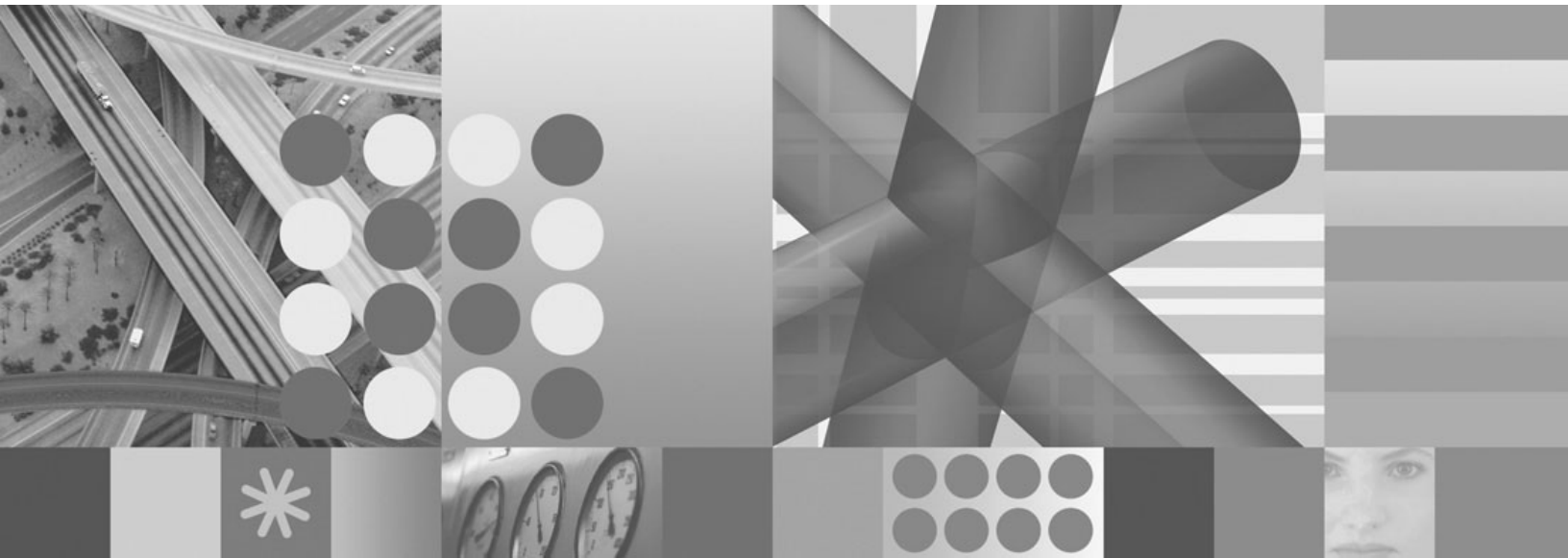




Fix Pack 002 Readme and Documentation Addendum



Fix Pack 002 Readme and Documentation Addendum

First edition (June 2006)

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

© **Copyright International Business Machines Corporation 2006. All rights reserved.**

US Government Users Restricted Rights – Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.

Contents

Chapter 1. Fix Pack 002 overview	1
APARs addressed by this fix pack	1
Contents of this fix pack	2
Supported operating systems	2
Chapter 2. Installation instructions	7
Before you install the fix pack	7
Installation checklists	8
Fix pack installation planning worksheets	9
Monitoring server checklist	13
Portal server checklist	16
Portal desktop client checklist	18
Monitoring agent checklist - local installation	20
Monitoring agent checklist - remote installation	21
Additional installation information	22
Installing the full product media	22
Uninstalling the GA level of code	22
Upgrading your GA level of code	22
Adding agents to a patched environment	22
About the GA versions IBM Tivoli Monitoring V6.1 agent CDs for Windows platforms	22
Chapter 3. Known problems and limitations	25
Chapter 4. Installing and configuring the Warehouse Proxy on Linux computers	29
Software prerequisites	29

Overview of steps	29
Creating the Tivoli Data Warehouse database	29
Installing the Warehouse Proxy agent.	30
Copying the JDBC driver files to the local system	30
Configuring the Warehouse Proxy agent.	30
Start the Warehouse Proxy	33

Chapter 5. Installing and configuring multiple Warehouse Proxy agents	35
About multiple Warehouse Proxy support	35
Installing and configuring the proxy agents.	35
Verifying the configuration	36

Appendix A. Detailed installation procedures for installing the component patches	39
Installing the 6.1.0-TIV-ITM_INST-FP0002 patch	39
Installing patches using the itmpatch command	39
Installing application support	39
Using a response file to install the application support files	41
Adding patches to the agent depot	43
Deploying patches to remote agents	43

Appendix B. Using the patch installer	45
--	-----------

Appendix C. Notices	47
Trademarks	48

Chapter 1. Fix Pack 002 overview

Fix Pack 002 is a cumulative fix pack for IBM® Tivoli® Monitoring, Version 6.1.0. This readme and documentation addendum file provides details about installing the fix pack and information about changes to IBM Tivoli Monitoring in this release.

IBM Tivoli Monitoring, Fix Pack 002, contains the component patches listed in Table 1. See Chapter 2, “Installation instructions,” on page 7 for detailed installation procedures for all of these patches. Additionally, each patch has its own readme with additional information regarding APARs and product defects addressed by the patch.

Table 1. Fix Pack 002 component patches

Patch name	Description	Readme file name
6.1.0-TIV-ITM-FP002	General patch information	6.1.0-TIV-ITM-FP0002.README
6.1.0-TIV-ITM_INST-FP0002	IBM Tivoli Monitoring Global-common Component (required for all monitoring components)	6.1.0-TIV-ITM_INST-FP0002.README
6.1.0-TIV-ITM_TEMS-FP0002	Tivoli Enterprise™ Management Server	6.1.0-TIV-ITM_TEMS-FP0002.README
6.1.0-TIV-ITM_TEP-FP0002	Tivoli Enterprise Portal desktop client	6.1.0-TIV-ITM_TEP-FP0002.README
6.1.0-TIV-ITM_TEPS-FP0002	Tivoli Enterprise Portal Server	6.1.0-TIV-ITM_TEPS-FP0002.README
6.1.0-TIV-ITM_TEMA-FP0002	IBM Tivoli Monitoring Shared Libraries for the monitoring agent	6.1.0-TIV-ITM_TEMA-FP0002.README
6.1.0-TIV-ITM_UA-FP0002	Universal Agent	6.1.0-TIV-ITM_UA-FP0002.README
6.1.0-TIV-ITM_TDW-FP0002	Warehouse Summarization and Pruning agent and Warehouse Proxy agent	6.1.0-TIV-ITM_TDW-FP0002.README
6.1.0-TIV-ITM_UNIX-FP0002	UNIX® OS Monitoring agent	6.1.0-TIV-ITM_UNIX-FP0002.README
6.1.0-TIV-ITM_WIN-FP0002	Windows® OS Monitoring agent	6.1.0-TIV-ITM_WIN-FP0002.README
6.1.0-TIV-ITM_i5OS-FP0002	i5/OS™ OS Monitoring agent	6.1.0-TIV-ITM_i5OS-FP0002.README
6.1.0-TIV-ITM_UXLOG-FP0002	UNIX Log agent	6.1.0-TIV-ITM_UXLOG-FP0002.README

Note: If you are using the IBM Tivoli Monitoring - Tivoli Enterprise Console® event synchronization, ensure that you are at the Fix Pack 001 level of code.

APARs addressed by this fix pack

For a full listing of customer APARs addressed in this fix pack, including detailed information about the APARs, see the individual component readmes available at the IBM Support Web site.

Contents of this fix pack

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

- Support for the Warehouse Proxy on Linux[®] operating systems. See Chapter 4, "Installing and configuring the Warehouse Proxy on Linux computers," on page 29 for more information.
- Support for multiple Warehouse Proxy agents in a single monitoring environment. See Chapter 5, "Installing and configuring multiple Warehouse Proxy agents," on page 35 for more information.
- Enhanced ease of adding new views within the Tivoli Enterprise Portal. See the online help in the Tivoli Enterprise Portal for information.
- Enhanced firewall functionality through the use of a gateway feature. For information about this function, see the "Firewall Gateway Feature" document in the IBM Tivoli Monitoring information center (located at <http://publib.boulder.ibm.com/infocenter/tivihelp/v3r1/index.jsp?toc=/com.ibm.itm.doc/toc.xml>).
- Increased default security for the Tivoli Enterprise Portal.

When you are installing the full media that contains the fixes in IBM Tivoli Monitoring V6.1 Fix Pack 002 and related agent patches, there is a new requirement to type a Tivoli Enterprise Portal Server sysadmin password. You are prompted for this new password during installation. For silent installations, the SYSADMINPWSD=value is completed in the CMS_CONFIG section, which is the first value of that section. A Windows ID is then created as sysadmin with the supplied user ID.

The password is *only* required for fresh installations on Windows (not on Linux). Any upgraded installations continue to function in the same way as the installation from which you are upgrading. Because the password is verified by the Windows operating system, you must create a password that conforms to any Windows password rules. The sysadmin ID must also conform to account policies on the computer where the software is installed.

Supported operating systems

Fix Pack 002 adds support for additional operating systems. The following table shows which operating systems are supported for the different IBM Tivoli Monitoring components in this fix pack: monitoring server, portal server, portal client, monitoring agent, Warehouse Proxy, and Warehouse Proxy Summarization and Pruning agent. Support that has been added in this fix pack is marked with **bold** highlighting.

