

# Deployment Guide Series: IBM Tivoli Monitoring V 6.1

Step-by-step deployment guide for IBM  
Tivoli Monitoring V 6.1

Covers small to large  
environments

Discusses best practices  
for a deployment plan



Vasfi Gucer  
Ana Godoy





International Technical Support Organization

**Deployment Guide Series: IBM Tivoli Monitoring V  
6.1**

December 2005

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

**First Edition (December 2005)**

This edition applies to IBM Tivoli Monitoring Version 6, Release 1.

This document created or updated on November 21, 2005.

© Copyright International Business Machines Corporation 2005. All rights reserved.

Note to U.S. Government Users Restricted Rights -- Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.

# Contents

<b>Figures</b> .....	vii
<b>Tables</b> .....	xiii
<b>Examples</b> .....	xv
<b>Notices</b> .....	xvii
Trademarks .....	xviii
<b>Preface</b> .....	xix
The team that wrote this redbook .....	xix
Become a published author .....	xx
Comments welcome .....	xx
<b>Chapter 1. Introduction</b> .....	1
1.1 Enterprise management challenges .....	2
1.1.1 Business driving forces .....	2
1.2 IBM Tivoli Monitoring solutions .....	3
1.3 What's new for IBM Tivoli Monitoring, V5.x clients? .....	6
1.4 What's new for OMEGAMON XE/DE clients? .....	7
1.5 What's new for Distributed Monitoring, V3.7 clients? .....	7
1.6 IBM Tivoli Monitoring, V6.1 value proposition .....	7
1.7 IBM Tivoli Monitoring, V6.1 components .....	9
1.8 What is new in the IBM Tivoli Data Warehouse, V2.1? .....	13
<b>Chapter 2. Architecture and planning</b> .....	15
2.1 IBM Tivoli Monitoring, V6.1 components .....	16
2.1.1 Platform Support Matrix - IBM Tivoli Monitoring, V6.1 (GA) .....	22
2.2 IBM Tivoli Monitoring, V6.1 deployment scenarios .....	24
2.2.1 Demo installation - (single machine) .....	27
2.2.2 Small/Medium installation - (400 agents maximum) .....	28
2.2.3 Large installation - (4000 agents maximum) .....	30
2.2.4 Huge installation - (greater than 4000 agents) .....	33
2.2.5 Advanced large installation with firewall scenarios .....	39
2.2.6 Advanced huge installation - multiple TEMS processes .....	47
2.3 Scalability .....	50
2.4 Agent deployment architecture .....	53
2.4.1 IBM Tivoli Monitoring, V6.1 built-in Deployment Controller .....	54
2.4.2 IBM Tivoli Configuration Manager, V4.2 .....	56

2.4.3	Operating system image deployment . . . . .	56
<b>Chapter 3. Demonstration, proof of concept and small size installation. 59</b>		
3.1	DB2 Workgroup Server Edition installation and configuration. . . . .	60
3.1.1	Installing DB2 Workgroup Server Edition . . . . .	60
3.1.2	Creating the Tivoli Datawarehouse database . . . . .	64
3.1.3	Creating the database user. . . . .	65
3.1.4	Setting up ODBC connection for Tivoli Data Warehouse Proxy . . . .	69
3.2	IBM Tivoli Monitoring, V6.1 components installation. . . . .	70
3.2.1	Installing IBM Tivoli Monitoring, V6.1 . . . . .	71
3.2.2	Launching Tivoli Enterprise Portal . . . . .	93
3.2.3	Configuring Warehouse Summarization and Pruning Agent. . . . .	96
3.2.4	Installing IBM Tivoli Monitoring Agents . . . . .	98
<b>Chapter 4. Medium and large environment installation. . . . . 105</b>		
4.1	Lab environment . . . . .	106
4.1.1	Hardware and software configuration . . . . .	106
4.1.2	Lab architecture . . . . .	107
4.2	Installing IBM Tivoli Monitoring, V6.1 . . . . .	110
4.2.1	Planing the installation . . . . .	110
4.2.2	Define the architecture . . . . .	112
4.2.3	Creating a deployment plan . . . . .	112
4.2.4	Backup strategies . . . . .	117
4.2.5	Installing and configuring the scenario-1 environment . . . . .	117
4.2.6	Installing a Remote TEMS on a Windows and UNIX server. . . . .	131
4.2.7	Tivoli Enterprise Portal Server - TEPS . . . . .	135
4.2.8	Tivoli Enterprise Monitoring Agent - TEMA . . . . .	143
4.2.9	Deploying TEMA from command line interface. . . . .	171
4.2.10	Installing a new managed systems - Microsoft Exchange example	173
4.2.11	Tivoli Enterprise Portal -TEP. . . . .	174
4.2.12	Warehouse Proxy installation and configuration . . . . .	178
4.2.13	Summarization and Pruning agent (SPA) installation and configuration	186
4.2.14	Event Synchronization installation . . . . .	196
4.2.15	Configuring the Hot Standby. . . . .	211
4.2.16	Installing and configuring the scenario-2 environment . . . . .	218
4.2.17	Replacing a Hub TEMS server with a new one. . . . .	225
4.3	Uninstalling IBM Tivoli Monitoring, V6.1 . . . . .	228
4.3.1	Uninstalling the entire IBM Tivoli Monitoring environment . . . . .	228
4.3.2	Uninstalling an individual IBM Tivoli Monitoring agent or component. .	231
4.3.3	Uninstalling the IBM Tivoli Enterprise Console Event Synchronization	232

<b>Chapter 5. Working with IBM Tivoli Monitoring, V6.1</b>	235
5.1 Understanding Tivoli Enterprise Portal client	236
5.1.1 Launching the Tivoli Enterprise Portal	236
5.1.2 Tivoli Enterprise Portal components	236
5.2 Working with Tivoli Enterprise Portal	238
5.2.1 Creating a new workspace and add custom views	238
5.2.2 Working with queries	244
5.2.3 Working with a situation and events	269
5.2.4 Policies for automation	275
5.3 Working with Tivoli Data Warehouse	282
<b>Related publications</b>	291
IBM Redbooks	291
Other publications	291
Online resources	291
How to get IBM Redbooks	292
Help from IBM	292
<b>Index</b>	293





# Figures

1-1	IBM Tivoli Monitoring solutions . . . . .	4
1-2	Monitoring composite application infrastructures. . . . .	5
1-3	IBM Tivoli Monitoring, V6.1 emerges from the best of OMEGAMON and ITM 5 8	
1-4	BM Tivoli Monitoring 6.1 components . . . . .	10
1-5	Tivoli Enterprise Portal. . . . .	13
2-1	IBM Tivoli Monitoring, V6.1 component model . . . . .	16
2-2	Platform support matrix - IBM Tivoli Monitoring, V6.1 . . . . .	23
2-3	Platform support matrix - IBM Tivoli Monitoring, V6.1 (continued). . . . .	24
2-4	IBM Tivoli Monitoring, V6.1, lab topology. . . . .	26
2-5	IBM Tivoli Monitoring, V6.1, small/medium topology design . . . . .	29
2-6	IBM Tivoli Monitoring, V6.1, large topology design . . . . .	31
2-7	IBM Tivoli Monitoring, V6.1, huge installation topology . . . . .	34
2-8	Right clicking on Tivoli Enterprise Portal reveals Create Instance option	36
2-9	Inputting the Instance Name within the dialog box . . . . .	36
2-10	Inputting the Tivoli Enterprise Portal hostname in the TEP Server field	37
2-11	The newly defined Tivoli Enterprise Portal instance . . . . .	38
2-12	Example of additional Tivoli Enterprise Portal instances . . . . .	38
2-13	Advanced Installation with firewalls, warehouse proxy agent on less secure side	45
2-14	Advanced Installation with firewalls, warehouse proxy agent on more secure side	46
2-15	Large installation with multiple TEMS processes running on single system	49
2-16	Universal sources of scalability and performance numbers. . . . .	51
2-17	Agent deployment architecture . . . . .	54
3-1	DB2 Setup wizard- Select the installation type . . . . .	61
3-2	DB2 Setup wizard - Select installation folder. . . . .	62
3-3	Set user information for the DB2 Administration Server . . . . .	63
3-4	DB2 Setup wizard - Start copying files. . . . .	64
3-5	Services management console . . . . .	65
3-6	Computer Management, adding a New User. . . . .	66
3-7	New User interface . . . . .	67
3-8	Adding Groups to itm61 user. . . . .	68
3-9	Adding Administrators group. . . . .	69
3-10	Create New Data Source . . . . .	70
3-11	Welcome to IBM Tivoli Software . . . . .	71
3-12	Software License Agreement. . . . .	72

3-13	Checking necessary prerequisite software . . . . .	73
3-14	Choose Destination Location . . . . .	74
3-15	User Data Encryption Key . . . . .	75
3-16	Encryption Key . . . . .	75
3-17	Selecting IBM Tivoli Monitoring, V6.1 components . . . . .	76
3-18	Selecting Tivoli Enterprise Monitoring Agents . . . . .	77
3-19	Selecting other IBM Tivoli Monitoring Components. . . . .	78
3-20	Agent Deployment . . . . .	79
3-21	Start Copying Files. . . . .	80
3-22	Setup Type. . . . .	81
3-23	Define TEP Host Information . . . . .	82
3-24	TEPS Data Source Config Parameters - DB2 . . . . .	83
3-25	TEPS configuration completes successfully . . . . .	83
3-26	Warehouse ID and Password for TEP Server . . . . .	84
3-27	TEP Server Configuration . . . . .	85
3-28	TEP Server Configuration . . . . .	85
3-29	Reconfigure warehouse connection information . . . . .	86
3-30	Warehouse Proxy Database Selection . . . . .	86
3-31	Configure DB2 Data Source for Warehouse Proxy . . . . .	87
3-32	Manage Tivoli Enterprise Monitoring Services. . . . .	87
3-33	Tivoli Enterprise Portal presentation files. . . . .	88
3-34	Tivoli Enterprise Monitoring Server Configuration . . . . .	89
3-35	Hub TEMS Configuration . . . . .	89
3-36	TEMS Location . . . . .	90
3-37	Manage Tivoli Enterprise Monitoring Services. . . . .	90
3-38	Select the application support to add to the TEMS . . . . .	90
3-39	Configuration Defaults for Connecting to a TEMS. . . . .	91
3-40	InstallShield Wizard Complete . . . . .	92
3-41	Manage Tivoli Enterprise Monitoring Services. . . . .	93
3-42	The security certificate message . . . . .	94
3-43	Logon window . . . . .	94
3-44	Security Alert . . . . .	95
3-45	Tivoli Enterprise Portal Client Desktop . . . . .	96
3-46	Warehouse Summarization and Pruning Agent configuration . . . . .	97
3-47	Starting Warehouse Summarization and Pruning Agent . . . . .	98
3-48	Welcome Modify, repair, or remove program. . . . .	99
3-49	Information window. . . . .	99
3-50	Selecting Monitoring Agent for Windows OS . . . . .	100
3-51	Selecting the Agents to depot. . . . .	101
3-52	Configure agents default connection to Tivoli Enterprise Monitoring Server . . . . .	102
3-53	Monitoring Agent for Windows OS status . . . . .	103
4-1	Lab architecture or a large scale enterprise scenario-1 . . . . .	108

4-2	Lab architecture for a large scale enterprise scenario-2 . . . . .	109
4-3	License agreement windows . . . . .	118
4-4	Installation windows . . . . .	119
4-5	List of selected components to be installed . . . . .	120
4-6	Agent list for remote deployment . . . . .	121
4-7	Program Folder for the IBM Tivoli Monitoring, V6.1 installation . . . . .	122
4-8	Installation summary details. . . . .	123
4-9	List of components that will be configured . . . . .	124
4-10	Monitoring server configuration window. . . . .	124
4-11	Host and communication protocol configuration window . . . . .	127
4-12	Monitoring server start confirmation windows . . . . .	128
4-13	Application support to be added to TEMS . . . . .	128
4-14	Application addition support window . . . . .	129
4-15	Communication protocol configuration to a TEMS. . . . .	130
4-16	IBM Tivoli Monitoring, V6.1 services window . . . . .	130
4-17	Remote TEMS configuration window. . . . .	132
4-18	IBM Tivoli Monitoring, V6.1 Components List . . . . .	137
4-19	TEPS configuration option window . . . . .	138
4-20	Hostname where TEPS will be installed . . . . .	139
4-21	TEPS database configuration . . . . .	140
4-22	TEPS configuration completion window. . . . .	141
4-23	TEPS user configuration . . . . .	142
4-24	Communication protocol window configuration . . . . .	142
4-25	Configuration for connection to the TEMS . . . . .	143
4-26	IBM Tivoli Monitoring, V6.1 welcome installation window . . . . .	151
4-27	IBM Tivoli Monitoring, V6.1 license agreements . . . . .	152
4-28	IBM Tivoli Monitoring, V6.1 requisites information screen . . . . .	153
4-29	IBM Tivoli Monitoring, V6.1 default destination installation directory . . . . .	154
4-30	IBM Tivoli Monitoring, V6.1 encryption key confirmation . . . . .	155
4-31	Monitoring agents to be installed . . . . .	156
4-32	IBM Tivoli Monitoring, V6.1 program folder . . . . .	157
4-33	Installation summary details. . . . .	158
4-34	Configuration option choice . . . . .	159
4-35	Agent communication protocols. . . . .	160
4-36	Agent's TEMS configuration . . . . .	160
4-37	Tivoli monitoring services console. . . . .	161
4-38	Main OS/400 Menu window . . . . .	162
4-39	Primary language OS/400 definition window . . . . .	163
4-40	OS/400 TCP/IP configuration panel. . . . .	164
4-41	Configuring the monitoring agent. . . . .	168
4-42	Monitoring agent configuration window . . . . .	170
4-43	Informational window display . . . . .	181
4-44	Warehouse Proxy agent communication protocol configuration . . . . .	182

