of parsing errors.
IY96580	CT_Reset does not reset events correctly to the NODE value. After TEPS recycle the event status is not correct.
IY98783	Customers were complaining that large amounts of the error message were occurring in their traces when they recycled their HUB TEMS.
IY98977	If a situation has the MISSING clause in it, then the resulting TEC event has the msg slot value truncated due to the way the predicates with ( ) are handled by the code.
IY99396	Customers create a large number of Users in their TEP/S, then turn on security, then find out that the case the TEPS created the users with doesn't match the case on the OS for the HUB TEMS. To the customer, this is fine, as they are still allowed to login to their TEP with mismatched case, as well as use the tacmd login command without problems. It's not until they try to use the workspaces import/export/list functions that they run in to this problem.
IZ00146	When running tacmd addSystem with the -p _UNIX_STARTUP_.Username=xxxxxxxx INSTANCE=xxxxxxxx options, the unix agent startup files are not being updated. So when the agent is restarted it doesn't run using the supplied username/instance information.
IZ01503	ITM situation events from new UA application not being forwarded to TEC.
IZ01568	TEMS crashes with IndexOutOfBounds exception from kdystr when doing remote deploy commands like updateAgent.
IZ01896	tacmd createnode failed if the target machine was HP-UX and the name of the targeted disk partition was more than eight charaters. This was fixed by upgrading the fixpack level of RXA 2.2 used by agent deploy.
IZ01936	Viewsit output shows incorrect for autostart column
IZ02073	TEC Synchronization Installer can't create target rule base if the name is substring of another rule base. The Event Synch installer stops after error.
IZ02730	Recycling RTEMS causes raised events from the same situation distributed to agents attached to other RTEMS to be closed at the TEC server
IZ02751	Tacmd createNode does not provide enough debug information when the -o JLOG_LEVEL=DEBUG_MAX option is included. Additional tracing of RXA functions and additional diagnostic messages have been added.
IZ03564	PROVIDING RXA TRACING AND IMPROVED DIAGNOSTIC MESSAGES FOR REMOTE DEPLOY BPS_CREATED_DEFECT
IZ03567	Improve deployment performance by reduction of download size.

Table 29. Tivoli Enterprise Monitoring Server APARs that are fixed in Fix Pack 7 (continued)

APAR Number	Symptom, as described in the APAR database
IZ04897	tacmd viewsit displays incorrect distribution list for situations that has the same name as that of a workflow.
IZ05054	tacmd listsit -m output is incorrect for RTEMS.
IZ05672	The tacmd createNode processing aborts with exception when the depot contains invalid non-numeric directory names.
IZ06474	In an FTO environment, the mirror node goes OFFLINE at the acting Hub, even though it is still active.
IZ06558	Some error messages generated by utilities on the endpoint are not propogated to the User. When performing any of the remote deployment commands there are times when the error messages and code produced by the utilities executed on the endpoint are not returned to the user. The user may receive a ″success″ message when the operation failed.
IZ06864	Agents fail to reconnect using default KDS_NCSLISTEN at TEMS Because of this APAR fix, the workaround that is described in the readme for Fix Pack 6 is no longer necessary.
IZ09686	tacmd listsystemlist fails when lists with combined affinities are present.
IZ10196	When small LA fixes are applied to endpoint and machine is fast the update is applied, and the endpoint Agents are restarted successfully. However, Remote Deploy TEMS code does not detect the endpoint Agent restart and therefore Remote Deploy reports timeout error to user.
IZ11410 (IZ09613)	WINDOWS HANDLE leak in KDSMAIN while reflex actions.
IZ11449	TEC displays PARSING_FAILED~'LINE 1: SYNTAX ERROR' If an ITM event data contains single quotes after escaped semi-colon or tilde, the single quote(s) is not properly escaped causing parsing error on the TEC server.
IZ11560	TEMS crashes when an invalid pointer in a filter handle is passed to a function. The complete failing call stack can differ but the stacks will have a line similar to the following: #4 0x080e45d1 in VSF12_SetupFilter ()
IZ13791	The ″tacmd updateAgent″ command cannot be used to update an agent which is located on a Thai locale machine. The problem is that th_TH (The Thai identifier) is not present in the locale tables used to map locales to codepages, instead ti_TI is present.
IZ15697	Situation generates events for agents after they are removed from an MSL.
IZ16693	When remotely configuring a T6 (ITCAM) Agent using the TEP Console, the TEMS Server stops functioning
IZ17050	PROCESS_NAME.RAS log grows without bound. Errant process results in system crash because error-handling recursion causes unbounded growth of process_name.RAS file thereby filling entire file system.
IZ18174	In the originnode adjustment method (ko4async.cpp) various variables are pointers to within the event record. When the size of the event record is close to max buffer allotment, an APPEND method for SITCOUNTKEY forces the record to be reallocated. This causes a TEMS crash when any of the pointer variables are referenced.
IZ18916	A Situation may fail to run on an agent when it is connected to a given RTEMS. This condition can occur if agent switching occurs while an RTEMS is down and situations are distributed to those agents via MSLs. The problem will likely affect large installations as for the symptom to manifest, the processes of building the in-core Access List and of synchronising the Node List tables must overlap.
IZ18978	If an ITM event data contains single quotes after escaped semi-colon or tilde, the single quote(s) is not properly escaped causing parsing error on the TEC server.
IZ19608	MAX_NODES in kfaadxwa.h is set to 32 which causes the following message from kfaxins2.c when this value is exceeded: ″KO4X_AddNode″) Adding node would exceed 32 maximum.
IZ19733	A Take Action command executed twice.

Table 29. Tivoli Enterprise Monitoring Server APARs that are fixed in Fix Pack 7 (continued)

APAR Number	Symptom, as described in the APAR database
IZ19991	Data returned as results of queries to CICS agents configured with subnodes that have similar names are not complete. For example, if the CICS agent contains subnodes named CI308 and CI308W, just the data from the subnode CI308W is returned by the query; no data from subnode CI308 will be present.
IZ19993	Situations created for tables defined as being a PureEvent type, distributed and associated to a specific subnode, becomes true when the condition is satisfied by any subnode of the same agent.
IZ20004	ITM WINDOWS OS AGENT DOES NOT START ON WINDOWS SERVER 2008 IBM Tivoli Monitoring Windows OS Agent fails to start on Microsoft Windows Server 2008 operating systems due to problems loading several dll's. Problem symptoms: 1. Memory dumps during agent startup. 2. Error Message ″The service did not respond to the start or control request in a timely fashion." 3. Agents installed on Windows Server 2008 are not displayed under ″Windows System″ node like other Windows OS agents.