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

Table 2. Supported non-Linux operating systems

Operating system	Monitoring server	Portal server	Portal client ¹	Monitoring agent ^{2,3}	Warehouse Proxy	Warehouse Summarization and Pruning agent
AIX [®] V5.1 (32/64 bit)				X		X

Table 2. Supported non-Linux operating systems (continued)

Operating system	Monitoring server	Portal server	Portal client ¹	Monitoring agent ^{2,3}	Warehouse Proxy	Warehouse Summarization and Pruning agent
AIX V5.2 (32/64 bit)	X			X		X
AIX V5.3 (32/64 bit)	X			X		X
Solaris Operating Environment V8 (32/64 bit)	NEW			X		X
Solaris V9 (SPARC)	X			X		X
Solaris V10 (SPARC)	X			X		X
Solaris V10 (x86-64) on AMD Opteron	NEW			NEW		
HP-UX 11i (32/64 bit) with patch PHSS_30970				X		
HP-UX 11.23 on Itanium2				NEW		
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 ⁵	X	X	X	X	X	X
Windows 2003 Server EE (32 bit) with Service Pack 1 ⁵	X	X	X	X	X	X
Windows 2003 SE (64 bit)				NEW		
Windows 2003 EE (64 bit)				NEW		
Windows 2003 Server on Itanium2				NEW		
OS/400 [®] 5.2				X		
i5/OS 5.3				X		

Table 2. Supported non-Linux operating systems (continued)

Operating system	Monitoring server	Portal server	Portal client ¹	Monitoring agent ^{2,3}	Warehouse Proxy	Warehouse Summarization and Pruning agent
i5/OS 5.4				X		
z/OS [®] 1.4 ⁶	X			X		
z/OS 1.5	X			X		
z/OS 1.6	X			X		
z/OS 1.7	X			NEW		

Notes:

1. The Tivoli Enterprise Portal desktop client is supported on marked platforms. However, the browser client can only be accessed from Windows computers running Internet Explorer 6.
2. The **Monitoring agent** column indicates the platforms on which an agent is supported. It does not indicate that any agent runs on any operating system. For example, to monitor a Linux computer, you must use a Linux monitoring agent, not a Windows monitoring agent.
3. If you are installing the OMEGAMON XE for Messaging agent on a 64-bit operating system, you must install the 32-bit version of the agent framework. See the OMEGAMON XE for Messaging bullet in Chapter 3, "Known problems and limitations," on page 25 for details on installing this framework.
4. For the Windows 2000 Professional and Windows XP 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.
5. For Windows 2003 Server: If you do not plan to deploy Service Pack 1 in your environment at this time, you must download and install Microsoft[®] Installer 3.1 (KB893803), which is available from the Microsoft Download Web site (www.microsoft.com/downloads).
6. For information about installing the monitoring server on z/OS, see the Program Directory that comes with that product.

Table 3. Supported Linux operating systems

Operating system	Monitoring server	Portal server	Portal client ¹	Monitoring agent ²	Warehouse Proxy	Warehouse Summarization and Pruning agent
RedHat Enterprise Linux 2.1 Intel [®]				X		X
RedHat Enterprise Linux 3 on Intel				NEW	NEW	NEW
RedHat Enterprise Linux 3 on zSeries [®] 31 bit				NEW	NEW	NEW
RedHat Enterprise Linux 3 on zSeries 64 bit				NEW	NEW	NEW
RedHat Enterprise and Desktop Linux 4 Intel	X	X	X	X	NEW	X
RedHat Enterprise Linux 4 on iSeries [™] and pSeries ^{®3}				NEW		

Table 3. Supported Linux operating systems (continued)

Operating system	Monitoring server	Portal server	Portal client ¹	Monitoring agent ²	Warehouse Proxy	Warehouse Summarization and Pruning agent
RedHat Enterprise Linux 4 on z/Series 31-bit	X	X		X	NEW	NEW
RedHat Enterprise 4 on zSeries 64 bit				NEW	NEW	NEW
SUSE Linux Enterprise Server 8 Intel				X	NEW	NEW
SUSE Linux Enterprise Server 8 for z/Series 31-bit				X	NEW	NEW
SUSE Linux Enterprise Server 8 for z/Series 64-bit				NEW	NEW	NEW
SUSE Linux Enterprise Server 9 Intel	X	X	NEW	X	NEW	NEW
SUSE Linux Enterprise Server 9 for iSeries and pSeries				NEW		
SUSE Linux Enterprise Server 9 for z/Series 31-bit	X	X		X	NEW	NEW
SUSE Linux Enterprise Server 9 for z/Series 64-bit				X	NEW	NEW

Notes:

1. The Tivoli Enterprise Portal desktop client is supported on marked platforms. However, the browser client can be accessed only from Windows computers running Internet Explorer 6.
2. The **Monitoring agent** column indicates the platforms on which an agent is supported. This column does not indicate that any agent runs on any operating system. For example, to monitor a Linux computer, you must use a Linux monitoring agent, not a Windows monitoring agent.
3. For RedHat Enterprise Linux on pSeries, you must install the 32-bit version of compat-libstdc++-33-3.2.3-47.3. This file can be found on the RedHat Enterprise Linux operating system installation media. Use the following command to install this package:

```
rpm -i compat-libstdc++-33-3.2.3-47.3.ppc.rpm
```

Chapter 2. Installation instructions

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

Table 4. Overall installation steps for Fix Pack 002

Goal	Where to find information
Ensure your monitoring environment is prepared for fix pack installation.	"Before you install the fix pack"
Gather the information you need to perform the installations.	"Fix pack installation planning worksheets" on page 9
Update your monitoring server.	"Monitoring server checklist" on page 13
Update your portal server.	"Portal server checklist" on page 16
Update your portal desktop clients.	"Portal desktop client checklist" on page 18
Update your remote monitoring servers.	"Monitoring server checklist" on page 13
Update your local monitoring agents.	"Monitoring agent checklist - local installation" on page 20
Remotely update other monitoring agents.	"Monitoring agent checklist - remote installation" on page 21

Before you install the fix pack

Do the following before you install this fix pack:

- *Note that you must upgrade all components to the same fix pack level. You cannot have a Fix Pack 001 portal server and a Fix Pack 002 monitoring server.*
- Any prerequisite fix packs or other software must be installed for all component patches you are going to install.
- Before installing any patches on UNIX or Linux computers, set the environment variable CANDLEHOME to the IBM Tivoli Monitoring installation directory by running the following command:

```
export CANDLEHOME=ITMinstall_dir
```

where *ITMinstall_dir* is the location where IBM Tivoli Monitoring is installed.

- Before you install the Tivoli Enterprise Portal Server component patch on a Windows computer, ensure that the Windows Script Host (WSH) is at least version 5.6. You can check the version by running the **cscript** command without any parameters.
- The fix pack for the Warehouse Proxy requires that you first install the 6.1.0-TIV-ITM_TEMA-FP0002 component patch. See "Installing patches using the `itmpatch` command" on page 39 for more information.
- To use the GUI version of the application support installer on a Linux or UNIX monitoring server, portal server, or portal client, you must install x-Windows. If you do not have x-Windows, you can run a silent installation of the application support files. See "Using a response file to install the application support files" on page 41 for detailed information.
- *Do not apply fix packs through full image or CD refresh to computers that already have IBM Tivoli Monitoring V6.1 installed.* Install the full image or CD refresh of IBM Tivoli Monitoring V6.1 only on computers where IBM Tivoli

Monitoring V6.1 is not currently installed or for products for which new operating system support has been added as part of a fix pack. Instead, use the individual component patches to apply a fix pack to existing IBM Tivoli Monitoring V6.1 installations. These patches are available from the IBM Software Support Web site.

- For the Warehouse Summarization and Pruning agent, if you are using Microsoft SQL server, consider installing the MS SQL 2005 JDBC driver. The Warehouse Summarization and Pruning agent might fail to run at the scheduled time on Windows computers because of a limitation of the number of tables it can retrieve. The MS SQL 2005 JDBC driver addresses this limitation. You can download the JDBC driver from the Microsoft Web site, <http://msdn.microsoft.com/data/jdbc/default.aspx>.

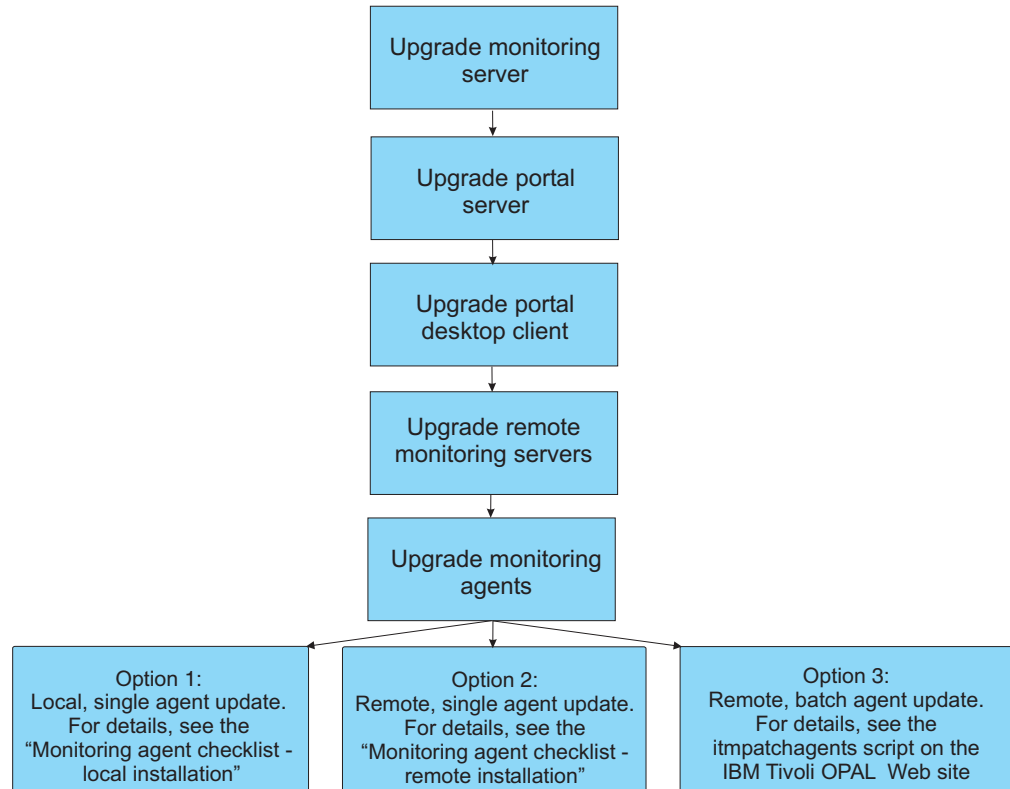
Installation checklists

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

- “Fix pack installation planning worksheets” on page 9
- “Monitoring server checklist” on page 13
- “Portal server checklist” on page 16
- “Portal desktop client checklist” on page 18
- “Monitoring agent checklist - local installation” on page 20
- “Monitoring agent checklist - remote installation” on page 21

Note: If your Warehouse Proxy agent or Summarization and Pruning agent are on machines other than the monitoring server or portal server, use the instructions in the “Monitoring agent checklist - local installation” on page 20 to install the updates.