4-45	Warehouse Proxy agent Hub TEMS and port configuration . . . . .	183
4-46	ITM Warehouse ODBC configuration confirmation window . . . . .	183
4-47	Database selection for Warehouse Proxy configuration . . . . .	184
4-48	Data source configuration window for the Warehouse Proxy . . . . .	185
4-49	Warehouse configuration status message . . . . .	185
4-50	Warehouse Proxy database configuration completion . . . . .	186
4-51	Configuring the SPA through the monitoring console . . . . .	187
4-52	Configuring the SPA connection protocol . . . . .	188
4-53	Configuring the SPA TEPS and database connection . . . . .	190
4-54	Configuring how data will be collected and pruned . . . . .	191
4-55	Scheduling the d collection and prunization . . . . .	192
4-56	Defining shift periods and vacation settings . . . . .	194
4-57	Configuring additional parameter for SPA . . . . .	195
4-58	Saving the Pruning and Summarization agent configuration . . . . .	196
4-59	SOAP server hub configuration . . . . .	200
4-60	SOAP Web interface configuration test . . . . .	201
4-61	SOAP Response . . . . .	202
4-62	Event synchronization Software License Agreement window . . . . .	203
4-63	Event synchronization configuration fields . . . . .	204
4-64	Event synchronization cache file configuration window . . . . .	206
4-65	Event synchronization Tivoli Enterprise Monitoring Server information	207
4-66	IBM Tivoli Enterprise Console rule base configuration . . . . .	208
4-67	Warehouse Proxy confirmation window configuration . . . . .	215
4-68	Warehouse Proxy Secondary TEMS communication protocol configuration	215
4-69	Warehouse Proxy primary TEMS configuration . . . . .	216
4-70	TEPS configuration window database backup confirmation . . . . .	217
5-1	Tivoli Enterprise Portal desktop application . . . . .	237
5-2	Navigator view . . . . .	239
5-3	Navigator Lowest Level . . . . .	239
5-4	Selecting Memory attribute . . . . .	240
5-5	Save Workspace message . . . . .	241
5-6	Save Workspace As . . . . .	241
5-7	Selecting the workspace . . . . .	242
5-8	Adding a View . . . . .	244
5-9	Assigning a query . . . . .	245
5-10	Click here to assign query . . . . .	246
5-11	Query Editor . . . . .	247
5-12	Create Query . . . . .	248
5-13	Selecting attributes . . . . .	249
5-14	New query . . . . .	250
5-15	Query Editor Specification . . . . .	251
5-16	Advance Options . . . . .	252

5-17	Filter Service Name . . . . .	253
5-18	New view - Service Status Stopped . . . . .	254
5-19	Service stopped . . . . .	255
5-20	Disk Space Chart Pie view . . . . .	256
5-21	Select Features . . . . .	257
5-22	Setup Type. . . . .	258
5-23	Select the application support to add to the TEMS . . . . .	259
5-24	Application support addition complete . . . . .	259
5-25	Monitoring Agent for DB2 Template. . . . .	260
5-26	Enter DB2 instance name . . . . .	260
5-27	Monitoring Agent for DB2 instance DB2 . . . . .	261
5-28	Change Startup . . . . .	262
5-29	Service Startup for Monitoring Agent for DB2 . . . . .	263
5-30	Service Log On Change. . . . .	263
5-31	Navigator update pending . . . . .	264
5-32	New agent add to Navigator . . . . .	264
5-33	Notepad view . . . . .	265
5-34	Selecting Filters . . . . .	266
5-35	DB2 Info view . . . . .	267
5-36	Filters . . . . .	268
5-37	Thresholds values . . . . .	268
5-38	Thresholds . . . . .	269
5-39	Create Situation . . . . .	271
5-40	Select condition . . . . .	272
5-41	Process Name . . . . .	272
5-42	Distribution Tab . . . . .	273
5-43	Situation Event Console triggered. . . . .	274
5-44	Edit Workflow . . . . .	276
5-45	NT_Process_Memory - Grapher View . . . . .	277
5-46	Change Policy Distribution. . . . .	278
5-47	Workflow Editor - application_test . . . . .	279
5-48	Wait until situation is True components. . . . .	280
5-49	Actions Settings . . . . .	281
5-50	application_test . . . . .	282
5-51	Historical Collection Configuration . . . . .	284
5-52	Groups collecting data . . . . .	285
5-53	Select the Time Span. . . . .	289
5-54	Disk Space Historical Data . . . . .	290



# Tables

2-1	Default port usage for IBM Tivoli Monitoring, V6.1 . . . . .	40
2-2	Extensive metrics. . . . .	52
4-1	Lab hardware and software configuration . . . . .	107
4-2	Installation steps . . . . .	110
4-3	Scenario-1 lab TEMS description . . . . .	113
4-4	Scenario-2 lab TEMS description . . . . .	113
4-5	Communications protocol description . . . . .	125
4-6	Steps for installing a Remote TEMS . . . . .	134
4-7	Commands owned by QSYS with *PUBLIC *CHANGE. . . . .	169
4-8	TEC Event Synchronization installation and configuration steps. . . . .	197
4-9	SOAP configuration steps . . . . .	198
4-10	BM Tivoli Enterprise Console Event Synchronization configuration fields. . . . .	204
4-11	IBM TEC Event Synchronization caches file configuration fields description . . . . .	206
4-12	How to install IBM Tivoli Monitoring, V6.1 components in scenario 2 . . . . .	225





# Examples

2-1	IBM Tivoli Monitoring, V6.1 algorithm to calculate listening port . . . . .	41
2-2	Example for KDC_FAMILIES=IP.PIPE COUNT . . . . .	42
3-1	Readme.txt. . . . .	92
4-1	Output of ./install.sh . . . . .	144
4-2	Output of ./install.sh . . . . .	144
4-3	Output of ./install.sh . . . . .	145
4-4	Post TEMA installation procedure . . . . .	148
4-5	Post TEMA installation procedure . . . . .	148
4-6	Output ./cinfo command. . . . .	149
4-7	Post TEMA installation procedure . . . . .	149
4-8	Deploying the agent on the targeted server. . . . .	172
4-9	Deploying an application agent . . . . .	173
4-10	Selecting install options . . . . .	176
4-11	List of products. . . . .	176
4-12	Installation complete message. . . . .	177
4-13	TEP desktop configuration. . . . .	177
4-14	./itmcmd config -S -t HUB_MADRID output . . . . .	213
4-15	Entering communication protocol and the port . . . . .	214
4-16	Select one of the following prompt. . . . .	218
4-17	Software Licensing Agreement . . . . .	218
4-18	Preparing to install the Global Security Kit message. . . . .	219
4-19	List of available OS for IBM Tivoli Monitoring, V6.1 installation. . . . .	220
4-20	Option list . . . . .	220
4-21	itmcmd config output . . . . .	221
4-22	Entering a secondary protocol . . . . .	222
4-23	KDC_PARTITION question . . . . .	223
4-24	Uninstalling the environment on UNIX. . . . .	230



# 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.*

*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 may 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.

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.

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 illustrates 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.

## Trademarks

The following terms are trademarks of the International Business Machines Corporation in the United States, other countries, or both:

@server®

@server®

Redbooks (logo) ™

iSeries™

i5/OS™

z/OS®

zSeries®

AIX®

AS/400®

Candle®

DB2®

IBM®

NetView®

OMEGAMON®

OS/400®

Redbooks™

Tivoli Enterprise™

Tivoli Enterprise Console®

Tivoli®

WebSphere®

The following terms are trademarks of other companies:

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

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

Intel, Xeon, Intel logo, Intel Inside logo, and Intel Centrino logo are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States, other countries, or both.

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

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

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

# Preface

The IBM® Tivoli® Monitoring Version 6.1 solution is the next generation of the IBM Tivoli family of products that help monitor and manage critical hardware and software in distributed environments. IBM Tivoli Monitoring, V6.1 has been emerged from the best of the IBM Tivoli Monitoring V5 and OMEGAMON® technologies. Integration of these great products, gives us a unique and comprehensive solution to monitor and manage both z/OS® and distributed environments.

IBM Tivoli Monitoring, V6.1 is easily customizable and provides real-time and historical data which allows you to quickly diagnose and solve issues with the new GUI via the IBM Tivoli Enterprise™ Portal component. This common, flexible and easy-to-use browser interface helps users to quickly isolate and resolve potential performance problems.

This redbook focuses on the planning and deployment of IBM Tivoli Monitoring Version 6.1 in small to medium and large environments. I

The target audience for this redbook is IT Specialists, who will be working on new IBM Tivoli Monitoring, V6.1 installations.

## The team that wrote this redbook

This redbook was produced by a team of specialists from around the world working at the International Technical Support Organization, Austin Center.

**Vasfi Gucer** is an IBM Certified Consultant IT Specialist at the ITSO Austin Center. He has been with IBM Turkey for 10 years, and has worked at the ITSO since January 1999. He has more than 13 years of experience in teaching and implementing systems management, networking hardware, and distributed platform software. He has worked on various Tivoli customer projects as a Systems Architect and Consultant. Vasfi is also a Certified Tivoli Consultant.

**Ana Godoy** has been working for IBM Brasil since 1996. She started working with hardware support for PC Company, worked two years as technical support, then become Leader of Product Support for products as Aptiva, ThinkPad and ViaVoice. In January 2002, she joined the Tivoli Support group in Brazil, specializing in Tivoli Management Framework, Remote Control and Tivoli Workload Scheduler. Currently, she is working as a Tivoli Support Specialist for

Distributing Monitoring, IBM Tivoli Monitoring, Tivoli Data Warehouse and the new IBM Tivoli Monitoring, V6.1 products.

Thanks to the following people for their contributions to this project:

Editor's name

International Technical Support Organization, Austin Center

Elizabeth Purzer

IBM USA

We also extend our thanks to the authors and all contributors of the *Getting started with IBM Tivoli Monitoring Version 6.1 on Distributed environments*, SG24-7143 redbook.

## Become a published author

Join us for a two- to six-week residency program! Help write an IBM Redbook dealing with specific products or solutions, while getting hands-on experience with leading-edge technologies. You'll team with IBM technical professionals, Business Partners and/or customers.

Your efforts will help increase product acceptance and customer satisfaction. As a bonus, you'll develop a network of contacts in IBM development labs, and increase your productivity and marketability.

Find out more about the residency program, browse the residency index, and apply online at:

[ibm.com/redbooks/residencies.html](http://ibm.com/redbooks/residencies.html)

## Comments welcome

Your comments are important to us!

We want our Redbooks™ to be as helpful as possible. Send us your comments about this or other Redbooks in one of the following ways:

- ▶ Use the online **Contact us** review redbook form found at:

[ibm.com/redbooks](http://ibm.com/redbooks)

- ▶ Send your comments in an email to:

[redbook@us.ibm.com](mailto:redbook@us.ibm.com)

- ▶ Mail your comments to:

IBM Corporation, International Technical Support Organization  
Dept. JN9B Building 905  
11501 Burnet Road  
Austin, Texas 78758-3493







# Introduction

This chapter provides an introduction to the concepts and components behind IBM Tivoli Monitoring, V6.1. If you are new to IBM Tivoli Monitoring, V6.1, you can also refer to *IBM Tivoli Monitoring, Version 6.1.0. Quick Start Guide*, SC32-1802, that provides concise information about the product.

This chapter has the following sections:

- ▶ “Enterprise management challenges” on page 2
- ▶ “IBM Tivoli Monitoring solutions” on page 3
- ▶ “What’s new for OMEGAMON XE/DE clients?” on page 7
- ▶ “What’s new for Distributed Monitoring, V3.7 clients?” on page 7
- ▶ “IBM Tivoli Monitoring, V6.1 value proposition” on page 7
- ▶ “IBM Tivoli Monitoring, V6.1 components” on page 9
- ▶ “What is new in the IBM Tivoli Data Warehouse, V2.1?” on page 13

## 1.1 Enterprise management challenges

Many readers will be familiar with the challenges faced by IT departments and IT support teams. The nature of ever-changing business demands and market dynamics very often put strains on IT resources, and we are constantly told to “do more, with less”.

The reality we are facing today includes situations where problems occur in systems and the environment well before we are notified, causing IT staff to operate in a reactive, and “fire-fighting” mode. In some environments, the fires seem to get bigger as the pressure, tight deadlines and high profile of business solutions shadows the need to plan an effective systems management solution.

Traditional Enterprise Management needs to change, as the modus operandi tends to include most if not all of the following:

- ▶ Reactive not proactive.
- ▶ Resources may be healthy while customer service levels are not acceptable.
- ▶ Events describe problems, not corrective actions.
- ▶ Events flow into the Operations Room at an incredibly high rate and “event storms” have performance impact on systems.
- ▶ Fixes are typically manual and inefficient.
- ▶ Can't prioritize problems because impacts are unknown.
- ▶ Can't detect most problems: Over 50% of all problems are reported through the helpdesk.
- ▶ Organizational boundaries breed incompatible tools, making end-to-end management and integration very difficult.
- ▶ Lack of vision and strategic direction increases costs.

### 1.1.1 Business driving forces

It can be noted that there are some key business driving forces behind an effective enterprise management, one being the need to improve the quality of service delivery and reduce the resources required to implement and use new information technologies. In addition the following factors must be taken into account when planning and defining the vision of enterprise management.

- ▶ The need to increase revenues, reduce costs, and compete more effectively.
- ▶ Companies need to deploy informational applications rapidly, and provide business users with easy and fast access to business information that reflects the rapidly changing business environment. Enterprise Management solutions must be transparent to the business solutions being delivered, and

they must be proactive to detect, resolve, and escalate potential issues which may impact the business service being delivered.