Table 30. Tivoli Enterprise Monitoring Server APARs that were fixed in the interim fixes for Fix Pack 6

APAR Number	Symptom, as described in the APAR database
IY80913	When using ″tacmd createNode″ to create a new Windows node we often get a failure because the level of GSKIT gets upgraded as part of the install and this requires a reboot of the remote node creating a failure in the installation process. **Note:** This APAR was first resolved in the following interim fix (IF) for Fix Pack 6: `6.1.0.6-TIV-ITM-IF0005`.
IY91952	The validation XML file for the command does not contain the characters in the regular expression that declares the legal characters for the -pl--propertyl--properties command line option. **Note:** This APAR was first resolved in the following interim fix (IF) for Fix Pack 6: `6.1.0.6-TIV-ITM-IF0005`.
IY93032	CTIRA_HOSTNAME environment variable can be used on to override the default Originnode name for the agent. Sometimes users include invalid characters like double quotes, when they set this parameter. A code was added in kfa to check for invalid characters in Originode and prevent agent from registering, if invalid characters are found. The validation takes place only if CMS_NODE_VALDIATION=Y environment variable is set on TEMS. If it is not set, the agent with invalid characters in Originnode can still be able to register. This particular problem was caused by the presence of double quotes around the Originnode name which prevented the user from deleting the entry from the managed system list (INODESTS). **Note:** This APAR was first resolved in the following interim fix (IF) for Fix Pack 6: `6.1.0.6-TIV-ITM-IF0001`.
IY95452	The **tacmd createNode** command creates an ″install.rsp″ file which is used to install the OS agent. However, this generated file does not always contain all of the necessary options, especially with regard to secondary protocols and their settings. A method has been created to allow the customer to create this file and have the **createNode** command use it instead of the generated default file. **Note:** This APAR was first resolved in the following interim fix (IF) for Fix Pack 6: `6.1.0.6-TIV-ITM-IF0001`.
IY95593	″tacmd listsystems -t -s″ option does not work on Linux. The return code from SOAP was not initialized to 0 which made the checking logic fail in spite of success being returned by SOAP. **Note:** This APAR was first resolved in the following interim fix (IF) for Fix Pack 6: `6.1.0.6-TIV-ITM-IF0001`.
IY96156	When agents switch away from their owning remote monitoring server due to an outage of that monitoring server, and then switch back again, situations no longer return events. Due to the maintenance of duplicate **objectaccesslist** records at the hub monitoring server, when the agents switch back to the original RTEMS the HUB TEMS thinks that the situations are already running and does not restart them. **Note:** This APAR was first resolved in the following interim fix (IF) for Fix Pack 6: `6.1.0.6-TIV-ITM-IF0001`.

Table 30. Tivoli Enterprise Monitoring Server APARs that were fixed in the interim fixes for Fix Pack 6 (continued)

APAR Number	Symptom, as described in the APAR database
IY99229	A segmentation exception was occurring in a function within the TEMS while dropping an object. A chain pointer had been corrupted by a previous drop call that did not hold the correct lock. **Note:** This APAR was first resolved in the following interim fix (IF) for Fix Pack 6: `6.1.0.6-TIV-ITM-IF0001`.
IY99621	A remote TEMS attached via ephemeral pipe will leave ″stale″ GLB entries (of the form ″0.0.0.n″) at the HUB if the remote TEMS re-registers without an intervening normal shutdown (where it explicitly unregisters the problem entries). Typically this occurs when a remote TEMS crashes after connecting to the HUB. Once this crash happens, the HUB will find old, stale remote TEMS entries first, and cause distributed requests to that REMOTE to fail with connection errors (these errors will contain the stale TEMS address) even though the remote and any attached agents appear online. **Note:** This APAR was first resolved in the following interim fix (IF) for Fix Pack 6: `6.1.0.6-TIV-ITM-IF0001`.
IZ01019	Distribute a situation to an MSL (it can contain one or more Managed servers). Make sure that it is started on the Navigation console. Then remove the MSL from the distribution list and check that the situation stays in open state on the Navigation console until HUB is recycled. **Note:** This APAR was first resolved in the following interim fix (IF) for Fix Pack 6: `6.1.0.6-TIV-ITM-IF0001`.
IZ01120	When a node is removed from an MSL, all distributions for that node are removed, not just the ones related to the MSL. **Note:** This APAR was first resolved in the following interim fix (IF) for Fix Pack 6: `6.1.0.6-TIV-ITM-IF0001`.

IZ01132	The TEMS crashes periodically with a core dump stack trace similar to the following:
	`(gdb) bt`
	`#0 0x400007a2 in _dl_sysinfo_int80 () from /lib/ld-linux.so.2`
	`#1 0x4035e7a5 in raise () from /lib/tls/libc.so.6`
	`#2 0x40360209 in abort () from /lib/tls/libc.so.6`
	`#3 0x402e31f7 in __cxa_call_unexpected () from /usr/lib/libstdc++.so.5`
	`#4 0x402e3244 in std::terminate () from /usr/lib/libstdc++.so.5`
	`#5 0x402e3787 in __cxa_pure_virtual () from /usr/lib/libstdc++.so.5`
	`#6 0x42c33570 in RequestImp::Start () from`
	`/banktools/itm6/li6243/ms/lib/KRANDREG`
	`#7 0x42c2f9a8 in ProxyRequest::Restart () from`
	`/banktools/itm6/li6243/ms/lib/KRANDREG`
	`#8 0x42c4bfb4 in DataServerRequest::ProcessStoredList () from`
	`/banktools/itm6/li6243/ms/lib/KRANDREG`
	`#9 0x42c4bdf6 in DataServerRequest::StartPersistScan () from`
	`/banktools/itm6/li6243/ms/lib/KRANDREG`
	`#10 0x42c247bc in ThreadTask::ExecuteUserTask () from`
	`/banktools/itm6/li6243/ms/lib/KRANDREG`
	`#11 0x42c24657 in startThread () from /banktools/itm6/li6243/ms/lib/KRANDREG`
	`#12 0x401ff371 in start_thread () from /lib/tls/libpthread.so.0`
	`#13 0x403feffe in clone () from /lib/tls/libc.so.6`
	Note: This APAR was first resolved in the following interim fix (IF) for Fix Pack 6: `6.1.0.6-TIV-ITM-IF0005`.

IZ01791	During a remote TEMS recycle: The remote cat/atr files for one or more applications was backlevel at the remote TEMS compared to the hub TEMS. During history uadvisor processing, the khd processing noticed that the data included ″unknown″ columns and used a remote SQL to hub TEMS to get the syscolumns data. This was very cpu and elapsed time intensive and as a result the main SITMON thread got monopolized and could not handle or process heartbeat requests. Thus all agents appeared to be offline at the hub TEMS.
IZ02774	Unable to create system list of type UM using the tacmd createsystemlist command. **Note:** This APAR was first resolved in the following interim fix (IF) for Fix Pack 6: `6.1.0.6-TIV-ITM-IF0001`.
IZ03917	RTEMS takes a long time to shutdown if the HUB is gone. **Note:** This APAR was first resolved in the following interim fix (IF) for Fix Pack 6: `6.1.0.6-TIV-ITM-IF0005`.

Table 30. Tivoli Enterprise Monitoring Server APARs that were fixed in the interim fixes for Fix Pack 6 (continued)