Install your environment in the following order:



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

Note: If you have a large number of monitoring agents to which to deploy updates, consider using the `itmpatchagents` script, available as a sample from the IBM Tivoli Open Process Automation Library (<http://www-18.lotus.com/wps/portal/topal>). This script enables the automatic deployment of updates across your monitoring environment.

Fix pack installation planning worksheets

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

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

Table 5. Fix pack planning worksheet

IBM Tivoli Monitoring installation directory (CANDLEHOME environment variable): Note: This directory is referred to as <i>ITMInstall_dir</i> in this document			
Patch installation directory (where you extract the patch files): Note: This directory is referred to as <i>patch_dir</i> in this document			
What is needed	Other components also installed on this computer (circle those that apply)	How to gather this information	When this information is used
Hub monitoring server host name	Portal server Portal desktop client Warehouse Proxy Summarization and Pruning agent	Manage Tivoli Enterprise Monitoring Server	"Monitoring server checklist" on page 13
Remote monitoring server host name	Portal server Portal desktop client Warehouse Proxy Summarization and Pruning agent	Manage Tivoli Enterprise Monitoring Server	"Monitoring server checklist" on page 13
Remote monitoring server host name	Portal server Portal desktop client Warehouse Proxy Summarization and Pruning agent	Manage Tivoli Enterprise Monitoring Server	"Monitoring server checklist" on page 13
Remote monitoring server host name	Portal server Portal desktop client Warehouse Proxy Summarization and Pruning agent	Manage Tivoli Enterprise Monitoring Server	"Monitoring server checklist" on page 13
Remote monitoring server host name	Portal server Portal desktop client Warehouse Proxy Summarization and Pruning agent	Manage Tivoli Enterprise Monitoring Server	"Monitoring server checklist" on page 13
Remote monitoring server host name	Portal server Portal desktop client Warehouse Proxy Summarization and Pruning agent	Manage Tivoli Enterprise Monitoring Server	"Monitoring server checklist" on page 13
Portal server host name	Monitoring server Portal desktop client Warehouse Proxy Summarization and Pruning agent	Manage Tivoli Enterprise Monitoring Server	"Portal server checklist" on page 16

Table 5. Fix pack planning worksheet (continued)

IBM Tivoli Monitoring installation directory (CANDLEHOME environment variable): Note: This directory is referred to as <i>ITMInstall_dir</i> in this document			
Patch installation directory (where you extract the patch files): Note: This directory is referred to as <i>patch_dir</i> in this document			
What is needed	Other components also installed on this computer (circle those that apply)	How to gather this information	When this information is used
Portal desktop client locations	Monitoring server Portal server Warehouse Proxy Summarization and Pruning agent	Manage Tivoli Enterprise Monitoring Server	"Portal desktop client checklist" on page 18
Warehouse Proxy agent location	Monitoring server Portal server Portal desktop client Summarization and Pruning agent	Manage Tivoli Enterprise Monitoring Server	"Monitoring server checklist" on page 13 "Portal server checklist" on page 16
Warehouse Summarization and Pruning agent location	Monitoring server Portal server Portal desktop client Warehouse Proxy	Manage Tivoli Enterprise Monitoring Server	"Monitoring server checklist" on page 13 "Portal server checklist" on page 16
Agent types to update (product codes)		tacmd listSystems	"Monitoring server checklist" on page 13 "Monitoring agent checklist - local installation" on page 20

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

Table 6. Agent updates table

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

Monitoring server checklist

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

Note: The process for updating the hub and remote monitoring servers is the same, although you must update the hub monitoring server first, as shown in the fix pack installation flow chart.

Table 7. Checklist for installing the fix pack on the monitoring server

✓	Installation step
	1. Gather information about the monitoring components in your environment. See “Fix pack installation planning worksheets” on page 9.
	2. Download and extract the patch files to a temporary location on your computer. Patch directory:
	3. Before installing any patches, stop the monitoring server (and portal server, if present) through the Manage Tivoli Enterprise Monitoring Services utility (CandleManage on Linux and UNIX). Also stop the Manage Tivoli Enterprise Monitoring Services utility. You can also run the following command to stop Linux or UNIX monitoring servers: <code>itmcmd server stop <i>server_name</i></code> where <i>server_name</i> is the name of the monitoring server.
	4. Install the 6.1.0-TIV-ITM_INST-FP0002 patch. On Windows computers, run the following command from the command line: <code>cd <i>patch_dir</i></code> <code>install_kui.bat</code> On UNIX or Linux computers, run the following command from the command line: <code>cd <i>patch_dir</i></code> <code>./install_kui.sh</code> where <i>patch_dir</i> is the directory where you extracted the patch files.
	5. Run the itmpatch command to install the 6.1.0-TIV-ITM_TEMS-FP0002 patch. For Windows computers: <code>ITMinstall_dir\bin\itmpatch.exe -h ITMinstall_dir -i patch_dir\6.1.0-TIV-ITM_TEMS-FP0002</code> where <i>ITMinstall_dir</i> is the IBM Tivoli Monitoring installation directory. For Linux and UNIX computers: <code>\$CANDLEHOME/bin/itmpatch -h \$CANDLEHOME -i patch_dir/6.1.0-TIV-ITM_TEMS-FP0002</code>
	6. Start the monitoring server through the Manage Tivoli Enterprise Monitoring Services utility. On Linux and UNIX computers, you can run the following command to start the monitoring server: <code>itmcmd server start <i>server_name</i></code> where <i>server_name</i> is the name of the monitoring server.

Table 7. Checklist for installing the fix pack on the monitoring server (continued)

✓	Installation step
	<p>7. Optionally install the following IBM Tivoli Monitoring component patches for components on the same computer as your monitoring server:</p> <ul style="list-style-type: none"> • IBM Tivoli Monitoring Share Libraries for the monitoring agent - 6.1.0-TIV-ITM_TEMA-FP0002 (a prerequisite for the Warehouse Proxy agent patch) • Warehouse Proxy agent on Windows - 6.1.0-TIV-ITM_TDW-FP0002 • Warehouse Summarization and Pruning agent on Windows and UNIX - 6.1.0-TIV-ITM_TDW-FP0002 <p>Use the itmpatch command. See “Monitoring agent checklist - local installation” on page 20 for more information.</p> <p>Restart these agents after you update them.</p>
	<p>8. Run the application support installer to add the application support files for the OS agents (Windows, UNIX, and i5/OS) to the monitoring server. Application support files are located in a subdirectory of the agent patch package.</p> <p>Download and extract the agent patch file (the 6.1.0-TIV-ITM_<i>platform</i>-FP002.tar file) for each OS agent in your environment and follow these steps to run the application support installer.</p> <p>Note: This GUI requires x-Windows on UNIX and Linux computers. If you do not have x-Windows, you can run a silent installation of the application support files. See “Using a response file to install the application support files” on page 41 for information.</p> <ol style="list-style-type: none"> a. Extract the compressed files that contain the application support files for each patch. Look for a file named "<i>pc_tems_teps_tepd_fp0002.tar</i>," where <i>pc</i> is "k" plus the 2-letter product code for the agent. For example, the file for the UNIX OS agent is <i>kux_tems_teps_tepd_fp0002.tar</i>. Note: Extract the application support files for each OS agent to a unique directory; otherwise, files from the different agents will over-write each other. b. From the directory where you extracted the application support files, launch the application support installer by running the following command: <pre>java -jar <i>directory</i>\CD-ROM\setup.jar</pre> <p>where <i>directory</i> is the directory where you extracted the support files.</p> <p>Note: If you do not have the Java™ JRE in your path statement, invoke the JRE executable file directly by specifying the path to it on the command line.</p> <p>For example, to run the application support installer for the Windows OS agent, run the following command: <pre>c:\program files\ibm\java142\jre\bin\java -jar / D:\FP2_IMAGES\6.1.0-TIV-ITM_WIN-FP0002\CD-ROM\setup.jar</pre> <p>See “Installing application support” on page 39 for more information.</p></p> c. Follow the prompts in the application support installation wizard. d. Repeat this for each OS agent in your environment. <p>See “Installing application support” on page 39 for more information about installing this support, including information about identifying the Java installation directory and the detailed steps for the application support installation wizard.</p> <p>Note: Before you install the application support on any remote monitoring servers, ensure that the hub monitoring server is running.</p> <p>Attention: The agent component fix pack might include modifications to product-provided situations. These changes are not merged automatically. While the changes are included, the updates fail and error messages are displayed when you install the application support. The changes made to each agent’s situations are listed in the agent component readme. You can edit your situations, using the change descriptions provided in the agent component readmes, to merge the changes. For more information on editing a situation, see the “Customizing a situation” section of Chapter 10, “Situations for event-based monitoring” in the <i>IBM Tivoli Monitoring User’s Guide</i>.</p>

Table 7. Checklist for installing the fix pack on the monitoring server (continued)

✓	Installation step
	<p>9. If you are planning on remote deploying the agent patches (or the common component patch), run the tacmd addBundles command to add the patches to the agent depot (an installation directory from which you deploy agents and maintenance packages) on the monitoring server.</p> <pre>\$CANDLEHOME/bin/tacmd addBundles -i <i>patch_name</i> -n</pre> <p>where <i>patch_name</i> is the name of the patch to add to the agent depot, such as 6.1.0-TIV-ITM_WIN-FP0002.</p> <p>Repeat this step for each agent patch. Ensure that you include all of the prerequisite patches. For example, the OS agent patches require the TEMA patch, so it needs to be in the depot before you can deploy the OS agent patches.</p> <p>You can remote deploy the following patches:</p> <ul style="list-style-type: none"> • 6.1.0-TIV-ITM_INST-FP0002 -- IBM Tivoli Monitoring Global-common Component (UI) • 6.1.0-TIV-ITM_TEMA-FP0002 -- ITM Shared Libraries (AX [UNIX] or GL [Windows]) • 6.1.0-TIV-ITM_UA-FP0002 -- Universal Agent (UM) • 6.1.0-TIV-ITM_UNIX-FP0002 -- UNIX OS Monitoring Agent (UX) • 6.1.0-TIV-ITM_WIN-FP0002 -- Windows OS Monitoring Agent (NT) • 6.1.0-TIV-ITM_UXLOG-FP0002 -- UNIX Log Agent (UL) <p>See “Adding patches to the agent depot” on page 43 for more information.</p>
	<p>10. Install the remaining component patches: portal server, portal desktop client, and monitoring agents (local and remote).</p>