- ▶ The need to manage and model the complexity of today's business environment.
- ▶ Corporate mergers and deregulation means that companies today are providing and supporting a wider range of products and services to a broader and more diverse audience than ever before. Understanding and managing such a complex business environment and maximizing business investment is becoming increasingly more difficult. Enterprise management systems provide more than just basic monitoring mechanisms, they also offer sophisticated issue detection, event correlation, and application and transaction discovery and performance management tools that are designed to handle and process the complex business information associated with today's business environment.
- ▶ The need to reduce IT costs and leverage existing corporate business information.
- ▶ The investment in IT systems today is usually a significant percentage of corporate expenses, and there is a need not only to reduce this overhead, but also to gain the maximum business benefits from the information managed by IT systems. New information technologies like corporate intranets, thin-client computing, and subscription-driven information delivery help reduce the cost of deploying business intelligence systems to a wider user audience, especially information consumers like executives and business managers. Maintaining the maximum uptime of these systems is becoming more and more critical.

## 1.2 IBM Tivoli Monitoring solutions

IBM Tivoli Monitoring solutions provide a means to manage distributed resources through centralized control and configuration, and for many years IBM Tivoli has been a market leader in Enterprise Monitoring solutions. IBM Tivoli Monitoring has been the backbone for availability monitoring across operating systems and application components.

Breadth of Monitoring to support IT Environment						
Platforms	Databases	Applications	Business Integration	Web Infrastructure	Messaging & Collaboration	Best Practice Library
Unix	DB2	SAP mysap.com	CICS	WebSphere		40+ Custom Packages available
Windows Cluster(s)	Oracle	.NET	Web Services	IIS	Lotus Domino	Examples: Cisco Works S1 Tuxedo etc . .
Linux	SQL	Citrix	IMS	iPlanet		
Z/OS	Sybase	Siebel Tuxedo	WebSphere MQ	Apache	Exchange	
VMWare	Informix		WebSphere MQ Integrator	WebLogic		
OS/400						
IBM Tivoli Monitoring Engine						

Figure 1-1 IBM Tivoli Monitoring solutions

IBM Tivoli Monitoring solutions provides a solid foundation for the development of management solutions addressing the complex needs of today's IT infrastructures. A set of modules built on top of IBM Tivoli Monitoring provide a comprehensive set of solutions for companies facing the challenge of monitoring composite application infrastructures. These modules are delivered through a set of offerings that include:

- ▶ IBM Tivoli Monitoring for Applications
- ▶ IBM Tivoli Monitoring for Business Integration
- ▶ IBM Tivoli Monitoring for Databases
- ▶ IBM Tivoli Monitoring for Messaging and Collaboration

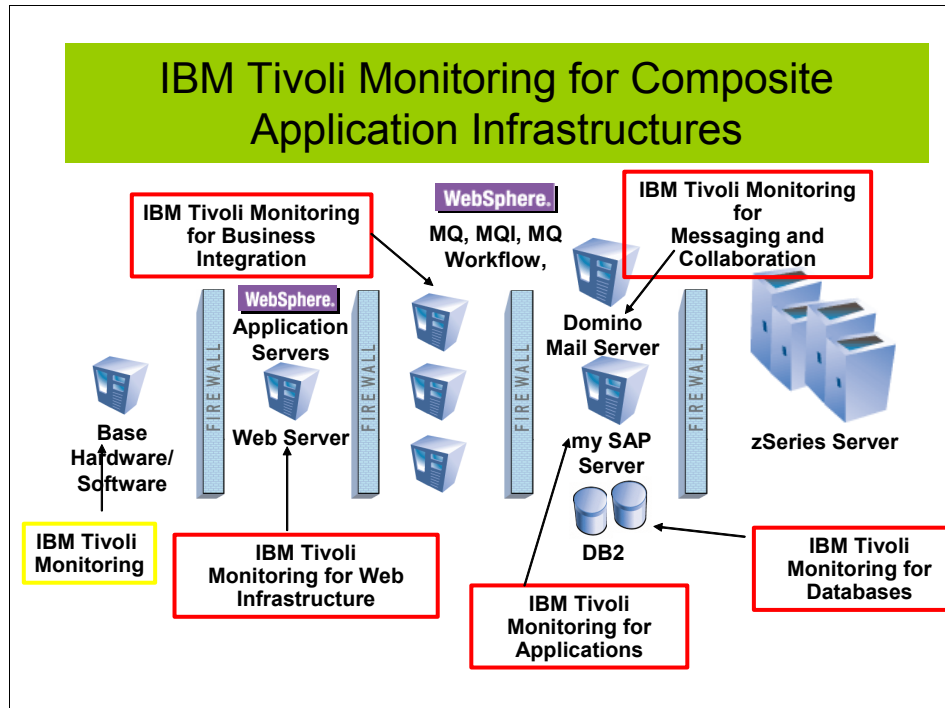


Figure 1-2 Monitoring composite application infrastructures

The latest generation of IBM Tivoli Monitoring solutions have service oriented themes, and are now focused on:

- ▶ Consolidating monitoring platforms.
- ▶ Ensuring customers can take advantage of and realize the return on their monitoring investments.
- ▶ Improving visualization and analysis of monitoring data.
- ▶ Improving management of monitoring environment.
- ▶ Simplifying the installation, configuration, and deployment of the solutions with a simplified User Interface.
- ▶ Improving the integration of Tivoli products.
- ▶ Elevating the value of products through process integration.

## 1.3 What's new for IBM Tivoli Monitoring, V5.x clients?

IBM Tivoli Monitoring, V6.1 maintains many of the components of IBM Tivoli Monitoring, V5.x, such as integration with the Common Information Model (CIM) and Windows® Management Instrumentation (WMI), and the powerful and extremely customizable resource model based monitoring. Highlights of IBM Tivoli Monitoring, V6.1 are:

- ▶ Clients can adopt some or all of IBM Tivoli Monitoring, V6.1 component.
- ▶ The new Integrated Portal (Tivoli Enterprise Portal) provides the user interface for IBM Tivoli Monitoring, V6.1, and integrating applications replaces the Web Health Console and provides a single management and operational view into the enterprise infrastructure. This portal provides tremendous value and is integral to the enterprise monitoring solution. Some of its features are:
  - Improves usability and visualization.
  - Provides Integrated Administration and Runtime Portal.
  - Authorization control for systems, applications, functions, and geographical views.
  - Views which can easily be customized and linked together for efficient use by a specific audience.
  - Easy administration of management rules.
- ▶ All IBM Tivoli Monitoring, V5.1 configurations remain supported.
- ▶ Ability to integrate data coming from various sources such as IBM Tivoli Monitoring 5, OMEGAMON, OMEGAMON Z, IBM Tivoli Enterprise Console®, and IBM Tivoli Data Warehouse.
- ▶ Enhanced process control with a single console for incident and problem management supporting custom workflow (through linking and custom workspace).
- ▶ Deep performance based data and granular information.
- ▶ Granular historical data providing.
  - Trending with the Data Warehouse.
  - Forensic data for problem reconstruction.
  - Simplified schema for easier manipulation and extraction of data.
- ▶ Web Services (SOAP) interface to access real time and historical information.

IBM Tivoli Monitoring, V5.x and IBM Tivoli Monitoring, V6.1 coexistence is covered in detail in

## 1.4 What's new for OMEGAMON XE/DE clients?

OMEGAMON clients will gain many enhancements and new features such as:

- ▶ Additional resources can now be managed, such as Citrix and .NET support.
- ▶ More agents and more agent deployment support.
- ▶ There is now deployment support in the following areas:
  - Centralized agent deployment capabilities.
  - Enhanced internal infrastructure management.
  - Integration with Tivoli Management Framework environment.
- ▶ Command line interface support & Web Services interface.
- ▶ Increased scalability.
- ▶ Enhanced integration with Tivoli products such as:
  - IBM Tivoli Enterprise Console
  - IBM Tivoli Monitoring V5.1
- ▶ Enhanced Data Warehousing such as Aggregation and Pruning controls to manage the Tivoli Data Warehouse, which replaces the Candle® Data Warehouse.

## 1.5 What's new for Distributed Monitoring, V3.7 clients?

Customers who are still using Distributing Monitoring, V3.7, now have the opportunity to upgrade to a modern Monitoring console, warehouse and monitoring infrastructure.

The upgrade procedure will provide the following benefits:

- ▶ Automated programmatic upgrade to IBM Tivoli Monitoring, V6.1.
- ▶ The new visualization interfaces, ease of use and the new Data Warehouse.
- ▶ The IBM Supported upgrade procedures to bring your modules forward.

## 1.6 IBM Tivoli Monitoring, V6.1 value proposition

IBM Tivoli Monitoring, V6.1 continues the paradigm of enterprise resource monitoring and this release has a number of important themes, as shown in Figure 1-3.

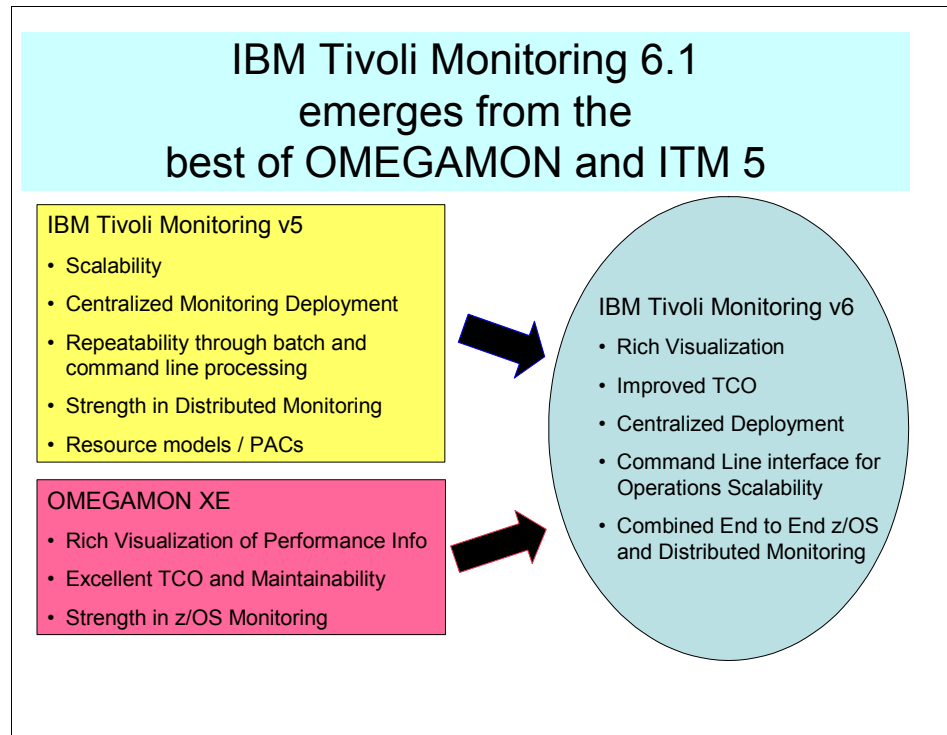


Figure 1-3 IBM Tivoli Monitoring, V6.1 emerges from the best of OMEGAMON and ITM 5

The combination of two best of breed solutions - OMEGAMON and IBM Tivoli Monitoring 5.x has resulted in IBM Tivoli Monitoring, V6.1. The key themes in this release are namely:

- ▶ An easy to use solution:
  - Flexible interface for personalizing information.
  - Integration of event management, real-time and historical analysis.
- ▶ Visualization of information:
  - Robust real time and historical reports.
  - Focus on availability and performance.
  - Monitoring infrastructure visibility.
- ▶ Reduce Total Cost of Ownership:
  - Simple agent and management rule deployment.
  - Light weight agents.
  - Support for new technology (Clusters, Virtualization).



- ▶ Integration of products and processes:
  - Enterprise view for Distributed and zSeries®.
  - Integrated view of existing monitoring, new monitoring, and IBM Tivoli Enterprise Console (ITEC).
  - Added focus of the IT Infrastructure Library, ITIL (), which is a series of documents that are used to aid the implementation of a framework for IT Service Management (ITSM). This framework defines how Service Management is applied within specific organizations, and is completely customizable for application within any type of business or organization that has a reliance on IT infrastructure.

## 1.7 IBM Tivoli Monitoring, V6.1 components

IBM Tivoli Monitoring, V6.1 (ITM) has been designed to provide access to information which is crucial to daily operations. This information related to the availability and performance for components, applications and services within your enterprise infrastructure.

The various components which provide the technology for this information will now be introduced:

### **Tivoli Monitoring Services**

Tivoli Monitoring Services is the framework for IBM Tivoli Monitoring, V6.1 and comprises all components as well as describes how they interact. Those components include but are not limited to:

- ▶ TEMA - Tivoli Enterprise Monitoring Agent
- ▶ TEMS - Tivoli Enterprise Monitoring Server
- ▶ TEPS - Tivoli Enterprise Portal Server
- ▶ TEP - Tivoli Enterprise Portal

Figure 1-4 on page 10 shown the IBM Tivoli Monitoring components.