APAR Number	Symptom, as described in the APAR database
IZ03993	FAULT resulting from failed ACCEPT() calls. HANG due to unexpected status from receive. HANG due to shared condition variables. LOOP due to unexpected status on loopback session. PERF TCP/IP_NODELAY disabled on z/OS.
IZ04294	Added a new option to the listsystems command to display the non standard IBM managed systems. The new options are as follows: `-ns │ --nonstandard`. . **Note:** This APAR was first resolved in the following interim fix (IF) for Fix Pack 6: `6.1.0.6-TIV-ITM-IF0001`.
IZ04639	Message 1DE00070=KDE1_STC_BADPIPEHANDLE will be seen in the RKLVLOG immediately prior to the ABEND. There's a very small timing window that opens when a connection is broken, and the pipe listener thread is processing an event list containing the disconnected ASD. **Note:** This APAR was first resolved in the following interim fix (IF) for Fix Pack 6: `6.1.0.6-TIV-ITM-IF0002`.
IZ04644	ITM 6.1 kdsmain process terminates with a segmentation fault producing a core file. The failure is the result of a storage overlay. . **Note:** This APAR was first resolved in the following interim fix (IF) for Fix Pack 6: `6.1.0.6-TIV-ITM-IF0001`.
IZ05394	tacmd exportWorkspaces gets error (generates java.lang.NullPointerException) if user password starts with ″ ″ character, or with ″&″ on Linux/UNIX platforms. **Note:** This APAR was first resolved in the following interim fix (IF) for Fix Pack 6: `6.1.0.6-TIV-ITM-IF0003`.
IZ08198	Very slow startup time for remotes in large environment. The problem has to do with new agents coming on-line. The Hub is generating EIB records for every agent in the MSL. Upon receiving these EIB events, the remote then writes them into the local access list table blindly. The remote should not have stored those entries marked as _FAGEN. **Note:** This APAR was first resolved in the following interim fix (IF) for Fix Pack 6: `6.1.0.6-TIV-ITM-IF0001`.
IZ08818	There is a performance issue for history uadvisors when the catalog file is back level (missing columns) or does not exist. When a history uadvisor is started and the catalog file is either back level or does not exist, iterative SQL calls are issued to the SYSCOLUMNS table. This results in excessive I/O and impedes the startup of the uadvisor. **Note:** This APAR was first resolved in the following interim fix (IF) for Fix Pack 6: `6.1.0.6-TIV-ITM-IF0001`.
IZ09522	TEMS crashes when sit returns large amount of data. If a situation returns more than 999 buffers of event data, the TEMS can crash in the TADVSIOR code when formatting the sequence field causing stack overlay. **Note:** This APAR was first resolved in the following interim fix (IF) for Fix Pack 6: `6.1.0.6-TIV-ITM-IF0005`.
IZ09714	Segmentation fault in pthread_mutex_init when an IP.PIPEconnection receives an inbound DISCONNECT notification while the connection is still in setup (XID exchange in-progress). The fault is due to the unconditional use of the CCB pointer in KDEP1_AttachChannel. This fault is typically preceded by the following RAS1 log message: Status 1DE0000B=KDE1_STC_DISCONNECTED=32: Broken pipe . **Note:** This APAR was first resolved in the following interim fix (IF) for Fix Pack 6: `6.1.0.6-TIV-ITM-IF0002`.
IZ10689	SNA setup hangs with locking embrace. Intra-process SNA pipes that are created to prevent deadly embraces when SNA conversations are attempted back to the originating process do not carry the correct port. Since the port number is wrong, the SNA interface is attempting to start a real SNA conversation (with itself) rather than the correct behavior which is utilization of the loopback pipe. The real SNA conversation setup hangs with a locking embrace and the RTEMS will basically be unusable. This error can be exposed any time a REMOTE TEMS has SNA configured, and the REMOTE starts before the HUB. This can happen even when SNA is not the preferred protocol. This was also fixed in the TEMA via APAR IZ10691. **Note:** This APAR was first resolved in the following interim fix (IF) for Fix Pack 6: `6.1.0.6-TIV-ITM-IF0001`.
IZ10696	Subnodes do not come back online after the HUB is recycled. While the HUB tems was down, the RTEMS tried to re-establish a distributed request to the HUB. As a result, the local TEMS heartbeat can be blocked and times out. When FA detected the lost of local TEMS heartbeat, it proceeded to mark all agent/subnodes attached to it to offline. Since subnodes only registers once and does not heartbeat, once marked offline, they will not come back online again even when the local TEMS heartbeats again. **Note:** This APAR was first resolved in the following interim fix (IF) for Fix Pack 6: `6.1.0.6-TIV-ITM-IF0001`.

Table 30. Tivoli Enterprise Monitoring Server APARs that were fixed in the interim fixes for Fix Pack 6 (continued)

APAR Number	Symptom, as described in the APAR database
IZ10759	Agent workspaces are empty on the Tivoli Enterprise Portal even though the nodes are online. In a large environment with many agents, the Tivoli Enterprise Portal Server **nodestatus** request can be delayed, either by other processing in the portal server or at the monitoring server. If during this delay, two consecutive heartbeats are received from a node with no state change (for example, two `o4online='Y'` statements), the incore **nodestatus** entry will have the EVENT flag reset. This normally is ok because all incoming **nodestatus** are put on a queue waiting for retrieval. However if during this delay, the **nodestatus** garbage collect task was run, all queued entries will be removed and the request will revert back to reading from incore **nodestatus** table next time the request is redriven. However since the EVENT flag is now turned off in the status record, these records are filtered away and never sent back to the portal server. In this case, it was the remote monitoring server node statuses being filtered away. So in the portal, the agents are online but their controlling remote monitoring server is not. The portal server does not even attempt to issue the report request, resulting in empty workspaces. **Note:** This APAR was first resolved in the following interim fix (IF) for Fix Pack 6: `6.1.0.6-TIV-ITM-IF0001`.
IZ11497	A **netstat** display of active connections shows sockets associated with the Tivoli Enterprise Monitoring Server (**http daemon**) process on port 1920 in the CLOSE_WAIT state. This results when the **http daemon** is operating in 'header mode' and receives a disconnect from the session partner. The socket pair remain in CLOSE_WAIT until the monitoring server process terminates. **Note:** This APAR was first resolved in the following interim fix (IF) for Fix Pack 6: `6.1.0.6-TIV-ITM-IF0002`.
IZ12842	A situation that is distributed to a managed server list (MSL) may not run at an agent even though it is running on another agent that belongs to the same MSL and which is connected to the same Tivoli Enterprise Monitoring Server. Neither restarting the agent nor the situation will start the situation on the agent. The situation may start running on the agent if the agent switches to another monitoring server. **Note:** This APAR was first resolved in the following interim fix (IF) for Fix Pack 6: `6.1.0.6-TIV-ITM-IF0005`.
IZ13313	Right after remote monitoring server start up, the message log shows a series of 1120 errors. **Note:** This APAR was first resolved in the following interim fix (IF) for Fix Pack 6: `6.1.0.6-TIV-ITM-IF0003`.
IZ14201	On-line subnodes of agents that are connected to an remote monitoring server appear to be off line in Tivoli Enterprise Portal. See also OA23794. **Note:** This APAR was first resolved in the following interim fix (IF) for Fix Pack 6: `6.1.0.6-TIV-ITM-IF0005`.
IZ16736	TEMS on a z/OS machine may hang during shutdown. **Note:** This APAR was first resolved in the following interim fix (IF) for Fix Pack 6: `6.1.0.6-TIV-ITM-IF0005`.
IZ16738	Agents may fail to restart some situations after the agent has reconnected to its monitoring server. This applies only to agents on distributed platforms, not to z/OS agents. **Note:** This APAR was first resolved in the following interim fix (IF) for Fix Pack 6: `6.1.0.6-TIV-ITM-IF0005`.

Table 30. Tivoli Enterprise Monitoring Server APARs that were fixed in the interim fixes for Fix Pack 6 (continued)

APAR Number	Symptom, as described in the APAR database
IZ16739	If Warehousing Proxy Agent (WPA) is not running or WPA fails to warehouse the data, then no STH file trim is done and the STH file grows unrestricted. A new variable has been introduced, called KHD_TOTAL_HIST_MAXSIZE to control this behavior. KHD_TOTAL_HIST_MAXSIZE represents the total size of all binary files in historical files directory expressed in MBytes. The default behavior will be the same as currently, i.e. no growth limit. The default behavior will be achieved by setting the default value for KHD_TOTAL_HIST_MAXSIZE to zero. If this variable is not added, the default behavior is no growth limit. Collection on the TEMA: 1. If you want to limit the size of the short history files stored for Linux OS agent (lz), you will need to add this variable to a common configuration file in a location of your choosing: KHD_TOTAL_HIST_MAXSIZE=5 (5 MB of storage) 2. Add the following statement to *each agent's configuration file: For example:CANDLEHOME/config/lz.ini or KNTENV KBB_ENVPATH==<fully qualified path to common configuration file> *There is no global process/agent that can monitor the short term history files for all agents on the TEMA. Collection on the TEMS (calculates STH file size for all agents): 1. Add the following to the TEMS ENV file if Windows or INI file if Linux/UNIX: KHD_TOTAL_HIST_MAXSIZE=5 (5 MB of storage). **Note:** The OS agent is required to get the latest shared common code that is required for this warehouse fix. **Note:** This APAR was first resolved in the following interim fix (IF) for Fix Pack 6: `6.1.0.6-TIV-ITM-IF0005`.
IZ16775	TEMS configured as Backup SYSPLEX Proxy hangs in shutdown if Primary SYSPLEX Proxy is not shutdown first. **Note:** This APAR was first resolved in the following interim fix (IF) for Fix Pack 6: `6.1.0.6-TIV-ITM-IF0005`.
IZ16776	The 'HISTORICAL SUMMARIZED AVAILABILITY' workspace view shows negative numbers. **Note:** This APAR was first resolved in the following interim fix (IF) for Fix Pack 6: `6.1.0.6-TIV-ITM-IF0005`.