Portal server checklist

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

Table 8. Checklist for installing the fix pack on the portal server

✓	Installation step
	1. Gather information about the monitoring components in your environment. See “Fix pack installation planning worksheets” on page 9.
	2. Download and extract the patch files to a temporary location on your computer. Patch directory:
	3. Before installing any patches, stop the portal server (and monitoring server, if present) through the Manage Tivoli Enterprise Monitoring Services utility (CandleManage on Linux). Also stop the Manage Tivoli Enterprise Monitoring Services utility. On Linux computers, you can run the following command to stop the portal server: <code>./itmcmd agent stop cq</code>
	4. Install the 6.1.0-TIV-ITM_INST-FP0002 patch. On Windows computers, run the following command from the command line: <code>cd patch_dir</code> <code>install_kui.bat</code> On Linux computers, run the following command from the command line: <code>cd patch_dir</code> <code>./install_kui.sh</code> where <i>patch_dir</i> is the directory where you extracted the patch files.
	5. Use the itmpatch command to install the 6.1.0-TIV-ITM_TEPS-FP0002 patch. For Windows computers: <code>itmpatch.exe -h ITMinstall_dir -i patch_dir\6.1.0-TIV-ITM_TEPS-FP0002</code> where <i>ITMinstall_dir</i> is the IBM Tivoli Monitoring installation directory. For Linux computers: <code>\$CANDLEHOME/bin/itmpatch -h \$CANDLEHOME -i patch_dir/6.1.0-TIV-ITM_TEPS-FP0002</code>
	6. On Windows computers, reconfigure the portal browser client from the Manage Tivoli Enterprise Monitoring Services utility: a. In Manage Tivoli Enterprise Monitoring Services, right-click the Tivoli Enterprise Portal - Browser client and click Reconfigure . b. In the Configure Tivoli Enterprise Browser window, click OK without making any changes. On Linux computers, run the following command and complete the configuration as prompted: <code>./\$CANDLEHOME/bin/itmcmd config -A cq</code>
	7. Start the portal server through the Manage Tivoli Enterprise Monitoring Services utility. On Linux computers, you can run the following command to stop the portal server: <code>./itmcmd agent start cq</code>

Table 8. Checklist for installing the fix pack on the portal server (continued)

✓	Installation step
	<p>8. Optionally install the following IBM Tivoli Monitoring component patches for components on the same computer as your monitoring server:</p> <ul style="list-style-type: none"> • IBM Tivoli Monitoring Share Libraries for the monitoring agent - 6.1.0-TIV-ITM_TEMA-FP0002 (a prerequisite for the Warehouse Proxy agent patch) • Warehouse Proxy agent on Windows - 6.1.0-TIV-ITM_TDW-FP0002 • Warehouse Summarization and Pruning agent on Windows and UNIX - 6.1.0-TIV-ITM_TDW-FP0002 <p>Use the itmpatch command. See “Monitoring agent checklist - local installation” on page 20 for more information.</p> <p>Restart these agents after you update them.</p>
	<p>9. Run the application support installer to add the application support files for the OS agents (Windows, UNIX, and i5/OS) to the portal server. Application support files are located in a subdirectory of the agent patch package.</p> <p>Download and extract the agent patch file (the 6.1.0-TIV-ITM_<i>platform</i>-FP002.tar file) for each OS agent in your environment and follow these steps to run the application support installer.</p> <p>Note: This GUI requires x-Windows on UNIX and Linux computers. If you do not have x-Windows, you can run a silent installation of the application support files. See “Using a response file to install the application support files” on page 41 for information.</p> <ol style="list-style-type: none"> a. Extract the compressed files that contain the application support files for each patch. Look for a file named “<i>pc_tems_teps_tepd_fp0002.tar</i>,” where <i>pc</i> is “k” plus the 2-letter product code for the agent. For example, the file for the UNIX OS agent is <i>kux_tems_teps_tepd_fp0002.tar</i>. Note: Extract the application support files for each OS agent to a unique directory; otherwise, files from the different agents will over-write each other. b. From the directory where you extracted the application support files, launch the application support installer by running the following command: <pre>java -jar <i>directory</i>\CD-ROM\setup.jar</pre> <p>where <i>directory</i> is the directory where you extracted the support files.</p> <p>Note: If you do not have the Java JRE in your path statement, invoke the JRE executable file directly by specifying the path to it on the command line.</p> <p>For example, to run the application support installer for the Windows OS agent, run the following command: <pre>c:\program files\ibm\java142\jre\bin\java -jar / D:\FP2_IMAGES\6.1.0-TIV-ITM_WIN-FP0002\CD-ROM\setup.jar</pre> <p>See “Installing application support” on page 39 for more information.</p></p> c. Follow the prompts in the application support installation wizard. d. Repeat this for each OS agent in your environment. <p>See “Installing application support” on page 39 for more information about installing this support, including information about identifying the Java installation directory and the detailed steps for the application support installation wizard.</p>
	<p>10. Install the remaining component patches: portal desktop client and monitoring agents (local and remote).</p>

Portal desktop client checklist

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

Table 9. Checklist for installing the fix pack on the portal desktop client

✓	Installation step
	1. Gather information about the monitoring components in your environment. See “Fix pack installation planning worksheets” on page 9.
	2. Download and extract the patch files to a temporary location on your computer. Patch directory:
	3. Before installing any patches, stop the Manage Tivoli Enterprise Monitoring Services utility (CandleManage on Linux and UNIX) if it is running.
	4. Install the 6.1.0-TIV-ITM_INST-FP0002 patch. On Windows computers, run the following command from the command line: <code>cd patch_dir</code> <code>install_kui.bat</code> On UNIX or Linux computers, run the following command from the command line: <code>cd patch_dir</code> <code>./install_kui.sh</code> where <i>patch_dir</i> is the directory where you extracted the patch files.
	5. Use the itmpatch command to install the 6.1.0-TIV-ITM_TEP-FP0002 patch. For Windows computers: <code>itmpatch.exe -h ITMinstall_dir -i patch_dir\6.1.0-TIV-ITM_TEP-FP0002</code> where <i>ITMinstall_dir</i> is the IBM Tivoli Monitoring installation directory. For Linux computers: <code>\$CANDLEHOME/bin/itmpatch -h \$CANDLEHOME -i patch_dir/6.1.0-TIV-ITM_TEP-FP0002</code>

Table 9. Checklist for installing the fix pack on the portal desktop client (continued)

✓	Installation step
	<p>6. Run the application support installer to add the application support files for the OS agents (Windows, UNIX, and i5/OS) to the portal desktop client. Application support files are located in a subdirectory of the agent patch package.</p> <p>Download and extract the agent patch file (the 6.1.0-TIV-ITM_<i>platform</i>-FP002.tar file) for each OS agent in your environment and follow these steps to run the application support installer.</p> <p>Note: This GUI requires x-Windows on UNIX and Linux computers. If you do not have x-Windows, you can run a silent installation of the application support files. See “Using a response file to install the application support files” on page 41 for information.</p> <ol style="list-style-type: none"> a. Extract the compressed files that contain the application support files for each patch. Look for a file named "<i>pc_tems_teps_tepd_fp0002.tar</i>," where <i>pc</i> is "k" plus the 2-letter product code for the agent. For example, the file for the UNIX OS agent is <i>kux_tems_teps_tepd_fp0002.tar</i>. Note: Extract the application support files for each OS agent to a unique directory; otherwise, files from the different agents will over-write each other. b. From the directory where you extracted the application support files, launch the application support installer by running the following command: <pre>java -jar <i>directory</i>\CD-ROM\setup.jar</pre> <p>where <i>directory</i> is the directory where you extracted the support files.</p> <p>Note: If you do not have the Java JRE in your path statement, invoke the JRE executable file directly by specifying the path to it on the command line.</p> <p>For example, to run the application support installer for the Windows OS agent, run the following command: <pre>c:\program files\ibm\java142\jre\bin\java -jar / D:\FP2_IMAGES\6.1.0-TIV-ITM_WIN-FP0002\CD-ROM\setup.jar</pre> <p>See “Installing application support” on page 39 for more information.</p> </p> c. Follow the prompts in the application support installation wizard. d. Repeat this for each OS agent in your environment. <p>See “Installing application support” on page 39 for more information about installing this support, including information about identifying the Java installation directory and the detailed steps for the application support installation wizard.</p>
	<p>7. Install the monitoring agents (local and remote).</p>

Monitoring agent checklist - local installation

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

Note: This checklist is for a local installation of the monitoring agent patch. You can also use the remote deployment function to deploy the patches across your monitoring environment. To use remote deploy, use the steps in the "Monitoring agent checklist - remote installation" on page 21.

Table 10. Checklist for locally installing the fix pack on an agent

✓	Installation step
	1. Gather information about the monitoring components in your environment. See "Fix pack installation planning worksheets" on page 9.
	2. Download and extract the patch files to a temporary location on your computer. Patch directory:
	3. Before installing any patches, stop all running IBM Tivoli Monitoring services through the Manage Tivoli Enterprise Monitoring Services utility (CandleManage on Linux and UNIX). Also stop this utility.
	4. Install the 6.1.0-TIV-ITM_INST-FP0002 patch. On Windows, run the following command from the command line: <code>cd patch_dir</code> <code>install_kui.bat</code> On UNIX or Linux, run the following command from the command line: <code>cd patch_dir</code> <code>./install_kui.sh</code> where <i>patch_dir</i> is the directory where you extracted the patch files.
	5. Run the itmpatch command to install the agent patches. <code>itmpatch -h ITMinstall_dir -i patch_file</code> See "Installing patches using the itmpatch command" on page 39 for more information.

Monitoring agent checklist - remote installation

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

Attention:

1. You must have already added these updates to your agent depot, as specified in the “Monitoring server checklist” on page 13.
2. You cannot use the remote deploy function to update an agent locally. If you need to update an agent on the local computer, use the procedure outlined in “Monitoring agent checklist - local installation” on page 20.