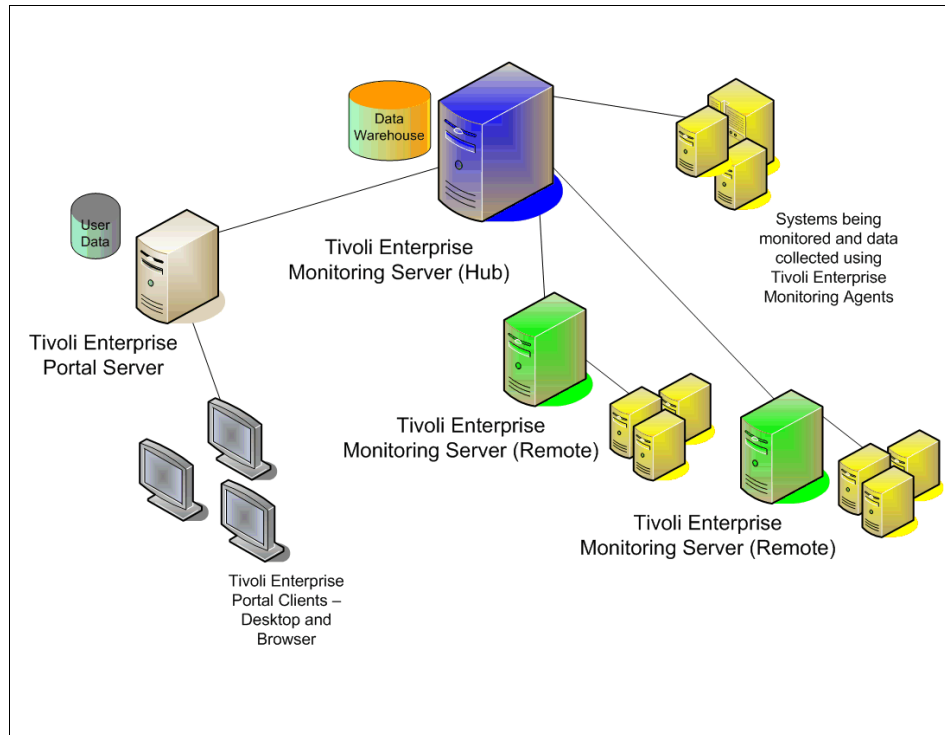


Figure 1-4 BM Tivoli Monitoring 6.1 components

## TEMA - Tivoli Enterprise Monitoring Agent

The Tivoli Enterprise Monitoring Agents are data collectors within your monitoring solution, and are installed to gather data from one or more systems which you need to monitor. The data which is collected is sent to a central repository called the Tivoli EA management agent collects information about the attributes of a particular managed system. Examples of agents are:

- ▶ Operating System Agent.
- ▶ Universal Agent - The Tivoli Universal Agent is a monitoring agent you can configure to monitor any data you collect. It lets you integrate data from virtually any platform and any source, such as custom applications, databases, systems, and subsystems.
- ▶ Application Agents - These collect data from databases, WebSphere® Application Server, WebSphere MQ, etc...

At the GA time the following Operating System Agents will be supported:

- ▶ AIX® 5.1, 5.2, 5.3

- ▶ Solaris™ 8, 9, 10
- ▶ HP UX 11i, 11.23
- ▶ Windows 2000 Server, Advanced Server
- ▶ Windows XP Pro
- ▶ Windows 2003 Server 32 bit (SE & EE)
- ▶ OS/400® 5.2, 5.3
- ▶ RHEL 2.1
- ▶ RHEL 3 (Intel®, zSeries)
- ▶ RHEL 4 (Intel, AMD64/EM46T, zSeries)
- ▶ SLES 8 (Intel, zSeries)
- ▶ SLES 9 (Intel, zSeries)

**Note:** Windows 2003 Server 64 bit platform will be supported post GA as a Fix Pack.

## **TEMS - Tivoli Enterprise Monitoring Server**

The Tivoli Enterprise Monitoring Server is the central repository of data which comes from the Tivoli Enterprise Monitoring Agents.

It particularly stores the definitions for conditions that indicate a problem with a particular resource, and also controls the security for your monitoring solution.

Each enterprise monitoring solution must contain one Hub TEMS, and can include multiple Remote TEMSs, which are used to provide scalability in large installations.

At the GA time, the following platforms will be supported for TEMS:

- ▶ AIX 5.2, 5.3
- ▶ Solaris 9, 10
- ▶ Windows 2000 Server, Advanced Server
- ▶ Windows XP Pro (Demo only)
- ▶ Windows 2003 Server 32 bit (SE & EE)
- ▶ RHEL 4 (Intel, zSeries)
- ▶ SLES 9 (Intel, zSeries)

## TEPS - Tivoli Enterprise Portal Server

The Tivoli Enterprise Portal Server functions as a repository for all user data, such as the user IDs and user access control for the monitoring data, meaning what data each user will be able to access and how it is displayed.

The TEPS connects to the Hub TEMS and provides a consistent look and feel for the users. The database to store TEP server information can be:

- ▶ MS SQL Server 2000
- ▶ IBM UDB 8.1
- ▶ IBM UDB 8.2

At the GA time, the following platforms will be supported for TEPS:

- ▶ Windows 2000 Server, Advanced Server
- ▶ Windows XP Pro
- ▶ Windows 2003 Server 32 bit (SE & EE)
- ▶ RHEL 4 (Intel, zSeries)
- ▶ SLES 9 (Intel, zSeries)

**Note:** Windows XP Pro is supported for demo purposes only.

## TEP - Tivoli Enterprise Portal

The Tivoli Enterprise Portal (TEP) is the consolidated user interface for IBM Tivoli Monitoring, and is used to connect to the Tivoli Enterprise Portal Server.

The Tivoli Enterprise Portal can be launched from an Internet Explorer browser, or can be installed as a client application on a workstation.

**Important:** Internet Explorer is the only browser supported for TEP.

At the GA time, the following platforms will be supported for TEP:

- ▶ Windows 2000 Pro
- ▶ Windows 2000 Server, Advanced Server
- ▶ Windows XP Pro
- ▶ Windows 2003 Server 32 bit (SE & EE)
- ▶ RHEL 4 (Intel)
- ▶ SLES 9 (Intel)

Figure 1-5 on page 13 shows the Tivoli Enterprise Portal (browser mode).

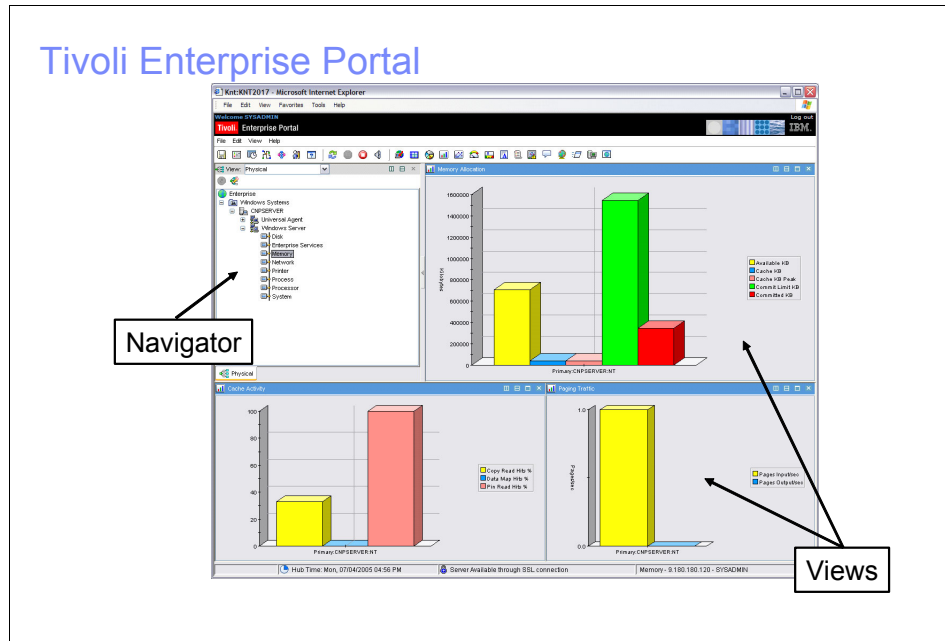


Figure 1-5 Tivoli Enterprise Portal

## 1.8 What is new in the IBM Tivoli Data Warehouse, V2.1?

A summary of the features provided in the IBM Tivoli Data Warehouse, V2.1 are:

- ▶ Step 1 of the Extract, Transform and Load (ETL) procedure is no longer required.
- ▶ The data is no longer aggregated before it is loaded into the data warehouse.
- ▶ Crystal Enterprise is no longer needed.
- ▶ There are no more data marts.
- ▶ The various data collectors have a common core, and application specific plugins.
- ▶ The historical and real time data have the ability to aggregate/prune, cross correlate and hold process/business views.
- ▶ The Tivoli Enterprise Portal has the ability to display real time and historical data and various chart forms.

In summary, the Tivoli Data Warehouse is more consumable than ever before.





# Architecture and planning

This chapter explains the IBM Tivoli Monitoring, V6.1 architecture and how each component operates within an IBM Tivoli Monitoring installation. We explore four architectural designs for IBM Tivoli Monitoring, V6.1 using scenarios based on several factors: number of agents, hardware availability, and network restrictions. There is an overview section covering IBM Tivoli Monitoring, V6.1 agent deployment using several unique strategies. Lastly, there is a tips and hints section discussing design/implementation strategies which compliments the official IBM Tivoli Monitoring, V6.1 product manuals.

This chapter discusses the following:

- ▶ “IBM Tivoli Monitoring, V6.1 components” on page 16
- ▶ “IBM Tivoli Monitoring, V6.1 deployment scenarios” on page 24
- ▶ “Scalability” on page 50
- ▶ “Agent deployment architecture” on page 53

## 2.1 IBM Tivoli Monitoring, V6.1 components

An IBM Tivoli Monitoring, V6.1 installation consists of various components collectively labeled the Tivoli Monitoring Services framework. This framework is a combination of several vital components. Additionally, optional components can be installed which extend the monitoring functionality of this framework. For platform support details for all the major IBM Tivoli Monitoring, V6.1 components, please refer to “Platform Support Matrix - IBM Tivoli Monitoring, V6.1 (GA)” on page 22.

Figure 2-1 on page 16 shows the IBM Tivoli Monitoring, V6.1 component model.

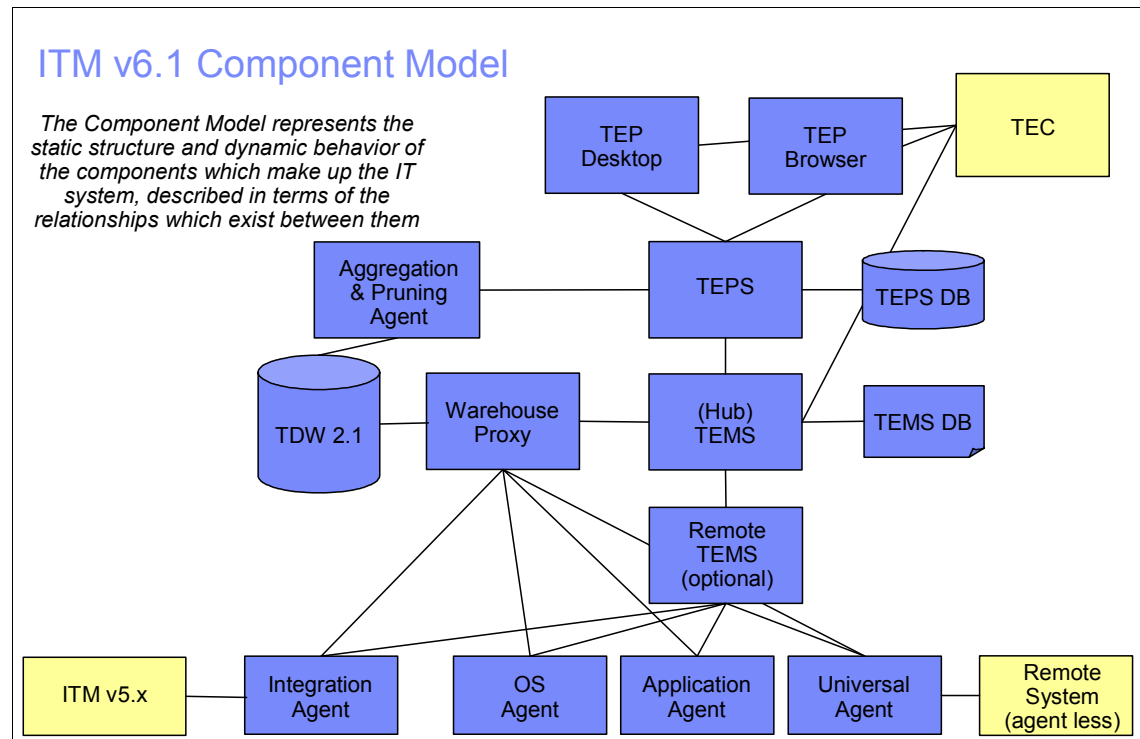


Figure 2-1 IBM Tivoli Monitoring, V6.1 component model

Every IBM Tivoli Monitoring, V6.1 installation requires the following components:

- Tivoli Enterprise Monitoring Server (TEMS)

The TEMS (referred to as the *monitoring server*) is the initial component to install which begins building the IBM Tivoli Monitoring Services foundation. It is the key component on which all other architectural components depend on



directly. The TEMS acts as a collection and control point for alerts received from agents, and collects their performance and availability data.

The TEMS is responsible for tracking the heartbeat request interval for all the Tivoli Enterprise Management Agents connected to it.

The TEMS stores, initiates, and tracks all situations and policies. The TEMS is the central repository for storing all active conditions and short term data on every Tivoli Enterprise Management Agent. Additionally, the TEMS is responsible to initiate and track all generated actions that invoke a script/program on the Tivoli Enterprise Management Agent.

The TEMS storage repository is a proprietary database format (referred to as the *Enterprise Information Base - EIB*) grouped as a collection of files located on the TEMS.

These files start with a filename prefix qa1 and located in:

<installation\_dir/tables/<tems\_name>

<installation\_dir>: IBM Tivoli Monitoring, V6.1 home directory

<tems\_name>: Tivoli Enterprise Monitoring Server name

**Note:** <tems\_name> is the monitoring server name, not necessary the TEMS hostname.

The primary TEMS is configured as a Hub(\**LOCAL*). All IBM Tivoli Monitoring, V6.1 installations require at least one TEMS configured as a Hub. Additional Remote(\**REMOTE*) TEMS can be installed afterwards to introduce a scalable hierarchy into the architecture.