Tivoli Enterprise Portal APARs

The following APARs are addressed in Fix Pack 7. This section includes a separate table of fixes for the Tivoli Enterprise Portal client. The tables list the APAR fixes that are included in Fix Pack 7 and were originally fixed in the interim fixes for Fix Pack 6. *All the interim fixes for Fix Pack 6 are included in Fix Pack 7.*

Table 31. Tivoli Enterprise Portal client APARs that are fixed in Fix Pack 7

APAR Number	Symptom, as described in the APAR database
IY90505	When multiple events are selected in the event console for acknowledgement and notes are added, only the first event selected has notes added. All other events are only acknowledged.
IY92098	After sorting History Collection, information for selected row does not match
IY96035	French language translations being applied to certain portions of ITM when no language packs are installed.
IY98725	TEP client was allowing special characters to be used in situation and MSL names ($%-).
IY99836	Tep client allows the product provided situation MS_Offline to be distributed to managed systems other than the hub tems.
IZ01324	Count function not available for ″String″ type columns.
IZ02932	When the tep clients historical configuration dialog is first opened, if you select the first group in the drop down list the controls to configure the dialog are disabled.

Table 31. Tivoli Enterprise Portal client APARs that are fixed in Fix Pack 7 (continued)

APAR Number	Symptom, as described in the APAR database
IZ03175	The presentation for the navigator tree view is empty (just a placeholder), and thus an empty presentation is exported to XML, which violates the XML schema. The log file contains the following error: ″ERROR: cvc-complex-type.2.4.b: The content of element ’presentations’ is not complete.″
IZ03222	TEP client hangs if a Graphic View node with a link is double clicked. The problem occurs randomly, when you double-click a link.
IZ07614	TEP lack a way to provide filtering of the first or last n-rows of a request result
IZ12743	Controls for summarization and pruning for group CCC logs in the tep historical configuration dialog are enabled.

Table 32. Tivoli Enterprise Portal APARs that were fixed in the interim fixes for Fix Pack 6

APAR Number	Symptom, as described in the APAR database
IY93225	Correlated situations cannot be associated with navigator items in custom Navigator Views. They can be associated with navigator items in the Physical Navigator View fine. **Note:** This APAR was first resolved in the following interim fix (IF) for Fix Pack 6: `6.1.0.6-TIV-ITM-IF0001`.
IZ02417	When saving a situation that contains an embedded situation or an until clause that waits on a situation, the client first checks to make sure the until/embedded situation has a common distribution with the parent situation. The same code path is used for both types of situations, but extra logic is executed for until situations. This extra logic was also being executed for embedded situations and was causing the entire situation collection to be scanned on the Tivoli Enterprise Portal server. This operation can take several minutes in environments with a high number of situations. **Note:** This APAR was first resolved in the following interim fix (IF) for Fix Pack 6: `6.1.0.6-TIV-ITM-IF0001`.
IZ03852	When running migrate-export, or reconfiguring the Tivoli Enterprise Portal Server to point to a different hub (Windows portal server only), the migrate-export script may report the following error message: `"Error deleting query object"`. The **saveexport.sql** dump file will be incomplete. **Note:** This APAR was first resolved in the following interim fix (IF) for Fix Pack 6: `6.1.0.6-TIV-ITM-IF0001`.

Tivoli Enterprise Portal Server APARs

The following Tivoli Enterprise Portal Server APAR fixes are delivered in Fix Pack 7:

- Table 33 lists the APAR fixes that are provided in Fix Pack 7.
- Table 34 on page 122 lists the APAR fixes that are included in Fix Pack 7 and were originally fixed in the interim fixes for Fix Pack 6. *All the interim fixes for Fix Pack 6 are included in Fix Pack 7.*

Table 33. Tivoli Enterprise Portal Server APARs that are fixed in Fix Pack 7

Header	Header
IY92133	In the physical tree, nodes for a z/OS LPAR exist both inside the Sysplex folder, and outside the Sysplex folder at the same level. The systems under each LPAR node are identical.
IY96004	When a minor change is made to a universal agent metafile, the new ODI file is uploaded to the TEPS, but any changes to attribute definitions is not shown in the client. The only way to see the new ODI data is to restart the TEPS. **Note:** TEPS restart is not needed but TEP has to be restarted in any case to see the changes after the fix is in place.
IY97174	User creates a new query and clicks OK or Apply to save the query, and no error messages are shown. Upon returning to the query editor, the query is not shown in the list of queries. Examining the TEPS log shows the following error message: [IBM][CLI Driver][DB2/NT] SQL0433N Value ″tableCount=1@table1.name=KFWQUERY@ta ble1.columnCount=0@prope″ is too long. SQLSTATE=22001

Table 33. Tivoli Enterprise Portal Server APARs that are fixed in Fix Pack 7 (continued)

Header	Header
IY97433	When opening an XML file generated by KfwTMSDLA, it reports an error that a semicolon is missing. The problem occurs only when the XML file to be generated contains an ampersand character (&). If this instance of the ampersand character represents the literal character (for example, to signify the word "and"), you can replace the ampersand with the character code for ampersand (`&amp;`).
IY97555	Two different symptoms can occur depending on whether KFW_STARTJVM=Y or N is specified. 1. When the TEPS is started with KFW_STARTJVM=Y and it reaches the end of memory, KfwServices goes into a loop. It will use about 50% CPU for as long as you let it run. Issuing a kill -9 seems to be the only way to terminate the process. 2. When the TEPS is started with KFW_STARTJVM=N and it reaches the end of memory, KfwServices crashes with a segmentation fault (sig 11). The dump will show a malloc with a null pointer.
IY97946	The TEPS is incorrectly adding a prefix to columns which have the PRIMARYKEY option specified in the ODI file along with a BEHAV type.
IY98679	The red icon is not set for a logical object after TEP client logout/login, if the object is at the same hierarchical level of other logical objects, all assigned to the same physical managed node and all under a common logical parent node.
IZ00497	InstallPresentation step fails during upgrade or manual execution.
IZ00883	During a system reboot, if the TEPS backend database has not finished starting before TEPS attempts to start, the TEPS will immediately abort startup.
IZ03346	If a managed object name is greater than 64 characters, the attempt toinsert a record into the KFWTSIT table will fail, and data for that situation will not appear in the event details workspaces.
IZ05421	Seeding for ITM 6.1 Agent for ITM 5.1.2 Endpoint fails on Linux/AIX with an error stating libjvm.so not found.
IZ05457	When adding situations via the tacmd command line utility, the TEP client experiences slow performance and/or temporarily hangs for anywhere from one to several minutes.
IZ07556	Situations created via tacmd are not displayed as being associated with a navigator node until after the TEPS is recycled.
IZ08803	When issuing a long term history request, the result set includes data for all managed systems of the type being queried, instead of just data for the systems in the topology node's assigned managed systems list.
IZ10303	Timeouts can occur during periods of even moderate activity, because the CTAuthorization timeout interval default value of 2 minutes is too low.