Attention:

Table 11. Checklist for remotely deploying the fix pack to an agent

✓	Installation step
	<p>1. Ensure that the Manage Tivoli Enterprise Monitoring Services utility (the kinconfg.exe process) is stopped on all monitoring agents to which you are going to deploy patches.</p>
	<p>2. On the monitoring server, run the tacmd updateAgent command to remotely deploy the agent patches (which you previously added to the agent depot).</p> <pre>tacmd updateAgent -t pc -n node_name</pre> <p>where:</p> <p><i>pc</i> Identifies the product to update, by product code. You have the following choices:</p> <ul style="list-style-type: none"> • AX (UNIX) or GL (Windows) - Tivoli Enterprise Monitoring Agent • NT - Windows OS agent • UI - Common install component (INST patch) • UL - UNIX Log agent • UM - Universal agent • UX - UNIX OS agent <p><i>node_name</i> Identifies the node, the directory on 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.</p> <p>The following example updates the Windows OS agent to the latest level available in the agent depot:</p> <pre>tacmd updateAgent -n Primary:WIN1:NT -t NT</pre> <p>The following example updates a Universal Agent running on UNIX to a specific fix pack level:</p> <pre>tacmd updateAgent -n unix1:KUX -t um -v 061002010</pre> <p>See “Deploying patches to remote agents” on page 43 for more information.</p>

Additional installation information

Be sure to review the following important additional installation information.

Installing the full product media

When you are installing the full product media, which has been updated to include the Fix Pack 002 changes and related agent patches, there are no other special installation instructions except what is noted in this file.

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

Uninstalling the GA level of code

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

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

Upgrading your GA level of code

You *cannot* upgrade an installed product with the fix pack media. The fix pack media replaces all components, overwriting any configuration and customization you have performed.

Adding agents to a patched environment

If you plan to add monitoring agents (both OS and non-OS agents) to your monitoring environment after you have applied Fix Pack 002 and you want to use the remote deploy function (instead of installing locally), you must use the **tacmd createNode** command (for OS agents) or **tacmd addSystem** command (for non-OS agents) to deploy the GA level of the agent and then patch that agent to the fix pack level using the **tacmd updateAgent** command.

You cannot have both the Fix Pack 002 full image and the Fix Pack 002 update image in the agent depot. If your agent depot already contains the full image, you can use the **tacmd removeBundles** command to remove the image from the depot. For example, to remove the AIX 5.3 UNIX OS agent full image bundle, run the following command:

```
tacmd removeBundles -i /mnt/bundles -t ux -p aix513 -v 06100201
```

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

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

The General Availability (GA) versions of the IBM Tivoli Monitoring V6.1 agent CDs for the Windows operating system must *NOT* be installed into an IBM Tivoli

Monitoring V6.1 Fix Pack 002 environment or be used to populate a Tivoli Enterprise Monitoring Server depot. The IBM Tivoli Monitoring V6.1 agent CDs have been refreshed for use with Fix Pack 002.

A problem with the installer on the GA version of the IBM Tivoli Monitoring V6.1 agent CDs for the Windows operating system will cause a currently installed Fix Pack 002 Tivoli Enterprise Monitoring agent framework component to be replaced by the older GA version. When this occurs, the IBM Tivoli Monitoring V6.1 Fix Pack 002 Windows OS agent fails. The problem exists only on the Windows version of the IBM Tivoli Monitoring V6.1 agent CDs.

The IBM Tivoli Monitoring V6.1 agent CDs for the Windows operating system have been refreshed with an updated agent installer as well as a Fix Pack 1 level of the Tivoli Enterprise Monitoring agent framework component. In case a GA version of an IBM Tivoli Monitoring V6.1 agent CD was used to install an agent on a Windows operating system after installing IBM Tivoli Monitoring V6.1 Fix Pack 002 Windows OS agent, running the installer from the refreshed IBM Tivoli Monitoring V6.1 agent CD allows the previous version of Tivoli Enterprise Monitoring agent framework component to be restored to the Fix Pack 002 version. The agent version is *NOT* updated. The agents remain at the GA version.

It is important to note that when the Tivoli Enterprise Monitoring agent framework is overlaid by the GA version on computers where the IBM Tivoli Monitoring V6.1 Fix Pack 002 Windows OS agent has been installed, there is no way to administer the system remotely because the Windows OS agent is the prerequisite to all remote administration capabilities. The local installation procedure described above is the only recovery mechanism.

You need to replace your GA version of the IBM Tivoli Monitoring V6.1 agent CD images for the Windows operating system with the refreshed agent CD images. In addition, non-OS agents must also be recreated in the agent depot. If the GA version of non-OS agents has been placed in the agent depot, the agent bundle must be removed before it can be added back to the depot using the refreshed IBM Tivoli Monitoring V6.1 agent CDs.

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

Identifying a refreshed version of IBM Tivoli Monitoring agent CD images

Identify the refreshed IBM Tivoli Monitoring V6.1 agent CD images by examining the KGLWICMA.ver file in the VERFiles directory of the CD image. The KGLWICMA.ver file indicates a VRMF value of 06100201 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=06100201
```

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

```
C:\IBM\ITM\cms\Depot\Packages\WINNT\KUD\06100000\VERFILES
```

Summary of this section

Every General Availability (GA) version of the IBM Tivoli Monitoring V6.1 agent for Windows operating system CD and installation image must be replaced with the refreshed version. Every GA version of the IBM Tivoli Monitoring V6.1 agent bundle for the Windows operating system installed in a depot must be replaced with the refreshed version before it can be deployed into an IBM Tivoli Monitoring V6.1 Fix Pack 002 environment. You will encounter this scenario only when you install a GA-level application agent *AFTER* you have deployed the Fix Pack 001 or Fix Pack 002 OS agent.

Notes:

1. After you update the GA version of the IBM Tivoli Monitoring V6.1 agent bundle with the refreshed version, that agent bundle *cannot* be used to remotely uninstall the GA version of the agent from an endpoint system.
2. If the Fix Pack 002 version of the Windows OS agent is installed into a system that already contains a GA version agent, you must update that GA version agent with the refreshed version. If you install the Fix Pack 002 Windows OS agent on a computer, you must make sure that any other agents installed on that same computer are updated with that agent's refreshed version. All Windows application agents were refreshed with the updated version of the installation code when Fix Pack 001 was released.
3. If you install the Fix Pack 002 Windows OS agent after installing the GA version of the application agent, the agent framework is updated to the refreshed version. However, if you modify the GA version of the application agent installation by adding another agent from the same image, the KGLWICMA.ver file will no longer be accurate and it will appear as if the agent framework is at the unrefreshed GA version.
4. Do *not* use the **tacmd updateAgent** command to update a GA version of an IBM Tivoli Monitoring V6.1 agent on Windows with a refreshed version. If you do, you can cause the installation of the refreshed agent to create a duplicate entry in the Add/Remove Programs list on the computer that you are updating. If this occurs, delete the duplicate entry by subsequently running a local uninstall of the agent after you remove the refreshed version of the IBM Tivoli Monitoring V6.1 agent.

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

Chapter 3. Known problems and limitations

The following problems might occur during the use of this fix pack. Where available, workaround solutions are provided for the problems.

- The version of the monitoring server returned by the **tacmd listSystems** command and that returned from the **cinfo** command might not match. The **tacmd listSystems** command returns a version of "6.10.02.00," while the **cinfo** command returns the correct version, "6.10.02.01."
- An agent deployment command (such as **tacmd createNode**) fails with a timeout error:

```
KDY0014E - A timeout occurred while waiting for an agent task to complete
          on system
```

The monitoring server might stop working or shut down.

The workaround is to fix the underlying cause of the timeout by either increasing the monitoring server agent deploy timeout period (setting TIMEOUT in seconds in the KBBENV configuration file) or fixing the condition on the agent computer that is causing the timeout (examine the OS agent logs for more information on the cause of the timeout).

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

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

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

- You cannot use "win" in the directory path to remote deployment bundles. If the `imagePath` directory (specified using the `-i|--imagePath` command-line option) specifies a directory whose parent directory starts with "win" (case-insensitive), the CLI truncates the last directory off of the path and replaces it with "Deploy." This results in a "file not found error" being returned for the files in the deployment bundle descriptor file (*.DSC).

For example, a remote deployment bundle is located in "C:\Documents and Settings\Administrator\Desktop\test\win\bundles". We run the following command to deploy the bundle:

```
C:\IBM\ITM\BIN>tacmd addbundles -i
"C:\Documents and Settings\Administrator\Desktop\test\win\bundles" -t nt -f
```

The following output and error are returned:

```
KUICAB020I: Adding bundles to the C:\IBM\ITM\CMS\depot\ depot. The time required
to complete this
operation depends on the number and size of the added bundles.
```


KUICAB010E: The addbundles command did not complete. Refer to the following returned error:

```
java.io.FileNotFoundException:  
C:\Documents and Settings\Administrator\Desktop\test\win\Deploy\KNTWINNT.dsc  
(The system cannot find the path specified)
```

In this example, the CLI replaced the "bundles" directory at the end of the path with "Deploy"; because of this, it couldn't find the file C:\Documents and Settings\Administrator\Desktop\test\win\Deploy\KNTWINNT.dsc because the file actually existed at C:\Documents and Settings\Administrator\Desktop\test\win\bundles\KNTWINNT.dsc.

- If you are running the OMEGAMON XE for Messaging agent (a 32-bit agent) on a Linux or UNIX computer, you must install the 32-bit agent framework to support the application agent. Use the following steps to install the 32-bit framework:

1. In the directory where you extracted the base IBM Tivoli Monitoring V6.1 installation files, run the following command:

```
./install.sh
```

2. When prompted for the IBM Tivoli Monitoring home directory, press Enter to accept the default (/opt/IBM/ITM) or type the full path to a different directory.

3. If the installation directory does not already exist, you are asked if you want to create it. Type y to create this directory and press Enter.

4. The following prompt is displayed:

```
Select one of the following:
```

- 1) Install products to the local host.
- 2) Install products to depot for remote deployment (requires TEMS).
- 3) Exit install.