This Hub/Remote interconnection provides a hierarchical design allowing the Remote TEMS to control/collect its individual agent status and propagate the agent status up to the Hub TEMS. This mechanism allows the Hub TEMS to maintain an infrastructure wide visibility of the entire environment. This visibility get passed to the Tivoli Enterprise Portal Server for pre-formatting, ultimately displaying within the Tivoli Enterprise Portal client.

When security validation is configured, the Hub TEMS is the monitoring server to manage operating system level userids.

► Tivoli Enterprise Portal Server (TEPS)

The TEPS (referred to as the *portal server*) is a repository for all graphical presentation of monitoring data. The portal server database also consists of all the userids and user access controls for the monitoring workspaces. The TEPS provides the core presentation layer which allows for retrieval, manipulation, analysis, and pre-formatting of data. It manages this access

through user workspace consoles. The TEPS keeps a persistent connection to the Hub TEMS, and can be considered a logical gateway between the Hub TEMS and the Tivoli Enterprise Portal client. Any disconnection between the two components immediately disables access to the monitoring data used by the Tivoli Enterprise Portal client.

A RDBMS must be installed on the same physical system prior to the TEPS installation. This prerequisite is necessary because the TEPS installation will create the mandatory TEPS database, along with the supporting tables. Additionally, a ODBC (Open Database Connectivity) Data Source Name is configured to connect directly to the Tivoli Data Warehouse RDBMS. This ODBC connection is used whenever a pull of historical data from the Tivoli Data Warehouse is requested.

**Note:** Even though technically valid, implementing a *remote* RDBMS for the TEPS is not recommended. The TEPS is closely coupled to the RDBMS and the complexity of a *remote* RDBMS is difficult to maintain.

When installing the TEPS, a propriety integrated web server is installed for use with the Tivoli Enterprise Portal client in browser mode. Depending on the network topology and possible security implications, this may play a role in constructing the solution. Instead, an external web server installed on the same system as the TEPS can be used. Please refer to the *IBM Tivoli Monitoring, V6.1.0 Installation and Setup Guide*, GC32-9407, chapter 9 for additional details.

In large installations, it is recommended to install multiple TEPS which connect to one single Hub TEMS. See “Large installation - (4000 agents maximum)” on page 30 for further details.

► Tivoli Enterprise Portal (TEP)

The TEP client (referred to as the *portal client*) is a java-based user interface which connects to the TEPS to view all monitoring data collections. It is the user interaction component of the presentation layer. The TEP brings all these views together in a single window so you can see when any component is not working as expected. The client offers two modes of operation: a java desktop client and http browser.

Assuming a default installation, the browser mode TEP client can be found using this URL:

<http://<hostname>:1920///cnp/kdh/lib/cnp.html>

where <hostname> is the hostname of the Tivoli Enterprise Portal Server.

**Important:** IBM Tivoli Monitoring, V6.1 only supports Internet Explorer on the Windows Platform in browser mode.

The following products will have integrated interfaces into TEP:

- OMEGAMON Z
- OMEGAMON Distributed
- IBM Tivoli Monitoring 5.1.2
- IBM Tivoli Monitoring, V6.1
- NetView® for z/OS (release 5.2)
- IBM Tivoli Enterprise Console
- IBM Tivoli Composite Application Manager for Response Time Tracking
- IBM Tivoli Composite Application Manager for WebSphere
- IBM Tivoli Composite Application Manager for SOA

**Note:** In 2006, additional products such as IBM Tivoli Service Level Advisor, System Automation and Tivoli Business System Manager will also be integrated into the Tivoli Enterprise Portal. IBM Tivoli Service Level Advisor integrations will be available with Tivoli Data Warehouse, V2.1.1 version.

► Tivoli Enterprise Management Agent (TEMA)

The agents (referred to as *managed systems*) are installed on the system or subsystem requiring data collection and monitoring. The agents are responsible for data gathering and distribution of attributes to the monitoring servers, including initiating the heartbeat status.

The agents test attribute values against a threshold and report these results back to the monitoring servers. An alert icon is displayed in the TEP when a threshold is exceeded or a value is matched. These tests are called situations.

What prompts the monitoring server to gather data samples from the agents?

- Opening or refreshing a workspace that has data views (table or chart views). When this happens, the TEPS sends a sampling request to the Hub TEMS. The request is passed to the monitoring agent, if there is a direct connection, or through the Remote TEMS to which the monitoring agent connects. The monitoring agent takes a data sampling and returns the results through the monitoring server and portal server to the portal workspace.

- The sampling interval for a situation (a test taken at your monitored systems). The situation can have an interval as often as once per second or as seldom as once every three months. When the interval expires, the monitoring server requests data samples from the agent and compares the returned values with the condition described in the situation. If the values meet the condition, the icons change on the navigation tree.

Optionally, the agents can be configured to transfer data collections directly to the Warehouse Proxy Agent instead of using the Remote TEMS. If firewall restrictions are disabled or minimum, it is recommended to configure all the agents to transfer directly to Warehouse Proxy Agent. Otherwise, firewall security is a key factor in the location of the Warehouse Proxy Agent relative to the firewall zone and agents. Warehousing data through the Remote TEMS is limited and should only be used as a last resort.

Tivoli Enterprise Management Agents are grouped into two categories:

- Operating System (OS) Agents

Operating System Agents retrieve and collect all monitoring attribute groups related to specific operating system management conditions and associated data.

- Application Agents

Application Agents are specialized agents coded to retrieve and collect unique monitoring attribute groups related to one specific application. The monitoring groups are designed around an individual software application and provide in-depth visibility into the status and conditions of that particular application.

The following are examples of common management agents packaged along with IBM Tivoli Monitoring, V6.1:

- Window OS Agent
- Linux® OS Agent
- UNIX® OS Agent
- UNIX Log Agent (also supports logs on Windows Platform)
- i5 OS Agent
- Universal Agent

The Universal Agent is a special agent which leverages a full Application Programming Interface (API) to monitor and collect data for any type of software. Any application that produces data values, the Universal Agent can monitor and retrieve data from it. Essentially, IBM Tivoli Monitoring, V6.1 can now monitor any unique application regardless if the base product supports it.

The following are examples of common optional management agents packaged separately:

- Monitoring Agent for IBM Tivoli Monitoring 5.x Endpoint
- DB2® Agent
- Oracle Agent
- MS SQL Agent
- MS Exchange Agent
- Active Directory Agent

► Warehouse Proxy Agent (WPA)

The Warehouse Proxy Agent is a unique agent that performs only one task. The WPA collects and consolidates all the historical data collections from the individual agents to store in the Tivoli Data Warehouse. If using the Tivoli Data Warehouse, one WPA is required for each IBM Tivoli Monitoring, V6.1 installation. It uses ODBC (Open Database Connectivity) to write the historical data to a supported relational database.

**Restriction:** IBM Tivoli Monitoring, V6.1 currently only supports the WPA under the Windows platform. UNIX operating support for the WPA will be in a post GA release of IBM Tivoli Monitoring, V6.1

► WarehouseSummarization and Pruning agent (S&P)

The Summarization and Pruning agent is a unique agent that performs the aggregation and pruning functions for the historical raw data on the Tivoli Data Warehouse. It has advanced configuration options allowing exceptional customization of the historical data storage.

One S&P is recommended to manage the historical data in the Tivoli Data Warehouse. Due to the tremendous amounts of data processing necessary, it is recommended the S&P be always installed on the same physical system as the Tivoli Data Warehouse repository.

► Tivoli Data Warehouse (TDW)

The Tivoli Data Warehouse is the database storage that contains all the historical data collection. A Warehouse Proxy must be installed, to leverage the TDW function within the environment. In large scale deployments, a Tivoli Data Warehouse can be shared between monitoring installations.

An IBM Tivoli Monitoring, V6.1 installation can contain the following optional components:

► Monitoring Agent for IBM Tivoli Monitoring 5.x Endpoint

Also called IBM Tivoli Monitoring 5.x Endpoint Agent, this integration agent allows the collection and visualization of IBM Tivoli Monitoring 5.x resource models in the Tivoli Enterprise Portal. The visualization is the direct replacement for the Web Health Console. Additionally, the Agent provides roll-up function into the Tivoli Data Warehouse.

► Tivoli Enterprise Console Event Synchronization

The TEC Event Synchronization component sends updates to situation events back to the monitoring server that are forwarded to the event server. Actions performed at the Tivoli Enterprise Console for IBM Tivoli Monitoring, V6.1 situations are reflected in the Tivoli Enterprise Portal Server.

► IBM Tivoli Business Systems Manager (TBSM)

IBM Tivoli Business Systems Manager provides intelligent management software to help businesses increase operational agility by aligning IT operations to business priorities. Intelligent management software helps optimize IT operations according to the business goals of the organization, rather than focusing on the technology itself.

**Note:** IBM will provide a special program called TBSM feed from OMEGAMON (or shortly called the XE Feed) for IBM Tivoli Monitoring, V6.1 and IBM Tivoli Business Systems Manager integration. The XE Feed is planned to be made available as an LA fix to IBM Tivoli Business Systems Manager, V3.1 in 1Q 2006 and then rolled into IBM Tivoli Business Systems Manager, V3.2 release which is scheduled for Sept 2006.

### 2.1.1 Platform Support Matrix - IBM Tivoli Monitoring, V6.1 (GA)

The following table displays the full support matrix for the General Availability (GA) code release of IBM Tivoli Monitoring, V6.1. This table provides a quick overview of platform support, and planned support direction.

**Important:** Always review the latest Release Notes packaged with IBM Tivoli Monitoring, V6.1 to guarantee the latest platform support information.

Supported OS	TEMA	TEMS	TEP	TEPS	Warehouse Proxy	S&P Agent
<b>AIX 5.1</b> (32/64 bit)	A	C	C	C	D	A
<b>AIX 5.2</b> (32/64 bit)	A	A	C	C	D	A
<b>AIX 5.3</b> (32/64 bit)	A	A	C	C	D	A
<b>Sol 8</b> (32/64 bit)	A	C	D	D	D	A
<b>Sol 9</b> (32/64 bit)	A	A	C	C	D	A
<b>Sol 10</b> (32/64 bit)	A	A	C	C	D	A
<b>HP-UX 11i</b> (32/64 bit)	A	C	D	D	D	D
<b>Win 2K Pro</b> (32 bit)	R	R	A	R	D	A
<b>Win 2K Svr with SP 1</b> (32 bit)	A	A	A	A	A	A
<b>Win 2K Adv. Svr with SP 1</b> (32 bit)	A	A	A	A	A	A
<b>Win XP</b> (32 bit)	A	R	A	R	A	A
<b>Win 2003 Svr SE</b> (32 bit)	A	A	A	A	A	A
<b>Win 2003 Svr EE</b> (32 bit)	A	A	A	A	A	A
<b>OS/400 5.2</b>	A	R	R	R	D	R
<b>OS/400 5.3</b>	A	R	R	R	D	R
<b>z/OS 1.4</b>	A	A	R	D	D	
<b>z/OS 1.5</b>	A	A	R	D	D	
<b>z/OS 1.6</b>	A	A	R	D	D	
<b>z/OS 1.7</b>	A	A				
<b>RHEL 2.1 AS/ES Intel</b> (32 bit)	A	R	R	R	D	A
<b>RHEL 2.1 WS Intel</b>	A					A

Figure 2-2 Platform support matrix - IBM Tivoli Monitoring, V6.1

Key:

A – Indicates the platform is supported.

C – Indicates the platform will be certified for support or supported in a maintenance release.

D – Indicates the platform will not be supported in this release, but maybe supported in a later release.

R – Indicates the platform will probably not be supported in any release.

<b>RHEL 3 AS zSeries (31 bit)</b>	A	C	R	C	D	A
<b>RHEL 3 AS zSeries (64 bit)</b>	A	C	C	C		A
<b>RHEL 3 POWER I/P</b>	D	D	D	D	D	D
<b>RHEL 4 AS/ES Intel (32 bit)</b>	A	A	A	A	D	A
<b>RHEL 4 WS Intel (32 bit)</b>	A					A
<b>RHEL 4 AMD64/EM64T</b>	C	C	C	C	D	C
<b>RHEL 4 AS/ES Opteron/Xeon (64 bit)</b>	C					
<b>RHEL 4 WS Opteron/Xeon (64 bit)</b>	C					
<b>RHEL 4 AS zSeries (31 bit)</b>	A	A	R	A	D	A
<b>RHEL 4 AS zSeries (64 bit)</b>	A	C	C	C		A
<b>RHEL 4 i/pSeries</b>	D	D	D	D	D	D
<b>SLES 8 Intel (32 bit)</b>	A	C	C	C	D	A
<b>SLES 8 zSeries (31bit)</b>	A	A	R	A	D	A
<b>SLES 8 zSeries (64 bit)</b>	A	C	R	C	D	A
<b>SLES 8 i/pSeries</b>	D	D	D	D	D	D
<b>SLES 9 Intel (32 bit)</b>	A	A	A	A	D	A
<b>SLES 9 Opteron/Xeon (64 bit)</b>	C					
<b>SLES 9 zSeries (31bit)</b>	A	A	R	A	D	A
<b>SLES 9 zSeries (64 bit)</b>	A	C	R	C	D	A

Figure 2-3 Platform support matrix - IBM Tivoli Monitoring, V6.1 (continued)

**Key:**

A – Indicates the platform is supported.

C – Indicates the platform will be certified for support or supported in a maintenance release.

D – Indicates the platform will not be supported in this release, but maybe supported in a later release.

R – Indicates the platform will probably not be supported in any release.

**Notes:**

- Windows XP Pro is supported for demo purposes only.
- Windows 2003 Server 64 bit platform will be supported post GA as a Fix Pack.

## 2.2 IBM Tivoli Monitoring, V6.1 deployment scenarios

Deployment scenarios attempt to provide a realistic understanding of architecture design. These scenarios should be used for guidance to assist in the actual planning and deployment strategy used for a production installation. It is important to recognize that every deployment strategy is unique, and only proper planning can guarantee a successful implementation.