Table 34. Tivoli Enterprise Portal Server APARs that were fixed in the interim fixes for Fix Pack 6

APAR Number	Symptom, as described in the APAR database
IY97053	Running migrate-export more than ~30 times during a single Tivoli Enterprise Portal Server session causes all Tivoli Enterprise Portal clients to hang, new clients are unable to log in, and the following message appears many times in the portal server log: `ERRMSG: Warning: 32 active connections. Retry #4 on datasource`. The migrate-export scripts use the **KfwSQLClient** utility to send SQL requests to the portal server. One of these requests was not closed properly after it was finished. This resulted in a leaked database connection to the Tivoli Enterprise Portal Server DB. Once the Tivoli Enterprise Portal Server DB2 connection limit was reached, no new connections to the Tivoli Enterprise Portal Server DB could be opened. **Note:** This APAR was first resolved in the following interim fix (IF) for Fix Pack 6: `6.1.0.6-TIV-ITM-IF0001`.

Table 34. Tivoli Enterprise Portal Server APARs that were fixed in the interim fixes for Fix Pack 6 (continued)

APAR Number	Symptom, as described in the APAR database
IZ01185	View on a custom navigator node shows no data, displays error rc=350. There are other possible reasons for a query to return anrc=350 error code that do not necessarily indicate an error with this maintenance delivery. For other return codes,(ex. rc=5), please ensure the query is being distributed to the correct managed systems. Refer to the *IBM Tivoli Monitoring User's Guide* for more information. **Note:** This APAR was first resolved in the following interim fix (IF) for Fix Pack 6: `6.1.0.6-TIV-ITM-IF0005`.
IZ02344	After a recycle of the hub TEMS, the situation event console shows situations as stopped even though they are actually running. **Note:** This APAR was first resolved in the following interim fix (IF) for Fix Pack 6: `6.1.0.6-TIV-ITM-IF0001`.
IZ02988	Setting KFW_TOPOLOGY_CLUSTER_LIST causes all MQ agents to be grouped by the middle part of the system name. The default is for MQ agents to have a blank middle part, so those agents are grouped under the managing TEMS name. **Note:** This APAR was first resolved in the following interim fix (IF) for Fix Pack 6: `6.1.0.6-TIV-ITM-IF0001`.
IZ03955	After creating a new situation via the tacmd command line utility which is distributed to a non-existent managed system list, no MSL with that name is displayed in the MSL editor. In addition, a new MSL can not be created with that name. . **Note:** This APAR was first resolved in the following interim fix (IF) for Fix Pack 6: `6.1.0.6-TIV-ITM-IF0001`.
IZ06981	The newly created workspace in admin mode on a user defined subnode was not visible for the other user. **Note:** This APAR was first resolved in the following interim fix (IF) for Fix Pack 6: `6.1.0.6-TIV-ITM-IF0005`.
IZ07920	Situation Event Console gets out of sync with the Common Event Console. **Note:** This APAR was first resolved in the following interim fix (IF) for Fix Pack 6: `6.1.0.6-TIV-ITM-IF0001`.
IZ09453	After a random period of time, a query on a TEP workspace associated with a logical navigator node stops returning data. **Note:** This APAR was first resolved in the following interim fix (IF) for Fix Pack 6: `6.1.0.6-TIV-ITM-IF0005`.
IZ09511	After a certain number of users has logged in, the Tivoli Enterprise Portal Server will crash and generate a core dump. The portal server logs will have the following error message: `pthread_create, error: 12`. In addition, there might be other error or exception messages related to no resources, object deletion errors, and **pullSequence** errors. The number of users ranges from 20-30 concurrent users. **Note:** This APAR was first resolved in the following interim fix (IF) for Fix Pack 6: `6.1.0.6-TIV-ITM-IF0001`.
IZ10359	The distinct problems when displaying numeric data obtained via the JDBC in the Tivoli Enterprise Portal. 1. The portal client does not show any decimal point for data obtained via JDBC through custom queries. 2. The portal client may show decimal data from an Oracle database with an incorrect scale, when the data has trailing zeros to the right of the decimal point. 3. The portal client displays numbers (which have been unscaled) greater than 4294967294 (larger than 31 bit + sign) incorrectly. Sometimes as a negative number but always wrong. **Note:** This APAR was first resolved in the following interim fix (IF) for Fix Pack 6: `6.1.0.6-TIV-ITM-IF0005`.

IBM Tivoli Data Warehouse APARs

The following installation APAR fixes are delivered in Fix Pack 7:

- Table 35 on page 124 lists the APAR fixes that are provided in Fix Pack 7.
- Table 36 on page 125 lists the APAR fixes that are included in Fix Pack 7 and were originally fixed in the interim fixes for Fix Pack 6. *All the interim fixes for Fix Pack 6 are included in Fix Pack 7.*

Table 35. IBM Tivoli Data Warehouse APARs that are fixed in Fix Pack 7

APAR Number	Symptom, as described in the APAR database
IY93585	When the ″Count weekends as vacation″ option is selected in the configuration of the Summarization and Pruning agent and there is one or more vacation days identified, weekend days were not being considered to be vacation days and the resulting summarizations included weekends as regular days.
IY93720	Misleading ″UNABLE TO OPEN METAFILE...ENABLE.HDR″ Message in *._SY_*.log, which is a erroneous error message **Additional information on this APAR which has been fixed:** Reinstall application support for summarization and pruning on the Tivoli Enterprise Monitoring Server using the **Add TEMS application support** option in the context menu of the Manage Tivoli Enterprise Monitoring Services window and point to the new **ksy_upg.sql** file.
IY99013	Aggregated table not pruned when aggregation and pruning is configured for that metric. **Additional information on this APAR which has been fixed:** The summarization and pruning agent does not prune data for an aggregated metric when pruning is configured for that metric as well as other metrics that are not aggregated. In other words, if you aggregate just one metric and choose to prune also other metrics, the prune per the aggregated metric did not work.
IZ00483	View not created for a specific aggregated table if the table already exists.
IZ01666	100% CPU usage when database stopped while the WPA is running.
IZ02460	WPA crashes randomly on Windows when using Oracle as the TDW database.
IZ05039	Incorrect name created for *sy_java* log for Summarization and Pruning Agent when ibm.tdw.maxNumberDetailTraceFiles parm value is > 9.
IZ06109	S&P uses too much memory with a big number of agents.
IZ11543	Summarization and Pruning Agent startup Error: KSZ_CLASSPATH environment variable is not defined.
IZ12549	Warehousing from agents running on AS/400 fails if agent CCSID is not set to 37.

Table 36. IBM Tivoli Data Warehouse APARs originally fixed in the interim fixes for Fix Pack 6.