```
Please enter a valid number:
```

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

Type 1 to start the installation and press Enter.

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

6. Press Enter to display the agreement.

7. Type 1 to accept the agreement and press Enter.

8. Type a 32 character encryption key and press Enter. This key should be the same as the key that was used during the installation of the monitoring server to which this monitoring agent connects.

A numbered list of available operating systems is displayed.

9. Type the number for the *32-bit version* of the operating system that you are installing on. So, if you are installing on a 64-bit AIX V5.3 computer, type the number that corresponds to 32-bit AIX V5.3. The default value is your current operating system. Press Enter.

10. Type y to confirm the operating system and press Enter.

A numbered list of available components is displayed.

11. Type the number that corresponds to "Tivoli Enterprise Services User Interface V06.10.02.00" and press Enter.

A list of the components to install is displayed.

12. Type y to confirm the installation.

The installation begins.

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

You can now install the OMEGAMON XE for Messaging agent.

- In some instances when upgrading custom workspaces from OMEGAMON® 350 to IBM Tivoli Monitoring V6.1 Fix Pack 002, 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. IBM Tivoli Monitoring automatically sets the default workspace to the last workspace in the list.

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 **Cancel**.
5. Close the portal.
6. When you reopen the portal, the default workspace should be correctly displayed.

Chapter 4. Installing and configuring the Warehouse Proxy on Linux computers

Fix Pack 002 adds support for the Warehouse Proxy agent on Linux systems. The Warehouse Proxy on Linux uses a JDBC connection to export data collected from Tivoli Enterprise Monitoring agents to the Tivoli Data Warehouse. The Tivoli Data Warehouse can be located on the Linux system where you install the Warehouse Proxy agent or it can be located on a remote system.

Software prerequisites

The following prerequisite software is required for setting up a warehouse proxy on Linux computers:

- IBM DB2 UDB version 8 Fix Pack 10, or higher, is required to support the Tivoli Data Warehouse.
- X Windows is required to configure the Warehouse Proxy agent on Linux.

Overview of steps

Perform the following tasks to set up an operational Warehouse Proxy on Linux:

1. Create the Tivoli Data Warehouse database and a user to connect to the database.
2. Install the Warehouse Proxy agent.
3. Copy the JDBC driver files to the local system.
4. Configure the Warehouse Proxy agent.
5. Start the Warehouse Proxy agent.

Creating the Tivoli Data Warehouse database

To support a Warehouse Proxy on Linux, you must use IBM DB2[®] for the Tivoli Data Warehouse database. Refer to the DB2 product documentation for information on how to create a database or have a database administrator create the database for you. For guidance on planning the size and disk requirements for the Tivoli Data Warehouse database, see "Planning considerations for the Tivoli Data Warehouse" in the *IBM Tivoli Monitoring Installation and Setup Guide*.

When you create the database for the Tivoli Data Warehouse, follow these guidelines:

- Create the data warehouse database with UTF-8 encoding.
- Create a name for the data warehouse database, and a user name and password to access the data warehouse. Consider using the default values shown in Table 12. The default values are displayed in the fields of the configuration window for the Warehouse Proxy. (See Figure 2 on page 32.)

Table 12. Default values for Tivoli Data Warehouse parameters

Parameter	Default value
Tivoli Data Warehouse database name	WAREHOUS
User name	itmuser
User password	itmpswd1

- Give the user authority to create and update tables, to insert information into the tables, to create indexes for the tables, and to grant public authority to the tables. Include *create tablespace* and *create bufferpool* authorities.

Installing the Warehouse Proxy agent

To install the Warehouse Proxy agent on a Linux system, see the section entitled "Linux or UNIX: Installing a monitoring agent" in the *IBM Tivoli Monitoring Installation and Setup Guide*. Follow the instructions within the following subsections:

- "Installing the monitoring agent"
- "Changing the file permissions for agents" (if you used a non-root user to install the Warehouse Proxy)

Note: Do not use the patch installer to install the Warehouse Proxy agent on Linux.

Installation log files are in the `$CANDLEHOME/logs` directory:

- C trace : `<hostname>_hd_<date>-0<#>.log`
- Java trace: `<hostname>_hd_java_<date>-0<#>.log`

There can be 5 files maximum for the C trace and 6 files for the Java trace. The first log file (#1) is always kept; subsequent log files are kept up to the 5th (C trace) or 6th (Java trace) file. When the maximum number of files is reached, the next file replaces the oldest existing log file (#2).

Copying the JDBC driver files to the local system

JDBC driver JAR files are included with the IBM DB2 product installation on the system where your Tivoli Data Warehouse is located. If the Tivoli Data Warehouse is located on a remote system, copy the driver files to the local system (the Linux system where you installed the Warehouse Proxy agent).

Following are the directory locations and names of the driver files for DB2. You can copy the files to any directory on the local system.

```
<db2installdir>/java/db2jcc.jar  
<db2installdir>/java/db2jcc_license_cu.jar
```

where `<db2installdir>` is the directory where DB2 was installed. The default DB2 installation directory for DB2 Version 8.1 on Linux is `/opt/IBM/db2/V8.1`.

Configuring the Warehouse Proxy agent

After you install the Warehouse Proxy agent and the JDBC drivers on a Linux system, you are ready to configure the Warehouse Proxy agent. The purpose of configuration is to establish the JDBC connection between the Warehouse Proxy agent and the Tivoli Data Warehouse and to register the Warehouse Proxy agent with the Tivoli Enterprise Monitoring Server.

1. Log on to the Linux computer where the Warehouse Proxy agent is installed.
2. Start the Manage Tivoli Enterprise Monitoring Services utility:
 - a. Change to the bin directory:

```
cd install_dir/bin
```

b. Run the following command:

```
./itmcmd manage [-h install_dir] [-s]
```

where:

Table 13. Parameters for the itmcmd manage command

-h	(optional) An option used to specify the installation directory.
install_dir	The directory where the Warehouse Proxy agent is installed. The default installation directory is /opt/IBM/ITM.
-s	(optional) Option to specify safe mode operation. Safe mode invokes the JRE with the -nojit option (no just-in-time compiler). If you encounter a Java failure error, try running the command as before, but also specifying the -s option. Entering the above commands with -? displays the syntax for using the -s option.

The Manage Tivoli Enterprise Monitoring Services window is displayed.

Note: Note that the **Platform** column for agents lists the platform that the binary code was built on, not the platform that you are running on.

3. Right-click **Warehouse Proxy**.
4. Click **Configure**.

The Configure Warehouse Proxy window is displayed.

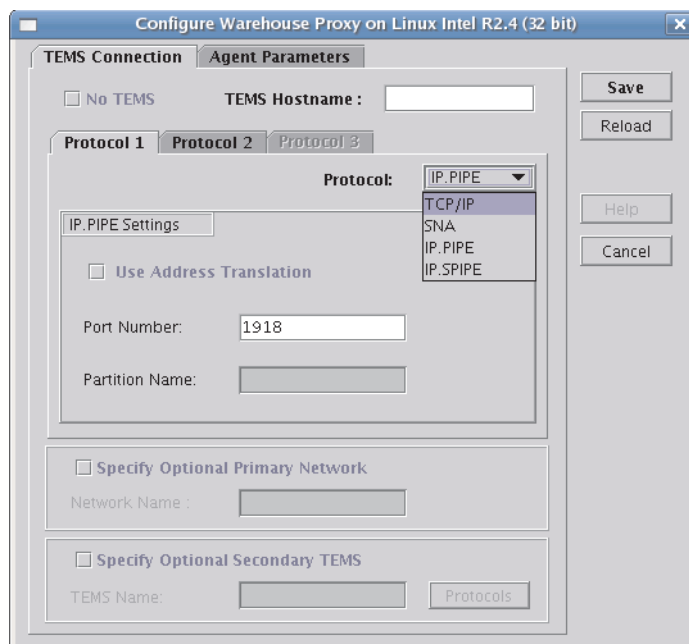


Figure 1. Registering the Warehouse Proxy agent with the Tivoli Enterprise Monitoring Server

5. On the TEMS Connection page, enter information about the Tivoli Enterprise Monitoring Server to which the Warehouse Proxy agent connects:

- Enter the host name of the monitoring server in the **TEMS Hostname** field. (If the field is not active, clear the **No TEMS** check box.)
 - Select the communications protocol that the monitoring server uses from the **Protocol** drop-down list.
 - Enter the port number of the monitoring server in the **Port Number** field.
6. Click the **Agent Parameters** tab.

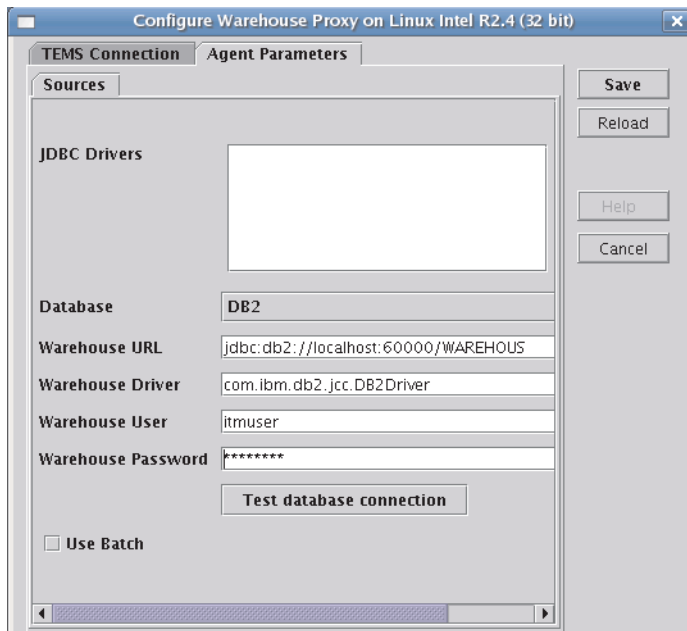


Figure 2. Configuring the JDBC connection for the Warehouse Proxy agent

7. Add the names and directory locations of the JDBC driver JAR files to the **JDBC Drivers** list box:
- a. Use the scroll bar at the bottom of the window to display the **Add** and **Delete** buttons, which are located to the right of the **JDBC Drivers** list box.
 - b. Click **Add** to display the file browser window. Navigate to the location of the driver files on this computer and select the driver files: db2jcc.jar and db2jcc_license_cu.jar.
 - c. Click **OK** to close the browser window and add the JDBC driver files to the list.

If you need to delete an entry from the list, select the entry and click **Delete**.

8. In the **Database** drop-down list, select **DB2**.
9. Change the default value displayed in the **Warehouse URL** field if it is not correct. The default Tivoli Data Warehouse URL for IBM DB2 is as follows:

```
jdbc:db2://localhost:60000/WAREHOUS
```

- If the Tivoli Data Warehouse is installed on a remote computer, specify the host name of the remote computer instead of localhost.
- Change the port number if it is different.
- If the name of the Tivoli Data Warehouse database is not WAREHOUS, replace WAREHOUS with the actual name. (See “Creating the Tivoli Data Warehouse database” on page 29.)

10. Verify the JDBC driver name, which is displayed in the **Warehouse Driver** field. (Note that the **Warehouse Driver** field displays the *driver name*, in contrast to the *driver JAR files* that are listed in the **JDBC Drivers** field.)

The JDBC driver name for IBM DB2 is as follows:

```
com.ibm.db2.jcc.DB2Driver
```

11. If necessary, change the entries in the **Warehouse User** and **Warehouse Password** fields to match the user name and password that were created for the Tivoli Data Warehouse. (See “Creating the Tivoli Data Warehouse database” on page 29.) The default user name is `itmuser` and the default password is `itmpswd1`.
12. Check the **Use Batch** check box if you want the Warehouse Proxy agent to submit multiple execute statements to the Tivoli Data Warehouse database for processing as a batch.
In some situations, such as crossing a network, sending multiple statements as a unit is more efficient than sending each statement separately. Batch processing is one of the features provided with the JDBC 2.0 API.
13. Click **Test database connection** to ensure you can communicate with the Tivoli Data Warehouse database.
14. Click **Save**.

Start the Warehouse Proxy

- To start the Warehouse Proxy agent from the Manage Tivoli Enterprise Services window, right-click **Warehouse Proxy** and select **Start**.
- To start the Warehouse Proxy agent from the command line, enter the following command:

```
./itmcmd agent start hd
```

where `hd` is the product code for the Warehouse Proxy agent.

Chapter 5. Installing and configuring multiple Warehouse Proxy agents

Fix Pack 002 introduces support for multiple warehouse proxies within a single hub monitoring server environment. The provision for multiple warehouse proxies provides for greater scalability and performance in historical data collection.

About multiple Warehouse Proxy support

The support for multiple warehouse proxies has the following important features:

- All Warehouse Proxy agents within a single hub monitoring server environment export data to a single Tivoli Data Warehouse.
- Each Warehouse Proxy agent is associated with a subset of monitoring server instances that you specify when you configure the proxy agent. Each warehouse proxy exports data only for monitoring agents that report to one of the monitoring servers on the specified list.

The following sequence of events explains how the monitoring agents, which collect the data for historical reports, know which Warehouse Proxy agent to use:

1. When a Warehouse Proxy agent starts, it registers with the global location broker on the hub monitoring server, sending it the list of monitoring servers that it is configured to serve. This registration process is repeated every hour.
2. Each monitoring server queries the global location broker at regular intervals to determine which warehouse proxy it is associated with. The monitoring server then sends the address of this warehouse proxy to all of its child monitoring agents to use during historical data exports. You can change the default query interval of 60 minutes to some other value.

When a Warehouse Proxy agent registers with the global location broker, it is registered as the default proxy agent if no other proxy agent is already configured as the default. When a monitoring server queries the global location broker for its associated warehouse proxy, the default proxy agent is used if that monitoring server is not on the list of servers for any proxy agent.

Installing and configuring the proxy agents

Use the following procedure to install and configure each Warehouse Proxy agent:

1. Install each proxy agent using the procedures described in the *IBM Tivoli Monitoring V6.1 Installation and Setup Guide*. To set up a proxy agent on Linux, see Chapter 4, "Installing and configuring the Warehouse Proxy on Linux computers," on page 29. (Note that a Warehouse Proxy on Linux must communicate with a Tivoli Data Warehouse on IBM DB2.)

The procedure for installing a proxy agent into an environment with multiple proxy agents is the same as the procedure for installing a single proxy agent.

2. Associate each proxy agent with the list of monitoring servers that you want the proxy agent to serve:
 - a. Open the environment file for the proxy agent:
 - (Windows) %CANDLE_HOME%\TMAITM6\KHDENV
 - (Linux) \$CANDLEHOME/config/hd.ini

- b. Add the environment variable KHD_WAREHOUSE_TEMS_LIST to the file and set it to specify a space-delimited list of monitoring server instance names. For example:

```
KHD_WAREHOUSE_TEMS_LIST=REMOTE_TEMS1 REMOTE_TEMS2
```

The name of a monitoring server is specified when the server is installed.

The default name of a monitoring server is HUB_ *host_name* (for a hub monitoring server) or REMOTE_ *host_name* (for a remote monitoring server), where *host_name* is the short host name.

3. Optionally modify the interval at which a monitoring server queries the global location broker to find out which warehouse proxy it is associated with:

- a. Open the environment file for the monitoring server:

- (Windows) %CANDLE_HOME%\CMS\KBBENV
- (UNIX or Linux) \$CANDLEHOME/config/ms.ini

- b. Change the following entry to specify a different query interval:

```
KPX_WAREHOUSE_REGCHK=60
```

The query interval is specified in minutes. The default value is 60 minutes.

4. Start the Warehouse Proxy agent:

- To start a Warehouse Proxy agent on Windows or Linux from the Manage Tivoli Enterprise Services window, right-click **Warehouse Proxy** and select **Start**.
- To start a Warehouse Proxy agent on Linux from the command line, enter the following command:

```
./itmcmd agent start hd
```

where hd is the product code for the Warehouse Proxy agent.

Verifying the configuration

Use the following trace settings to verify the configuration:

- To verify that a warehouse proxy is registering with the hub monitoring server and placing the correct entries into the global location broker:

1. Open the environment file for the proxy agent:

- (Windows) %CANDLE_HOME%\TMAITM6\KHDENV
- (Linux) \$CANDLEHOME/config/hd.ini

2. Add the following entry to the KBB_RAS1 trace setting:

```
KBB_RAS1=ERROR(UNIT:khdxrpcr STATE)
```

This setting prints the value of KHD_WAREHOUSE_TEMS_LIST and shows any errors associated with its components.

- To determine which warehouse proxy a particular monitoring server uses for its agents:

1. Open the environment file for the monitoring server:

- (Windows) %CANDLE_HOME%\CMS\KBBENV
- (UNIX or Linux) \$CANDLEHOME/config/ms.ini

2. Add the following entry to the KBB_RAS1 trace setting:

```
KBB_RAS1=ERROR(UNIT:kprwhpx STATE)
```

This setting prints entries in the RAS log of the monitoring server when a registration change occurs. The entry specifies the name and address of the new Warehouse Proxy agent that the monitoring server is using.

Appendix A. Detailed installation procedures for installing the component patches

The following sections provide detailed instructions for installing the fix pack component patches. Use these sections in conjunction with the installation checklists to complete your installation.

Installing the 6.1.0-TIV-ITM_INST-FP0002 patch

Run the following command to install the 6.1.0-TIV-ITM_INST-FP0002 patch on all monitoring components:

On Windows, run:

```
cd patch_dir
install_kui.bat
```

where *patch_dir* is the directory where you extracted the patch files.

On UNIX or Linux, run:

```
cd patch_dir
./install_kui.sh
```

Installing patches using the `itmpatch` command

Run the following command to install the component patches:

```
itmpatch -h ITMinstall_dir -i patch_file
```

where *ITMinstall_dir* is the location where IBM Tivoli Monitoring is installed and *patch_file* is the name and location of the patch.

You can also use the **itmpatch** command to generate a report that identifies the actions a patch will take. Run the following command to preview a patch:

```
itmpatch -h ITMinstall_dir -t patch_file
```

The following example installs the 6.1.0-TIV-ITM_TEMS-FP0002 patch on a Windows monitoring server:

```
itmpatch.exe -h c:\ibm\itm -i c:\temp\6.1.0-TIV-ITM_TEMS-FP0002
```

For additional information about the **itmpatch** command, including other parameters for the command, see Appendix B, “Using the patch installer,” on page 45.

Installing application support

Use the following steps to install the application support on the monitoring server, portal server, and portal desktop client. Application support files include the situations, policies, and workspaces for an agent. Application support files are located in a subdirectory of the agent patch package.

1. Download and extract the agent patch file (the 6.1.0-TIV-ITM_*platform*-FP002.tar file) for each OS agent in your environment

This creates a directory structure that contains patches for all of the supported operating systems.

2. Extract the compressed files that contain the application support files for each patch. Look for a file named "*pc_tems_teps_tepd_fp0002.tar*," where *pc* is "k" plus the 2-letter product code for the agent. For example, the file for the UNIX OS agent is *kux_tems_teps_tepd_fp0002.tar*.

Note: Extract the application support files for each OS agent to a unique directory; otherwise, files from the different agents will over-write each other.

3. Start the Application Support Installer GUI to install the patch. Run the following command from within the patch CD-ROM directory:

```
java -jar setup.jar
```

Note that you need to either have the IBM Java JRE v1.4.2 in your path or invoke the JRE executable directly by specifying the path to it on the command line. So, instead of the above command, you'd run:

```
Java_installDir\java -jar setup.jar
```

Note: To determine the location of the JRE on a UNIX computer, run the following command:

```
which java
```

This returns the install location for the Java JRE.

To ensure that the level of JRE is 1.4.2, run the following command from the directory where the JRE is installed:

```
java -version
```

If it is not 1.4.2, you must download the IBM Java JRE v1.4.2 from the IBM Software Support Web site.

4. Click **Next** on the Welcome window.
5. Type the location where IBM Tivoli Monitoring is installed on your monitoring server. For Windows computers, this location is detected automatically. For UNIX computers, either type the location in or click **Browse** to find the directory.
6. Type the location where the support files that you want to install are located. When you extract the downloaded file, the following directory structure is created:

```
CD-ROM
  TEMS
  TEPS
  TEPD
  product.properties
```

Type the path to the CD-ROM directory.

7. Click **Next**. A list of applications for which support can be installed is displayed.
8. Select component on which you want to install support (monitoring server, portal server, or portal desktop client) and click **Next**.
9. Select the applications for which you want to install application support and click **Next**.

10. If you are trying to install application support for a component that you have already installed support for, a warning window is displayed. You can choose to continue by simply clicking **Next**. The existing installed support files are overwritten.

If you do not want to overwrite your existing application files, clear the box next to the application and click **Next**. The application support files for this application are not installed.

11. Review the summary of what is going to be installed and click **Next**.

This summary tells you what is going to happen to your computer during the installation, such as starting, stopping, and restarting the monitoring server as application support for each application is installed.

A progress window is displayed to show the installation progress.

Note: If you are trying to install support for more than one component (monitoring server, portal server, or portal desktop client) and the support files are already installed, you get a warning for each component, enabling you to select which components you want to re-install support for.

12. When the installation is complete, click **Finish**.

13. Exit and then restart any portal clients (desktop or browser).

Using a response file to install the application support files

You can install the application support files on the IBM Tivoli Monitoring components through the silent install method using a response file.

Note: If your UNIX or Linux computer does not have X-Windows, you must use the silent installation method.

Performing a silent install involves the following three steps:

1. "Creating a response file"
2. "Running the silent installation" on page 42
3. "Examining the installation log file" on page 42

Creating a response file

Create a text file called response.txt that contains the following lines:

```
# IBM Tivoli Monitoring installation directory
-W Directories.itmhome="/opt/ibm"

# Directory where the application support media is located
-W Directories.mediaLocation="/opt/appsupport"

# Select "true" to install monitoring server support files
-W ComponentSelectionPanel.temsSelected="true"

# Select "true" to install portal server support files
-W ComponentSelectionPanel.tepsSelected="true"

# Select "true" to install portal desktop client support files
-W ComponentSelectionPanel.tepdSelected="true"

# Comma-separated list of directories with the application media location to
# install. These are directories that contain the product support files and
# are sub-directories under the specified media location
-W ProductSelectionPanel.products="kqf-v1.0,kqc-v1.0"

# Set this flag to "true" if you want to re-install if the
# specified product is already installed. This overwrites
```

```
# any previously installed support files for this product.
-W ProductSelectionPanel.reinstall="true"

# Setting this flag to "true" confirms that you have purchased
# an OMEGAMON DE license. If any product requires a DE LICENSE
# and this flag is "false" installation will fail
-W ProductSelectionPanel.deLicense="false"
```

Running the silent installation

Run the installation from the command-line interface by running the following command:

```
setup<platform> -silent -options response.txt
```

where <platform> is the operating system you are installing on:

- Windows: setupwin32.exe
- AIX: ./setupaix.bin
- Solaris: ./setupSolaris.bin
- Linux for Intel: ./setupLinux.bin
- Linux for z/OS: ./setuplinux390.bin

Examining the installation log file

The log file, named ITM_AppSupport_SilentInstall.log, is written to the /tmp directory on Linux and UNIX computers and on Windows, in the directory defined by the TEMP environment variable. Review the contents of this file to determine if the installation succeeded.

The following example shows a sample installation log file:

```
(Oct 13, 2005 6:52:20 PM), Started Silent Installation
(Oct 13, 2005 6:52:20 PM), Installing application support files for Tivoli
Enterprise Monitoring Server (TEMS)
(Oct 13, 2005 6:52:20 PM), Installing application support files for Tivoli
Enterprise Portal Server (TEPS)
(Oct 13, 2005 6:52:20 PM), Installing application support files for Tivoli
Enterprise Desktop Client (TEPD)
(Oct 13, 2005 6:52:20 PM), User confirmed that they have OMEGAMON DE License by
stating -W ProductSelectionPanel.deLicense="true" in the response file.
(Oct 13, 2005 6:52:20 PM), Application support files will be overwritten if
necessary. This was enabled by specifying the following in the response file:
-W ProductSelectionPanel.reinstall="true"
(Oct 13, 2005 6:52:20 PM), WARNING: Re-installing TEMS application support for
"IBM Tivoli OMEGAMON XE for Microsoft .NET: .NET Framework".
(Oct 13, 2005 6:52:20 PM), WARNING: Re-installing TEPS application support for
"IBM Tivoli OMEGAMON XE for Microsoft .NET: .NET Framework".
(Oct 13, 2005 6:52:21 PM), WARNING: Re-installing TEPD application support for
"IBM Tivoli OMEGAMON XE for Microsoft .NET: .NET Framework".
(Oct 13, 2005 6:52:21 PM), Starting the Tivoli Enterprise Monitoring Server (TEMS)
(Oct 13, 2005 6:52:29 PM), Adding TEMS support for IBM Tivoli OMEGAMON XE for
Microsoft .NET: .NET Framework Version 01.10.00.00
(Oct 13, 2005 6:52:30 PM), Stopping the Tivoli Enterprise Monitoring Server (TEMS)
(Oct 13, 2005 6:53:45 PM), Pausing 60 seconds
(Oct 13, 2005 6:55:15 PM), Starting the Tivoli Enterprise Monitoring Server (TEMS)
(Oct 13, 2005 6:55:39 PM), Stopping the Tivoli Enterprise Portal Server (TEPS)
(Oct 13, 2005 6:55:54 PM), Performing initial TEPS configuration
(Oct 13, 2005 6:55:54 PM), Adding TEPS support for IBM Tivoli OMEGAMON XE for
Microsoft .NET: .NET Framework Version 01.10.00.00
(Oct 13, 2005 6:55:54 PM), Performing final TEPS configuration - can take up to 20
minutes, please wait
(Oct 13, 2005 6:57:08 PM), Starting the Tivoli Enterprise Portal Server (TEPS)
(Oct 13, 2005 6:57:21 PM), Adding TEP Desktop Client support for IBM Tivoli
OMEGAMON XE for Microsoft .NET: .NET Framework Version 01.10.00.00
(Oct 13, 2005 6:57:21 PM), Installation completed successfully
```

Adding patches to the agent depot

You can remotely deploy the following patches:

- 6.1.0-TIV-ITM_INST-FP0002 -- IBM Tivoli Monitoring Global-common Component
- 6.1.0-TIV-ITM_TEMA-FP0002 -- ITM Shared Libraries
- 6.1.0-TIV-ITM_UA-FP0002 -- Universal Agent (UM)
- 6.1.0-TIV-ITM_UNIX-FP0002 -- UNIX OS Monitoring Agent (UX)
- 6.1.0-TIV-ITM_WIN-FP0002 -- Windows OS Monitoring Agent (NT)
- 6.1.0-TIV-ITM_UXLOG-FP0002 -- UNIX Log Agent (UL)

Run the following command from the patch directory to add the patches to the agent depot on the monitoring server:

```
$CANDLEHOME/bin/tacmd addBundles -i patch_file -n
```

where *patch_file* is the location of the patch.

Repeat this step for each agent patch.

For example, to add the 6.1.0-TIV-ITM_TEMA-FP0002 patch to the depot, run the following command:

```
$CANDLEHOME/bin/tacmd addBundles -i D:\FP2_IMAGES\6.1.0-TIV-ITM_TEMA-FP0002 -n
```

For additional information about the **tacmd addbundles** command, see the *IBM Tivoli Monitoring Installation and Setup Guide*.

Deploying patches to remote agents

Run the following command from the monitoring server to remotely deploy the agent patches (which you previously added to the agent depot):

```
$CANDLEHOME/bin/tacmd updateAgent -t pc -n node_name
```

where:

pc Indicates the two-letter product code for the agent (such as "UM" for the Universal Agent)

node_name

Indicates the name of the computer and OS agent to which you want to deploy the update. For example, "Primary:*host_name*:NT" is the node name for a Windows OS agent. You can use the **tacmd listSystems** command to determine the node name.

Repeat this step on each agent in your environment for each agent patch you want to deploy.

Note: If you have a large number of monitoring agents to which to deploy updates, consider using the `itmpatchagents` script, available as a sample from the IBM Software Support Web site (<http://www-306.ibm.com/software/sysmgmt/products/support/IBMTivoliMonitoringV6.html>). This script enables the automatic deployment of updates across your monitoring environment.

Appendix B. Using the patch installer

The patch installer runs as a standalone command-line interface (CLI) that you can run locally or remotely using the remote deployment function. The patch installer performs the following functions:

- Determines the set of products that are running in your environment so that it can restart products that might have been stopped to apply a patch
- Preserves file permissions when a patch updates files
- Delivers cumulative interim fix packs
- Installs agent components such as Java Runtime Environments and Global Security Kit (GSKit, which is used for Secure Socket Layer TCP/IP connections using public key encryption/decryption methodologies)
- Installs agent patches locally
- Can be used with remote deployment to remotely install agent patches

The Patch Installer creates and maintains a file called `patches.hist`, which is located in the `ITMinstall_dir/patchlogs` directory, that records each patch installation attempt. This file includes the following information:

- Which fix packs were installed
- Which components were fix packs installed against
- The date and time the patch was installed
- If the patch installation was successful or aborted because of an error.

Important: Each line in the `patches.hist` file corresponds to a patch installation attempt. This file is not rolled back and must never be deleted.

The `itmpatch` command has the following syntax:

```
itmpatch -h ITMinstall_dir {-i|-t} { patch_file_directory | patch_file }
```

where:

-h *ITMinstall_dir*

Defines the installation directory for IBM Tivoli Monitoring.

-i Specifies the path to the directory or patch file to be installed.

-t Generates a report of the actions that will be performed by the patch. This option does *not* install the patch. Use this option to preview the patch.

The following example creates a report about a patch on a UNIX computer:

```
$CANDLEHOME/bin/itmpatch -h $CANDLEHOME -t $PATCH
```

The following example installs a patch on a Windows computer:

```
itmpatch.exe -h %CANDLE_HOME -i %PATCH%
```

Appendix C. Notices

This information was developed for products and services offered in the U.S.A. IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785 U.S.A.

For license inquiries regarding double-byte (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

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

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law:

INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement might not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

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

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

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

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

Trademarks

IBM, the IBM logo, AIX, DB2, i5/OS, iSeries, OMEGAMON, OS/400, pSeries, Tivoli, the Tivoli logo, Tivoli Enterprise, Tivoli Enterprise Console, z/OS, and zSeries are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both.

Intel is a trademark of Intel Corporation in the United States, other countries, or both.

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

Microsoft is a registered trademark of Microsoft Corporation in the United States, other countries, or both.

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

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

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



Printed in USA