We will cover 4 types of environments, namely:

- ▶ “Demo installation - (single machine)” on page 27
- ▶ “Small/Medium installation - (400 agents maximum)” on page 28
- ▶ “Large installation - (4000 agents maximum)” on page 30
- ▶ “Huge installation - (greater than 4000 agents)” on page 33

**Note:** Our clasification here is based of number of IBM Tivoli Monitoring, V6.1 agents. In practice, sometimes number of employees is used to define the size of a business; such as companies with up to 1000 employees are considered as small to medium businesses, etc.

Figure 2-4 on page 26 depicts the interconnections of the various components at their simplest. There are other chapters throughout the book explaining the interconnections in further detail. Any limitation with hardware or software is noted in the later chapters.

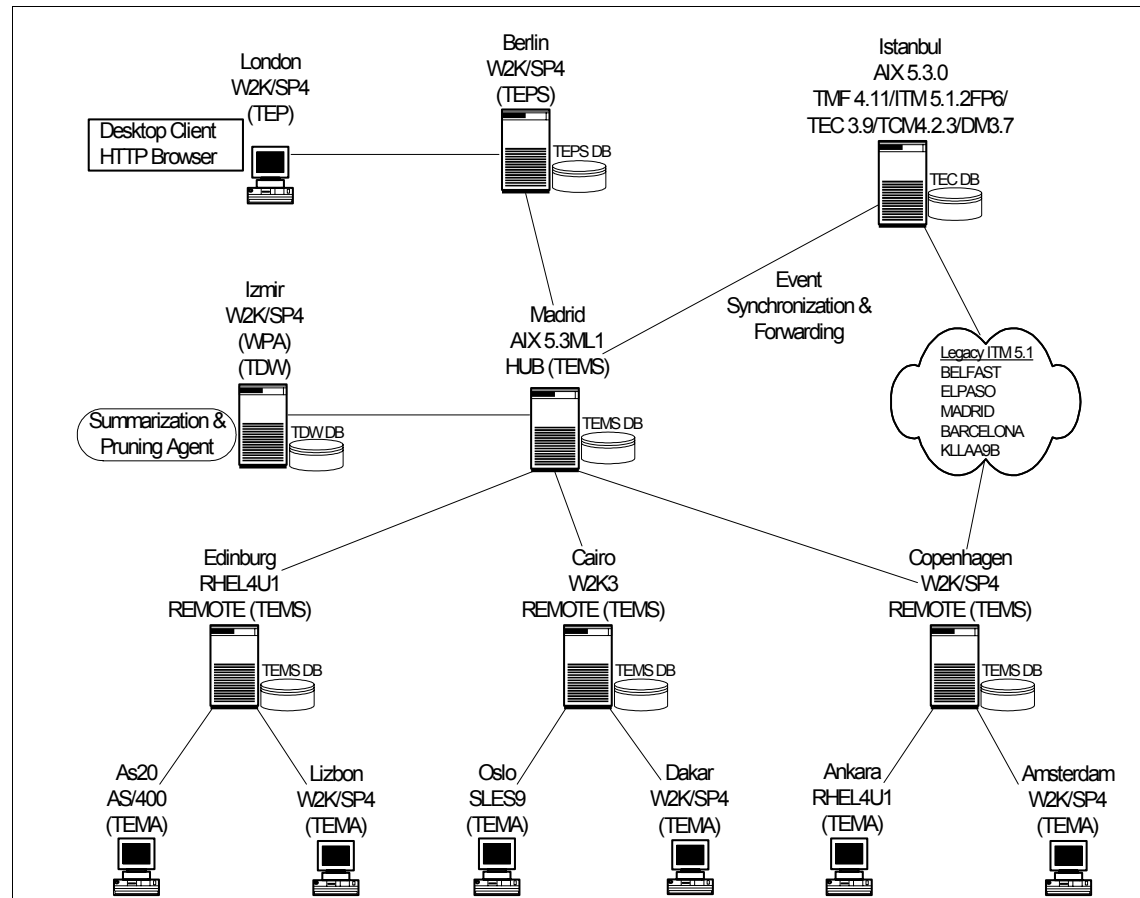


Figure 2-4 IBM Tivoli Monitoring, V6.1, lab topology

#### Notes:

- ▶ The Hot Standby system is Milan (AIX 5.3.0) which is not depicted in the diagram.
- ▶ All the TEMAs contain at least the OS Agent, several have additional agents.

In order to cover various topics throughout the Redbook development, we implemented an IBM Tivoli Monitoring, V6.1 installation which incorporates all relating content. This architecture covers all components which make up an IBM Tivoli Monitoring installation, including the built-in *Hot Standby* Hub Tivoli Enterprise Manager Server. Secondly, a legacy Tivoli Management Framework, V4.1.1 connects to the infrastructure to demonstrate the

interoperability among IBM Tivoli Monitoring, V6.1, IBM Tivoli Monitoring, V5.1.2 Fix Pack 6, IBM Distributed Monitoring, V3.7, and IBM Tivoli Enterprise Console, V3.9. To ensure the accuracy of the implementation and best practices, the environment contains a proportionate selection of heterogeneous hardware configurations with varying degrees of operating system platforms and levels.

We

**Attention:** All the capacity values especially for the Tivoli Enterprise Management Agents are based on approximation. The section headers below provide a recommended maximum number of agents. Also, we include an estimate on the maximum amount of physical systems within the paragraphs, that do not calculate out evenly. All these numbers are based on a proportionate amounts of agents deployed to every system. Actual production installations may vary greatly in agent disbursement.

## 2.2.1 Demo installation - (single machine)

For demonstration purposes, IBM Tivoli Monitoring, V6.1 can be installed onto one single machine running Windows XP. *This IBM Tivoli Monitoring, V6.1 installation should only be used for demonstration, and is not a supported implementation.* Leveraging Windows install shield, IBM Tivoli Monitoring, V6.1 can be installed using the single CD. The minimum required software is the following:

- ▶ Tivoli Enterprise Monitoring Server (TEMS)
- ▶ Tivoli Enterprise Portal Server (TEPS)
- ▶ Tivoli Enterprise Portal Client (TEP)
- ▶ Windows OS Agent

The Tivoli Warehouse Proxy, Tivoli Data Warehouse, Summarization and Pruning agent, and a DB2 installation can be optionally installed on the same system to illustrate the historical data collection features of IBM Tivoli Monitoring, V6.1.

**Note:** IBM Tivoli Monitoring, V6.1 demo (on a single Windows machine) installation will be covered in another Redbook, named *Deployment Guide Series: IBM Tivoli Monitoring V 6.1*, SG24-7188. This Redbook will also cover some proof of concept scenarios. Planned availability of this Redbook is December 2005.

### 2.2.2 Small/Medium installation - (400 agents maximum)

The small/medium installation is the fundamental design utilizing only the minimum required components. This scenario is perfect for prototyping IBM Tivoli Monitoring, V6.1 or using it within a production installation consisting of 400 agents. In fact, IBM Tivoli Monitoring, V6.1 by design excels in superiority for the small/medium installation. The out-of-box monitoring collections, GUI presentation layer, historical data collection, and robustness provide a full monitoring solution with a modest total cost of ownership (TCO).

It is implemented with the minimum hardware requirements necessary for a production IBM Tivoli Monitoring, V6.1 installation.

The installation consists of the following components:

- ▶ Tivoli Enterprise Monitoring Server
- ▶ Tivoli Enterprise Portal Server
- ▶ Tivoli Enterprise Portal
- ▶ Tivoli Warehouse Proxy Agent
- ▶ Tivoli Data Warehouse
- ▶ Summarization and Pruning Agent

Figure 2-5 on page 29 depicts the small/medium topology. The diagram provides an overview of each IBM Tivoli Monitoring, V6.1 connected component. For a comprehensive architecture, the optional Hot Standby node is depicted in this diagram.

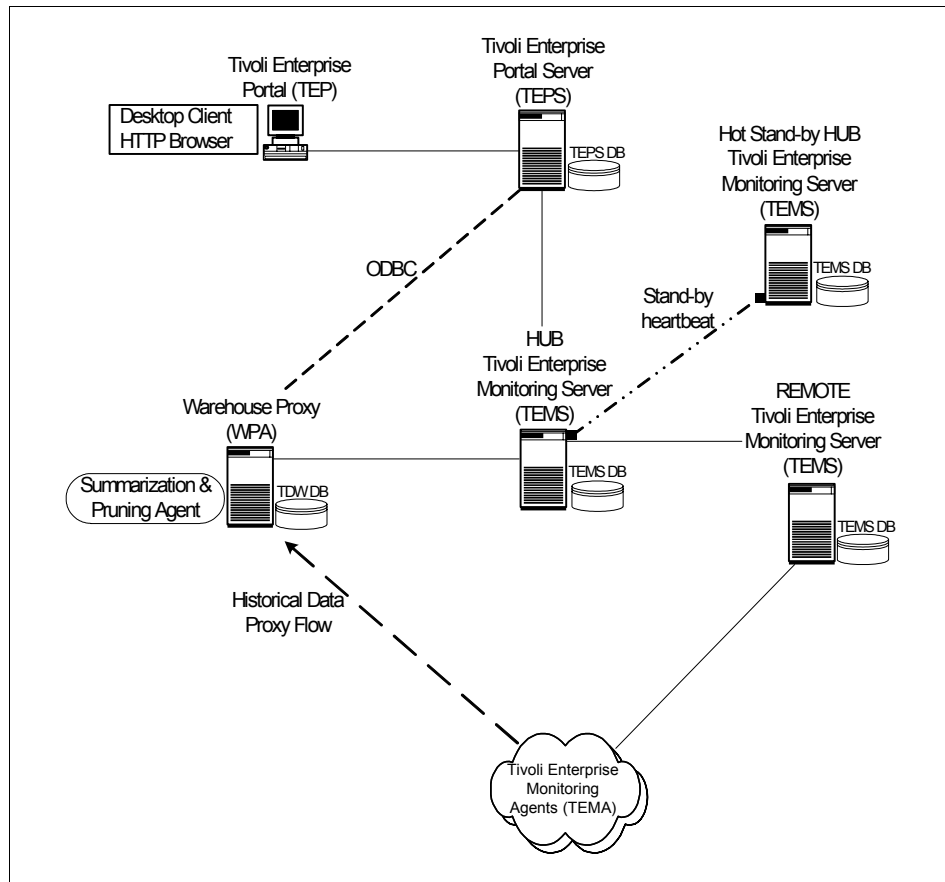


Figure 2-5 IBM Tivoli Monitoring, V6.1, small/medium topology design

We recommend installing at least three TEMS (including the Hot Standby node) in this scenario, even though the small/medium installation allows the use of only one TEMS. Implementing a Hub/Remote architecture in the early stages allows for growth and scalability. Furthermore, this design builds around IBM Tivoli Monitoring, V6.1 built-in fail over capabilities. The small/medium installation supports approximately 250 managed systems. This estimate assumes that each managed systems will have 2 agents each. The actual distribution of agents will not necessary be proportionate in a real installation, but this calculation provides the recommended total amount for one IBM Tivoli Monitoring, V6.1 installation. All the agents will connect to the Remote TEMS, only using the Hub TEMS as a failover monitoring server.

It is recommended to optionally install the Hot Standby node. Nevertheless, the Hot Standby is not required for the small/medium installation, especially if cost

restrictions exist for hardware deployment. The Hot Standby should always be considered though, since it offers failure protection with minimum increase in total cost of ownership.

**Attention:** A small/medium installation can not use a Remote TEMS as a Hot Standby node. Hot Standby nodes need to be configured as \*LOCAL always.

It is permitted to use the Hub TEMS to handle agent tasks directly. However, we do not recommend using the Hub TEMS for this purpose. The Hub TEMS should focus on data collecting/processing tasks between the TEMS and itself. If the environment expands, additional Remote TEMS should be installed to process the additional agent requirement. Additional agent deployments increases processing requirements for the Hub TEMS, which can degrade if the Hub is allowed to handle agent tasks directly.

For an average Tivoli Data Warehouse installation within a small/medium installation, it should be sufficient to have the Warehouse Proxy Agent and the Tivoli Data Warehouse repository on the same system. This installation provides historical data collection without the additional hardware. It is still a wise decision to monitor the Tivoli Data Warehouse post installation to ensure processing rate is on target.

### 2.2.3 Large installation - (4000 agents maximum)

The large installation builds upon the fundamentals of the small/medium installation. This design focuses on scalability. This Tivoli Monitoring environment consists of 4000 agents within a single Tivoli Monitoring installation. It requires the recommended hardware specification or higher to properly scale the infrastructure.

The installation consists of the following components:

- ▶ Tivoli Enterprise Monitoring Server
- ▶ Tivoli Enterprise Portal Server
- ▶ Tivoli Enterprise Portal
- ▶ Tivoli Warehouse Proxy Agent
- ▶ Tivoli Data Warehouse
- ▶ Summarization and Pruning Agent
- ▶ Tivoli Enterprise Console

Figure 2-6 on page 31 depicts the comprehensive architecture for all interconnected components. It points out the recommended strategy for the Tivoli

historical data collection. We highly advise structuring the historical collection flow as outlined in the diagram.