APAR Number	Symptom, as described in the APAR database
IZ05539	If Warehousing Proxy Agent (WPA) is not running or WPA fails to warehouse the data, then no STH file trim is done and the STH file grows unrestricted. A new variable has been introduced, called KHD_TOTAL_HIST_MAXSIZE to control this behavior. KHD_TOTAL_HIST_MAXSIZE represents the total size of all binary files in historical files directory expressed in MBytes. The default behavior will be the same as currently, i.e. no growth limit. The default behavior will be achieved by setting the default value for KHD_TOTAL_HIST_MAXSIZE to zero. If this variable is not added, the default behavior is no growth limit. Collection on the TEMA: 1. If you want to limit the size of the short history files stored for Linux OS agent (lz), you will need to add this variable to a common configuration file in a location of your choosing: KHD_TOTAL_HIST_MAXSIZE=5 (5 MB of storage) 2. Add the following statement to *each agent's configuration file: For example:CANDLEHOME/config/lz.ini or KNTENV KBB_ENVPATH==<fully qualified path to common configuration file> *There is no global process/agent that can monitor the short term history files for all agents on the TEMA. Collection on the TEMS (calculates STH file size for all agents): 1. Add the following to the TEMS ENV file if Windows or INI file if Linux/UNIX: KHD_TOTAL_HIST_MAXSIZE=5 (5 MB of storage). **Note:** The OS agent is required to get the latest shared common code that is required for this warehouse fix. **Note:** This APAR was first resolved in the following interim fix (IF) for Fix Pack 6: `6.1.0.6-TIV-ITM-IF0005`.
IZ05791	ITM 6.1 Warehouse Proxy agent fails to process data of BITSTRING datatype. **Note:** This APAR was first resolved in the following interim fix (IF) for Fix Pack 6: `6.1.0.6-TIV-ITM-IF0005`.
IZ09009	ITM 6.1 Warehouse Proxy agent fails to create index for TMZDIFF column. **Note:** This APAR was first resolved in the following interim fix (IF) for Fix Pack 6: `6.1.0.6-TIV-ITM-IF0005`.

Tivoli Universal Agent APARs

The following installation APAR fixes are delivered in Fix Pack 7:

- Table 37 lists the APAR fixes that are provided in Fix Pack 7.
- Table 38 on page 126 lists the APAR fixes that are included in Fix Pack 7 and were originally fixed in the interim fixes for Fix Pack 6. *All the interim fixes for Fix Pack 6 are included in Fix Pack 7.*

Table 37. Tivoli Universal Agent APARs that are fixed in Fix Pack 7

APAR number	Symptom, as described in the APAR database
IY94286	When using Remote Data Provider, the Data Provider does not reconnect to the target Universal Agent if that target Universal Agent is stopped and restarted.
IZ11625	A //SUMMARY attribute group in a SNMP Data Provider metafile will not collect any data because the SNMP Data Provider is not supporting the feature, whereas other Data Providers are supporting //SUMMARY.
IZ13897	When running Universal Agent on Unix/Linux platforms and monitoring SNMPv2 traps, the Source Name value displayed in 'TRAP' TEP report is incorrect; this APAR does not apply if Universal Agent is receiving SNMPv1 traps.
IZ15544	Universal Agent alternate instance can not register with SNMP trap listening process when Universal Agent is running on a multi-home machine.

Table 37. Tivoli Universal Agent APARs that are fixed in Fix Pack 7 (continued)

<table>
<tr><th>APAR number</th><th>Symptom, as described in the APAR database</th></tr>
<tr><td>IY92465</td><td>When using the //RECORDSET <records> statement, the UA File Data Provider concatenates all file records up to the maximum of number of records indicated by <records> or until it reaches the end of the file, whichever comes first. For example you can use the following statement:
<pre>
//APPL R01_AppName @Testing IY92465
//NAME R01_Name E
//SOURCE FILE /tmp/some.log tail
//RECORDSET 100
//ATTRIBUTES NONE
AnythingHere R 2048
</pre>
The UA File DP concatenates 100 records or until it reaches the end of the file. The IBM Tivoli Monitoring documentation indicates maximum value allowed for number of records is 32767. UA File Data Provider has a limit of 100,000 characters it can hold in its internal buffer. When using this record concatenation capability the calculation applied is : File's Record Length x RecordCount <= 100,000; for example 100 records with 1000 characters each or 10,000 records with 10 characters each. If this limit is exceeded and one or more of the defined attribute values are located beyond the 100,000th byte, those attribute values will be missing; the Tivoli Enterprise Portal will show incomplete records or truncated records. For example, if each record start with a number and you send less than the limit you will see data like the following:
<pre>
01 This is an example of data record starts with a number ....
20 This is an example of data record starts with a number ....
33 This is an example of data record starts with a number ....
</pre>
If the limit is exceeded you may see truncated lines like the following:
<pre>
01 This is an example of data ....
mple of data record starts with a number ....
ta record starts with a number ....
</pre></td></tr>
</table>

Table 38. Tivoli Universal Agent APARs originally fixed in the interim fixes for Fix Pack 6.

<table>
<tr><th>APAR number</th><th>Symptom, as described in the APAR database</th></tr>
<tr><td>IY92231</td><td>On UNIX platforms, it is not possible to group multiple blank-separated script arguments and pass them as a single argument to the Script Data Provider. Instead, each blank-separated argument is always treated separately. <b>Note:</b> This APAR was first resolved in the following interim fix (IF) for Fix Pack 6: <code>6.1.0.6-TIV-ITM-IF0005</code>.</td></tr>
<tr><td>IY93792</td><td>On UNIX platforms, the SNMP DP Managed Node List feature reports incorrect On-line/Off-line ping status information for monitored devices. <b>Note:</b> This APAR was first resolved in the following interim fix (IF) for Fix Pack 6: <code>6.1.0.6-TIV-ITM-IF0005</code>.</td></tr>
<tr><td>IY98018</td><td>Customer would like the UA behavior to be consistent with other agents and request that UA determine the value for &hostname using the search order:
<ol>
<li>The metafile specified HOSTADDR=xxxx override value on the //SOURCE statement, if specified.</li>
<li>The CTIRA_HOSTNAME as the secondary source for &hostname value, if specified.</li>
<li>Else the computer hostname.</li>
</ol>
<b>Note:</b> This APAR was first resolved in the following interim fix (IF) for Fix Pack 6: <code>6.1.0.6-TIV-ITM-IF0005</code>.</td></tr>
<tr><td>IY98193</td><td>The ICU ucnv_open call with a NULL converter (meaning, use the default converter) is failing. The U_FILE_ACCESS_ERROR is likely the result of an incorrect or unknown codepage, and shouldn't be related to the presence or absence of a particular resource bundle on the local system. <b>Note:</b> This APAR was first resolved in the following interim fix (IF) for Fix Pack 6: <code>6.1.0.6-TIV-ITM-IF0005</code>.</td></tr>
<tr><td>IY99376</td><td>KUMA610 consumes 100% of CPU. It seems to run for a while before consuming 100%. <b>Note:</b> This APAR was first resolved in the following interim fix (IF) for Fix Pack 6: <code>6.1.0.6-TIV-ITM-IF0005</code>.</td></tr>
</table>

Table 38. Tivoli Universal Agent APARs originally fixed in the interim fixes for Fix Pack 6. (continued)

APAR number	Symptom, as described in the APAR database
IZ00560	The Universal Agent can't derive SNMPTRAPENTERPRISE,SNMPTRAPOID for SNMPV2 trap. The customer has an unusual SNMP Agent, that emits SNMPv2 traps in a form that UA's SNMP data provider does not support. **Note:** This APAR was first resolved in the following interim fix (IF) for Fix Pack 6: `6.1.0.6-TIV-ITM-IF0001`.
IZ01183	When using ADDSOURCENAME metafile qualifier along with ManagedSystemName-= qualifier, value of DataSourceName attribute will be truncated if local host name's length is less than the length of name declared per ManagedSystemName= . **Note:** This APAR was first resolved in the following interim fix (IF) for Fix Pack 6: `6.1.0.6-TIV-ITM-IF0005`.
IZ03665	Bursts of SITSTOP requests CAUSE UA DEADLOCK. Universal Agent data provider stops processing data records; pulls the new records once recycled. **Note:** This APAR was first resolved in the following interim fix (IF) for Fix Pack 6: `6.1.0.6-TIV-ITM-IF0005`.
IZ03744	HTTP Data Provider can not process URL with recursive redirect. HTTP Data Provider does handle web server redirects. In fact, this is a fairly common occurrence, for example, http://www.tivoli.com gets redirected. What's unusual about the URL cited in the PMR, http://www.fredmeyerjewelers.com, is that it ends up redirecting back to itself. The HTTP DP has no provision for handling this type of recursion and so it never issues the HTTP Get command. **Note:** This APAR was first resolved in the following interim fix (IF) for Fix Pack 6: `6.1.0.6-TIV-ITM-IF0005`.
IZ03755	Dynamic filename not supporting globalized filenames. The path of a file that contains globalized text is not being converted, as it should. **Note:** This APAR was first resolved in the following interim fix (IF) for Fix Pack 6: `6.1.0.6-TIV-ITM-IF0005`.
IZ06342	Script losing parts of stdout, taints data rows. When UA Script data provider reads STDOUT from the buffer it is not properly tracking for CRLF to denote end of logical record. **Note:** This APAR was first resolved in the following interim fix (IF) for Fix Pack 6: `6.1.0.6-TIV-ITM-IF0005`.
IZ06382	Derived,scaled attr using scaled attr has incorrect value. If a scaled attribute is used in computing a derived attribute, which is also scaled, the resulting value for derived attribute will be incorrect. **Note:** This APAR was first resolved in the following interim fix (IF) for Fix Pack 6: `6.1.0.6-TIV-ITM-IF0005`.
IZ06988	UA KUMSTRAP allocates listen port when KUMP_SNMP_MONITOR_TRAP=N. The kumstrap executable (binary) of the Universal Agent on UNIX/Linux should check the KUMP_SNMP_MONITOR_TRAP env var at startup. **Note:** This APAR was first resolved in the following interim fix (IF) for Fix Pack 6: `6.1.0.6-TIV-ITM-IF0005`.
IZ07574	Solaris UA alt instance with script reads zero bytes on stdout. The effect on alternate UA instance is as if the script is never executed. **Note:** This APAR was first resolved in the following interim fix (IF) for Fix Pack 6: `6.1.0.6-TIV-ITM-IF0005`.
IZ07749	When using SNMP data provider, description of some received SNMP traps is truncated. **Note:** This APAR was first resolved in the following interim fix (IF) for Fix Pack 6: `6.1.0.6-TIV-ITM-IF0005`.
IZ08229	When a UA source name is specified with embedded hyphens, the actual IP address was not being saved first, subsequently causing UA to try and resolve host name from a hyphenated IP address. **Note:** This APAR was first resolved in the following interim fix (IF) for Fix Pack 6: `6.1.0.6-TIV-ITM-IF0005`.
IZ08899	When starting UA on a UNIX/Linux platform machine that has more than 12 network interfaces defined (multi-home) and using the SNMP data provider, the UA process will crash (core dump). **Note:** This APAR was first resolved in the following interim fix (IF) for Fix Pack 6: `6.1.0.6-TIV-ITM-IF0005`.
IZ10103	The KUMENV file is corrupted by **TEP Configure system** option. When trying to import a metafile using the configure system option on UA, it goes and corrupts the KUMENV file for that UA. **Note:** This APAR was first resolved in the following interim fix (IF) for Fix Pack 6: `6.1.0.6-TIV-ITM-IF0005`.

Table 38. Tivoli Universal Agent APARs originally fixed in the interim fixes for Fix Pack 6. (continued)

APAR number	Symptom, as described in the APAR database
IZ11286	The excessive child process terminate message floods the UA trace log, causing huge volumes of repetitive tracing. Th root cause is due to the 'TerminateProcess' logic checking the process list before Windows has had a chance to update the process list; this is likely to occur only when system load is high. **Note:** This APAR was first resolved in the following interim fix (IF) for Fix Pack 6: `6.1.0.6-TIV-ITM-IF0005`.

i5/OS monitoring agent APARs

The following APARs are addressed in Fix Pack 7. The table also lists the APAR fixes that are included in Fix Pack 7 and were originally fixed in the interim fixes (IF) or limited availability (LA) fixes for Fix Pack 6. *All the interim fixes for Fix Pack 6 are included in Fix Pack 7.*

APAR Number	Symptom, as described in the APAR database
IY98058	OS/400 AGENT FAILS WITH MCH6902, MCH3601, C2M1212 Agent job may raise exceptions like the following. MCH6902 - The requested heap space operation is invalid C2M1212 - The pointer parameter passed to free or realloc is not valid. This started occurring more on the latest versions of the i5/OS. **Note:** This APAR was first resolved in the following Limited Availability (LA) fix for Fix Pack 6: `6.1.0-TIV-ITM_i5OS-LA0006`.
IZ01049	OS400_MESSAGE.SELECT ATTRIBUTE NOT HANDLED CORRECTLY IN SITUATIONS. A situation created with the formula "*IF *VALUE OS400_Message.Select *EQ '*MNR'" fails to trigger. **Note:** This APAR was first resolved in the following Limited Availability (LA) fix for Fix Pack 6: `6.1.0-TIV-ITM_i5OS-LA0007`.
IZ01889	KFWITM217E REQUEST ERROR: SQLEXECDIRECT RC=-1: SQL_ERROR . **Note:** This APAR was first resolved in the following Limited Availability (LA) fix for Fix Pack 6: `6.1.0-TIV-ITM_i5OS-LA0006`.
IZ06741	ITM 6.1 - I5/OS AGENT FAILS TO END GRACEFULLY. This i5/OS agent is not ending properly and is going into a deadlock when data collection for certain resources is started. **Note:** This APAR was first resolved in the following Limited Availability (LA) fix for Fix Pack 6: `6.1.0-TIV-ITM_i5OS-LA0007`.
IZ09921	UTILIZATION OF I5/OS AGENT JOB HIGH WITH SNTP. The CT_AGENT job of the agent utilizes high CPU and causes eventual shutdown of the system when Simple Network Time Protocol (SNTP) is used by other applications to change the software clock of the system. **Note:** This APAR was first resolved in the following Limited Availability (LA) fix for Fix Pack 6: `6.1.0-TIV-ITM_i5OS-LA0008`.
IZ11945	ENHANCE DATA COLLECTION FOR JOBS ON BIG SYSTEMS. The existing agent code can process and send data to Tivoli Enterprise Management Server for a maximum of approximately 54,000 jobs. This is due to restrictions on the amount of data that can be stored in the internal memory buffers. This can cause data collection to be skipped on some jobs if more than 54,000 jobs are active on the system. This can lead to some job related situations not triggering as expected. **Note:** This APAR was first resolved in the following Limited Availability (LA) fix for Fix Pack 6: `6.1.0-TIV-ITM_i5OS-LA0008`.

Linux OS monitoring agent APARs

The following APARs are addressed in Fix Pack 7. The table also lists the APAR fixes that are included in Fix Pack 7 and were originally fixed in the interim fixes (IF) or limited availability (LA) fixes for Fix Pack 6. *All the interim fixes for Fix Pack 6 are included in Fix Pack 7.*

APAR Number	Symptom, as described in the APAR database
IZ04877	ITM 6.1 Linux OS Agent gives wrong values for process CPU percentages on RHEL 5. **Note:** This APAR was first resolved in the following Limited Availability fix: `6.1.0.6-TIV-ITM_LINUX-LA0006`
IZ11699	Linux agent running n SLES 8.0 with ps light consumes 5-10% of CPU. **Note:** This APAR was first resolved in the following Limited Availability fix: `6.1.0.6-TIV-ITM_LINUX-LA0007`

UNIX Logs monitoring agent APARs

The following APARs are addressed in Fix Pack 7. The table also lists the APAR fixes that are included in Fix Pack 7 and were originally fixed in the interim fixes (IF) or limited availability (LA) fixes for Fix Pack 6. *All the interim fixes for Fix Pack 6 are included in Fix Pack 7.*