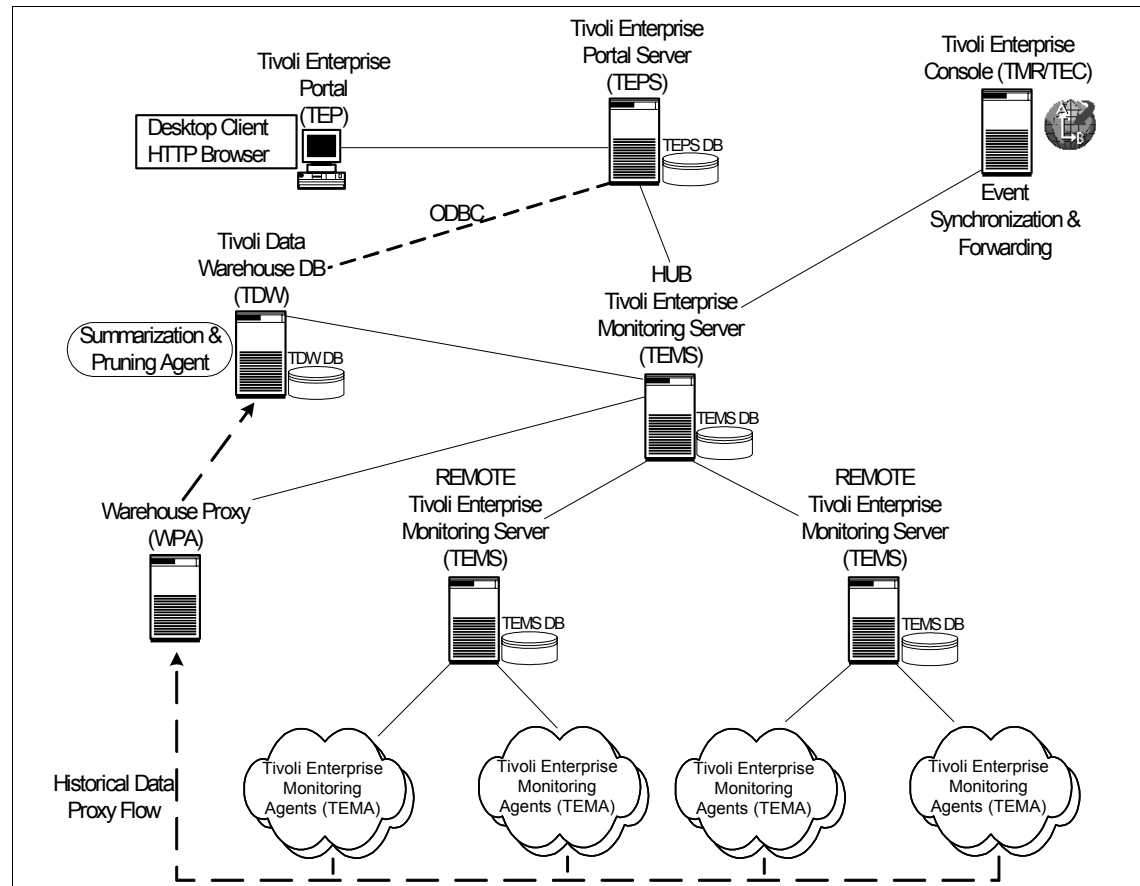


Figure 2-6 IBM Tivoli Monitoring, V6.1, large topology design

**Important:** For simplicity, the Hot Standby node is not shown in the topology diagram. In a large installation, it is strongly recommended to implement the Hot Standby node.

Performing an accurate plan and assessment stage is imperative for the large installation. Mapping all component topology with the recommended hardware specifications is critical in order to achieve a highly distributed environment with realistic goals. We recommend having a thorough understanding of the monitoring environment before preceding to implement any architectural design. It is important to account for all variables within the topology. Substantial

consideration should be given to the infrastructure hardware requirements, and the underlying network topology. Network bandwidth, latency, firewall restriction all require assessment.

The feature rich IBM Tivoli Monitoring, V6.1 is ideal for small/medium installations. Once installed, the installation begins leveraging the best practice functionality immediately. Default situations start running, and if historical data collection is turned on, the default attribute groups begin analysis, and warehousing. These default services can impede the large installation performance throughput, especially if unnecessary attributed group collections are enabled. We highly suggest changing the property *Run at Startup* on all situations to NO immediately after the TEMS, TEPS, and TEP are deployed. This practice ensure freedom to execute the business plan strategy (defining managed system list, customized situation, event mapping, date warehousing intervals, etc.) generated from the assessment and planning phrase. It is vital to the health of the large installation, that only the desired situations, and attribute groups are enabled.

A large monitoring installation will support approximately 1,500 managed systems within an environment. For the large installation, the estimate is 3 agents per managed system. In this installation, a disproportionate distribution of agents is highly anticipated, and this scenario should compliment your own environment analysis phrase. The recommended distribution is 400 agents across 10 REOMTE TEMS. Keeping 400 agents as the high point per monitoring server allows for capacity expansion without exhausting the resources of the infrastructure. For further details on scaling a large installation, please refer to “Scalability” on page 50.

**Tip:** Since IBM Tivoli Monitoring, V6.1 supports primary and secondary communication paths, it is highly suggested to install several backup Remote TEMS which exist solely for TEMA failover capabilities. When a failure of a Remote TEMS occurs, it is not advisable to double the maximum load of production Remote TEMS. Best practices should direct these orphan Tivoli Enterprise Management Agents to idle Remote TEMS.

The Tivoli Data Warehouse data requirement will be a substantial amount. We advise separating the Tivoli Warehouse Proxy Agent and the Tivoli Data Warehouse repository between two systems. The Summarization and Pruning agent should be installed on the Tivoli Data Warehouse system. We always recommend to keeping these two components together.

The large installation introduces the IBM Tivoli Enterprise Console as part of the topology. IBM Tivoli Monitoring, V6.1 has built-in capabilities for event processing that work extremely well in the small/medium installation. However, the large



installation can contain a reasonable increase in volume of event flow, and the Tivoli Enterprise Console is better adapted for large event flow management and correlation. The Tivoli Enterprise Console can be considered an event consolidation Manager of Managers.

The TCO is still nominal compared against IBM Tivoli Monitoring, V6.1 functionality, despite the large hardware requirements necessary to scale this installation properly. The entire large installation can be managed from a single GUI presentation layer down to installing/upgrading agents.

#### **2.2.4 Huge installation - (greater than 4000 agents)**

The huge installation scenario provides a guideline for any IBM Tivoli Monitoring installation which exceeds 4000 agents, or approximately 1,500 managed systems. The scope of the huge installation is similar to the large installation, except for additional configuration guidance.

The installation consists of the following components:

- ▶ Tivoli Enterprise Monitoring Server
- ▶ Tivoli Enterprise Portal Server
- ▶ Tivoli Enterprise Portal
- ▶ Tivoli Warehouse Proxy Agent
- ▶ Tivoli Data Warehouse
- ▶ Summarization and Pruning Agent
- ▶ Tivoli Enterprise Console

Figure 2-7 on page 34 depicts the interconnections between two autonomous IBM Tivoli Monitoring, V6.1 installations. It demonstrates the high level component interaction between two installations that handle 4,000 agent each, totaling 8,000 agents entirely.

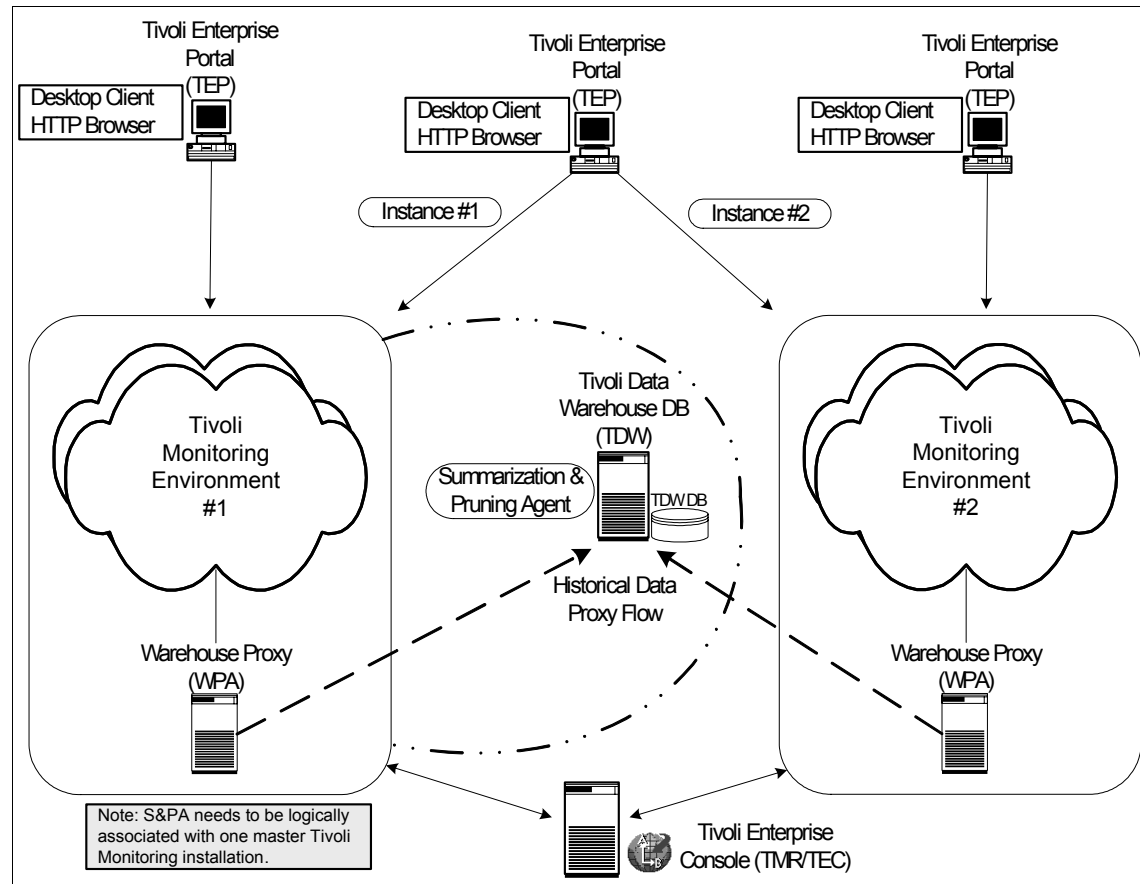


Figure 2-7 IBM Tivoli Monitoring, V6.1, huge installation topology

The recommended deployment strategy is the same as the large installation, except for the Tivoli Data Warehouse, and Summarization and Pruning agent. A huge installation can warehouse historical data collections to one single database server repository from two distinct IBM Tivoli Monitoring, V6.1 installations.

**Important:** As previously noted in “Large installation - (4000 agents maximum)” on page 30, make sure only the required attributed groups are enabled for Tivoli Data Warehousing. Enormous amounts of data can be collected between two large IBM Tivoli Monitoring, V6.1 installations. Best practice design is critical to ensure a stable, scalable environment.

The two installation are still built separately from each other. The only deviation, one IBM Tivoli Monitoring, V6.1 installation requires a logical association as the *master* control for the Summarization and Pruning agent.

**Note:** There can only be one S&P for a single TDW. Since, the S&P requires connections to a TEMS, one of the monitoring installations needs a logically designation as the master. This is not a programmatic assignment, but a logical identification for configuration and management of the S&P.

A flexible feature that is necessary in the huge installation is configuring multiple TEP instances within one single TEP desktop client. If a single TEP desktop client needs to connect to separate autonomous IBM Tivoli Monitoring, V6.1 installation, *instances* are created to associate the unique TEPS connection information.

### ***Defining TEP instances via Tivoli Manage Service GUI***

Use the following steps in the Manage Tivoli Enterprise Monitoring Services GUI to define TEP instances for additional Hub TEMS.

1. Start the Manage Tivoli Enterprise Monitoring Services GUI.

Windows:

Click **Start** → **Programs** → **IBM Tivoli Monitoring** → **Manage Tivoli Enterprise Monitoring Services**.

UNIX/Linux:

Type: **itmcmd manage**

2. Right click on Tivoli Enterprise Portal and click **Create Instance** as shown in Figure 2-8 on page 36.

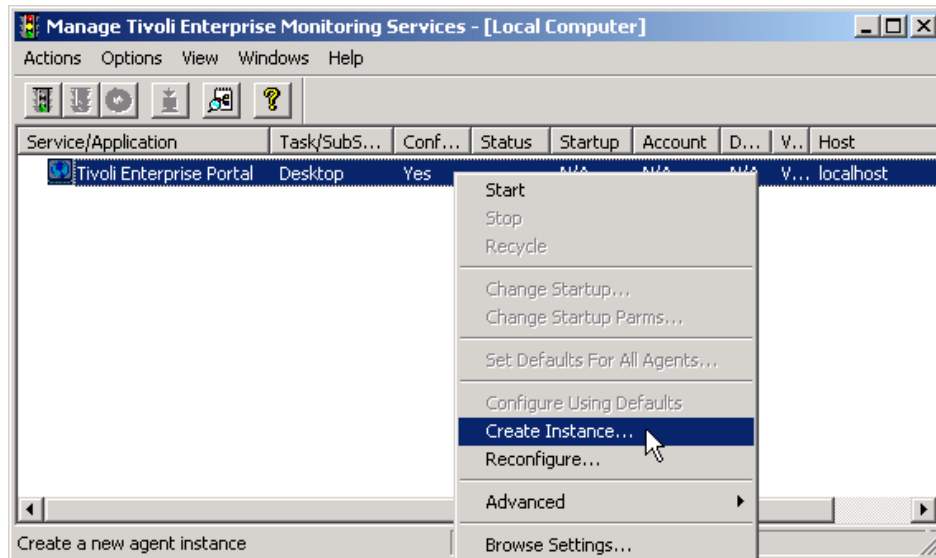


Figure 2-8 Right clicking on Tivoli Enterprise Portal reveals Create Instance option