APAR Number	Symptom, as described in the APAR database
IZ05425	UNIX Log Agent does not properly handle rolled logs. **Note:** This APAR was first resolved in the following Limited Availability fix: `6.1.0.6-TIV-ITM_UXLOG-LA0003`

Windows OS monitoring agent APARs

The following APARs are addressed in Fix Pack 7. The table also lists the APAR fixes that are included in Fix Pack 7 and were originally fixed in the interim fixes (IF) or limited availability (LA) fixes for Fix Pack 6. *All the interim fixes for Fix Pack 6 are included in Fix Pack 7.*

APAR Number	Symptom, as described in the APAR database
IZ04680	APAR IN ERROR AGAINST LA0045 AND LA0046 - THE PATCHES SHOULD BE MARKED WITH NO TEPD SUPPORT **Note:** This APAR was first resolved in the following Limited Availability (LA) fix for Fix Pack 6: `6.1.0.6-TIV-ITM_WIN-LA0047`.
IZ06386	When event log monitoring situations are enabled for the Monitoring agent for Windows OS and events are written to Windows event logs, the monitoring agent consumes high CPU. **Note:** This APAR was first resolved in the following Limited Availability (LA) fix for Fix Pack 6: `6.1.0.6-TIV-ITM_WIN-LA0050`.
IZ09227	When event log monitoring situations are enabled for the Monitoring Agent for Windows OS, and the remote IBM Tivoli Enterprise Monitoring Server is recycled, the Monitoring Agent for Windows OS does not reconnect to Remote Tivoli Enterprise Monitoring Server. **Note:** This APAR was first resolved in the following Limited Availability (LA) fix for Fix Pack 6: `6.1.0.6-TIV-ITM_WIN-LA0047`.
IZ10218	In the memory workspace of the Monitoring Agent for Windows OS, when any of the byte attribute values from Windows OS exceeds 2 GB, the byte value is displayed as unknown. The value for the KB attribute corresponding to byte value is displayed as zero. **Note:** This APAR was first resolved in the following Limited Availability (LA) fix for Fix Pack 6: `6.1.0.6-TIV-ITM_WIN-LA0048`.
IZ16996	The Windows agent on Windows 2003 experience a segment fault when the threads for the event processing code were in shutdown mode and terminating. The problem is seen because the shutdown messages use a double-wide string instead of a single byte string. **Note:** This APAR was first resolved in the following Limited Availability (LA) fix for Fix Pack 6: `6.1.0.6-TIV-ITM_WIN-LA0049`.
IZ17024	WINDOWS AGENT CAUSES MEMORY LEAK. Corrupt perfmon counters caused memory leaks in the agent because new instances for the corrupt counters were created each cycle. **Note:** This APAR was first resolved in the following Limited Availability (LA) fix for Fix Pack 6: `6.1.0.6-TIV-ITM_WIN-LA0050`.
IZ17149	STARTUP OF AGENT CAUSES LARGE AMOUNTS OF PAGE FAULTS. Using the 'Global' parameter to read all perfmon counters caused page faults. **Note:** This APAR was first resolved in the following Limited Availability (LA) fix for Fix Pack 6: `6.1.0.6-TIV-ITM_WIN-LA0050`.

APAR Number	Symptom, as described in the APAR database
IZ18645	WINDOWS AGENT CRASHES WHEN A PERFORMANCE COUNTER IS DISABLED. Disabling perfmon counters caused the agent to reference memory for data that did not exist because the perfmon counter was disabled. **Note:** This APAR was first resolved in the following Limited Availability (LA) fix for Fix Pack 6: `6.1.0.6-TIV-ITM_WIN-LA0050`.
IZ19100	STARTUP OF AGENT CAUSES LARGE AMOUNTS OF PAGE FAULTS. Using the 'Global' parameter to read all perfmon counters caused page faults. **Note:** This APAR was first resolved in the following Limited Availability (LA) fix for Fix Pack 6: `6.1.0.6-TIV-ITM_WIN-LA0050`.

UNIX OS monitoring agent APARs

The following APARs are addressed in Fix Pack 7. The table also lists the APAR fixes that are included in Fix Pack 7 and were originally fixed in the interim fixes (IF) or limited availability (LA) fixes for Fix Pack 6. *All the interim fixes for Fix Pack 6 are included in Fix Pack 7.*

APAR Number	Symptom, as described in the APAR database
IZ01659	TEMA filter object disabled if UTF8 data and COUNT(). Agent filter object does not get created, if the predicate has UTF8 columns and MIN(), MAX(), AVG(), SUM() or COUNT() functions, so the situation never gets triggered. **Note:** This APAR was first resolved in the following Limited Availability (LA) fix for Fix Pack 6: `6.1.0.6-TIV-ITM_UNIX-LA0014`.
IZ05941	UNIX OS agent displays only 32 bytes for the unicode mount point. **Note:** This APAR was first resolved in the following Limited Availability (LA) fix for Fix Pack 6: `6.1.0.6-TIV-ITM_UNIX-LA0014`.
IZ07201	User's name (length=2 OR 1) of UNIX process is not shown correctly. Agent does not properly display the "User Name" attribute of the "User Process" workspace. It displays some garbage characters. **Note:** This APAR was first resolved in the following Limited Availability (LA) fix for Fix Pack 6: `6.1.0.6-TIV-ITM_UNIX-LA0014`.
IZ16515	UX agent on an AIX 5.3 with dedicated processor reports in-correct CPU Metrics. **Note:** This APAR was first resolved in the following Limited Availability (LA) fix for Fix Pack 6: `6.1.0.6-TIV-ITM_UNIX-LA0015`.
IZ16520	Unix OS agent crashes on Solaris. This Agent crashes when the number of disks is equal to any in the series (n + (n/2)) and any one of those disks goes offline and comes back online at random. **Note:** This APAR was first resolved in the following Limited Availability (LA) fix for Fix Pack 6: `6.1.0.6-TIV-ITM_UNIX-LA0015`.

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.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

IBM Corporation
2Z4A/101
11400 Burnet Road
Austin, TX 78758 U.S.A.

Such information may be available, subject to appropriate terms and conditions, including in some cases payment of a fee.

The licensed program described in this document and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement or any equivalent agreement between us.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurement may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

All statements regarding IBM's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

All IBM prices shown are IBM's suggested retail prices, are current and are subject to change without notice. Dealer prices may vary.

This information is for planning purposes only. The information herein is subject to change before the products described become available.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs. You may copy, modify, and distribute these sample programs in any form without payment to IBM for the purposes of developing, using, marketing, or distributing application programs conforming to IBM's application programming interfaces.

Each copy or any portion of these sample programs or any derivative work, must include a copyright notice as follows:

© (your company name) (year). Portions of this code are derived from IBM Corp. Sample Programs. © Copyright IBM Corp. _enter the year or years_. All rights reserved.

If you are viewing this information in softcopy form, the photographs and color illustrations might not be displayed.

Trademarks

AIX, AS/400, Candle, CICS, DB2, i5/OS, IBM, the IBM logo, ibm.com, iSeries, NetView, OMEGAMON, OMEGAMON II, OS/400, pSeries, System p, Tivoli, Tivoli Enterprise, Tivoli Enterprise Console, z/OS, zSeries, and Passport Advantage are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both. If these and other IBM trademarked terms are marked on their first occurrence in this information with a trademark symbol (® or ™), these symbols indicate U.S. registered or common law trademarks owned by IBM at the time this information was published. Such trademarks may also be registered or common law trademarks in other countries. A current list of IBM trademarks is available on the Web at ″Copyright and trademark information″ at http://www.ibm.com/legal/copytrade.shtml.

Adobe, Acrobat, PostScript and all Adobe-based trademarks are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States, other countries, or both.

Intel and Itanium are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.

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

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

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

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.

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

Printed in USA

GI11-8885-00