3. Type the Instance Name and click **OK** (Figure 2-9).

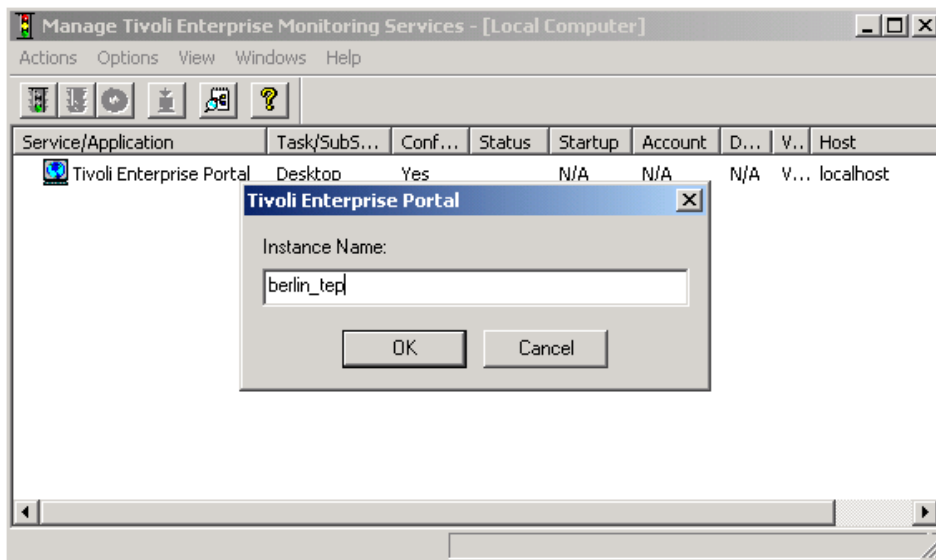


Figure 2-9 Inputting the Instance Name within the dialog box

4. Type the Tivoli Enterprise Portal hostname and click **OK** (Figure 2-10).

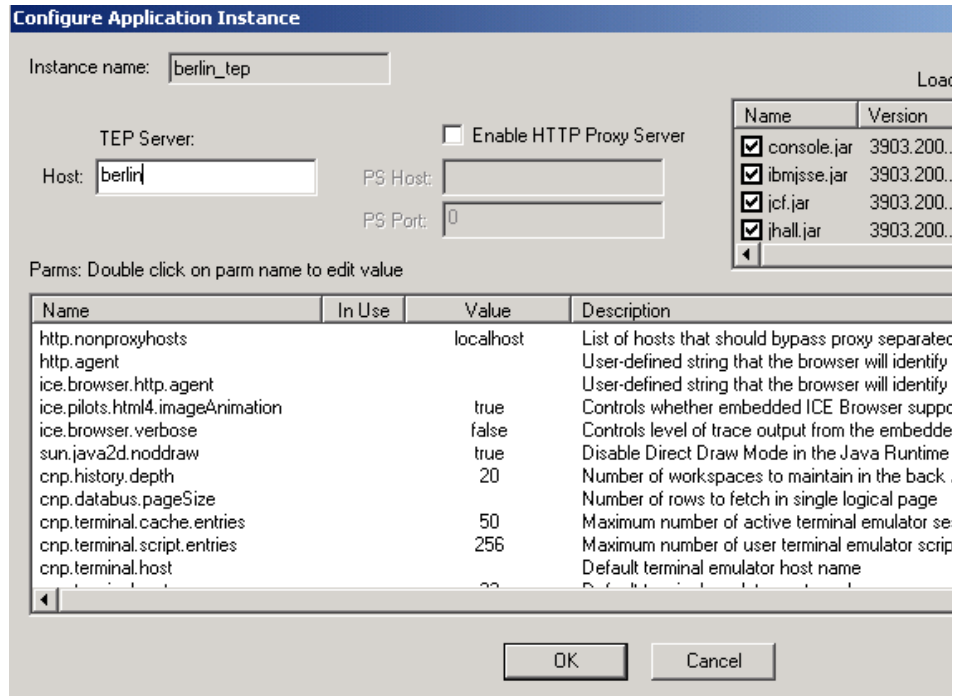


Figure 2-10 Inputting the Tivoli Enterprise Portal hostname in the TEP Server field

5. The new Tivoli Enterprise Portal is now displayed in the Manage Tivoli Enterprise Monitoring GUI (Figure 2-11 on page 38).

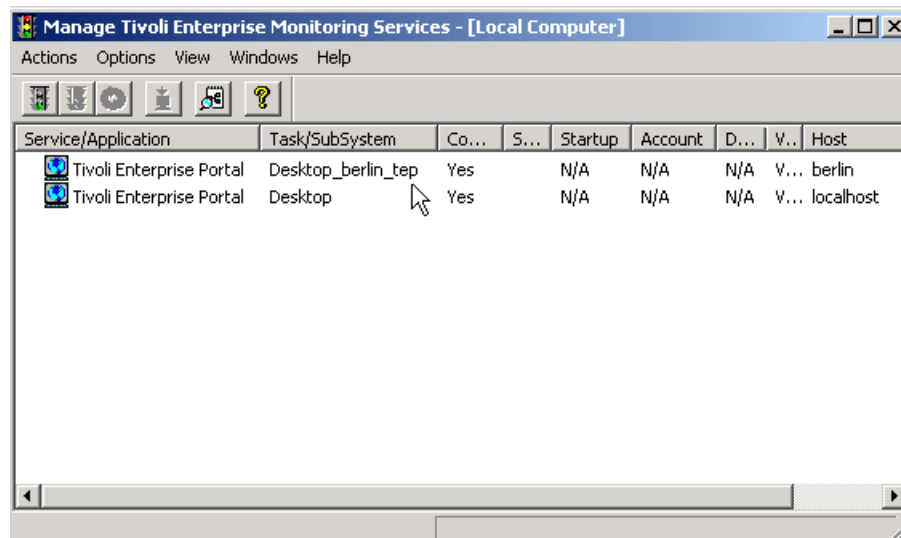


Figure 2-11 The newly defined Tivoli Enterprise Portal instance

Subsequent Tivoli Enterprise Portal instances are defined repeating steps 1 - 4 (Figure 2-12).

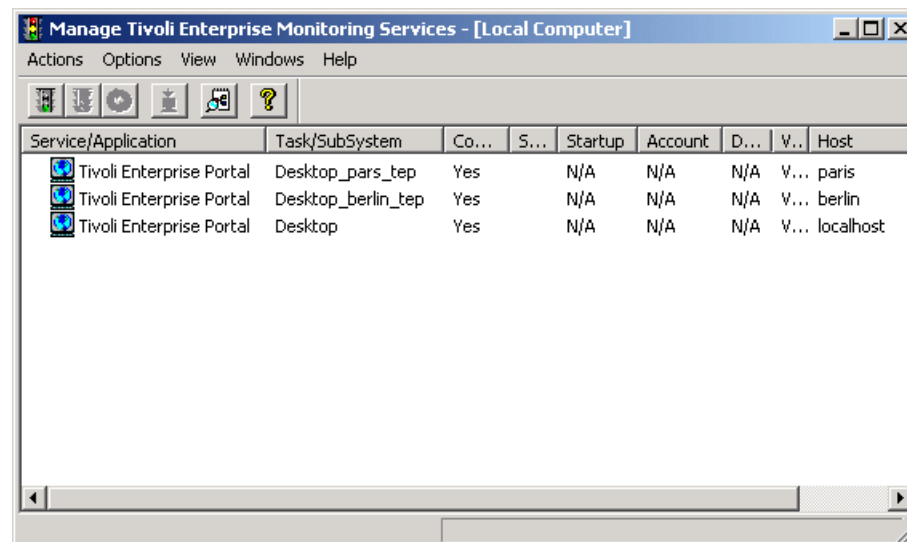


Figure 2-12 Example of additional Tivoli Enterprise Portal instances

## 2.2.5 Advanced large installation with firewall scenarios

In most IBM Tivoli Monitoring, V6.1 implementations, firewalls will play an important role throughout the architecture. For a successful implementation, it is important to understand the component communication flow. The configuration to support IBM Tivoli Monitoring, V6.1 within firewalls can be split into two major parts:

- The TEMS, TEPS, and TEMA protocol communication.
- The TEP and TEPS protocol communication.

**Tip:** Please refer to the *IBM Tivoli Monitoring, V6.1.0 Installation and Setup Guide*, GC32-9407, chapter 9 for expert advice on firewall scenarios. Chapter 9 has several excellent examples using firewalls involving the TEP and TEPS.

### Communications protocol selection

If installing IBM Tivoli Monitoring, V6.1 components across firewalls, it is recommended to configure the *IP.PIPE* (TCP communication) protocol. The *IP* (UDP communication) protocol is insufficient for firewall configurations. The connectionless UDP protocol would require opening up multiple ports across firewalls, to allow multiple connections from each individual IBM Tivoli Monitoring, V6.1 component. For example a TEMA communicating to the TEMS using IP (UDP communication) protocol requires multiple ports to operate properly. Secondly, using the *IP.PIPE* (TCP communication) will enable the *Emphemeral pipe* operation automatically if certain conditions match.

**Note:** When *IP.PIPE* is specified as your communications protocol, you may still see other ports being used in communication traces and logs, but these ports are virtual and multiplexed over the default *IP.PIPE* port.

The *IP.PIPE* protocol has some notable limitations:

- Only 16 IBM Tivoli Monitoring, V6.1 processes on a single system can share the base listening port (default port 1918) on a single network interface card when using the protocol. Any processes above 16, will fall back to using the IP protocol (only if configured). This mainly is a restriction when running large amounts of Tivoli Enterprise Management Agents on one physical system. It is not a limitation for the total amount of TEMA connecting to one TEMS. This may only occur when a system is required to run more than 16 Universal Agents or has more than 16 Database Agent instances. If firewall restrictions force the use of the *IP.PIPE* protocol, the only work around is to move excess Tivoli Enterprise Management Agents above 16 to another system.

- The TEMS may run out of sockets (listen threads). Evidence of this will be highlighted in the TEMS log:

message KDSMA010 – Communication did not succeed.

If this occurs, you should increase the number of sockets by changing the setting of KDS\_NCSLISTEN. The maximum value that can be set is 256.

The following Table 2-1 depicts the *default* listening ports for the IBM Tivoli Monitoring, V6.1 components. Use this table as a quick reference to understand the standard ports for an installation. Although supported it is not recommended to modify these default values.

Table 2-1 Default port usage for IBM Tivoli Monitoring, V6.1

IBM Tivoli Monitoring, V6.1 Component	Listening Port
Tivoli Enterprise Monitoring Server ( <i>ip.pipe</i> )	1918/tcp
Tivoli Enterprise Monitoring Server ( <i>ip.spipe</i> )	3660/tcp
Tivoli Enterprise Monitoring Server ( <i>ip</i> )	1918/udp
Tivoli Enterprise Portal Server	1920/tcp 15001/tcp
Tivoli Enterprise Console	5529/tcp
Tivoli Warehouse Proxy Agent	6014/tcp(1)

1. Refer to Example 1-1 on page 26

**Tip:** Although technically supported, do not deviate from the default listening ports unless for a valid reason. Listening port modification was not tested by IBM Tivoli Software Group.

Using IP.PIPE allows a few well know ports to be open through the firewall. Which port to open can be calculated using the Example 2-1 on page 41. If the firewall is not using NAT (Network Address Translation), the computation should be sufficient to have the components connect through the firewall.

Every system that has IBM Tivoli Monitoring, V6.1 installed will automatically reserve the well-known port (default 1918) for the Tivoli Enterprise Monitoring Server communication. No matter what order components startup on a system which has several IBM Tivoli Monitoring, V6.1 components installed, the default well-known port is only used by the TEMS.

**Note:** 1918 is the default *well-known* port, any well-known port can be configured, as long as the entire environment matches this port number.



For all other components except for the TEMS, the following calculation is used internally by IBM Tivoli Monitoring, V6.1 to reserve the listening ports.

*Example 2-1 IBM Tivoli Monitoring, V6.1 algorithm to calculate listening port*

---

“reserved port” = well-known port + ( $N \times 4096$ )

where:

$N$  = startup sequence

---

For example, the IBM Tivoli Monitoring, V6.1 component startup on the system Izmir follows this sequence:

1. The Universal Agent starts first: port 6014 ( $1918 + 1 \times 4096$ )
2. The Remote TEMS starts second: port 1918 (always reserved for TEMS)
3. The Windows OS Agent starts third: port 10110 ( $1918 + 2 \times 4096$ )
4. The Warehousing Proxy starts fourth: port 14206 ( $1918 + 3 \times 4096$ )

## Not all communication is through the firewall

Using the calculation from Example 2-1, it is now possible to control the port usage on individual systems. Additionally, using two parameters in the KDC\_FAMILIES environment variable allow for even finer control other than the startup sequence method. Ideally, all components that need access through the firewall should use the lower number ports, while components that do not cross the firewall use higher number ports.

This is accomplished by specifying the *SKIP* and *COUNT* parameters on the KDC\_FAMILIES environment variable for individual IBM Tivoli Monitoring, V6.1 component.

For example:

```
KDC_FAMILIES=IP.PIPE COUNT:1 PORT:1918 IP use:n SNA use:n IP.SPIPE use:n
```

- ▶ The COUNT parameter (coded as COUNT: $N$  – where  $N$  is an integer that indicates which port to reserve) for the components that need access across a firewall. If the process is unable to bind to the highest port respective to  $N$ , it immediately fails to startup.
- ▶ The SKIP parameter (coded as SKIP: $N$  – where  $N$  is an integer that indicates which port to reserve +1) for the components that do not need access across a firewall. If the process is unable to bind to the port respective to  $N$ , it will keep trying using the algorithm until all available ports are exhausted.

For example:

*Example 2-2 Example for KDC\_FAMILIES=IP.PIPE COUNT*

---

The system Izmir has installed:

- Tivoli Enterprise Monitoring Server
- Windows OS Agent
- Warehousing Proxy Agent

The well-known port is the default port 1918.

The Tivoli Enterprise Monitoring Server always uses port 1918.

The Windows OS agent does not require firewall access and should be coded with KDC\_FAMILIES=IP.PIPE SKIP:2 (port 10110).

If the Windows OS agent fails to open port 10110, it will try SKIP:3 attempting to bind now to port 10370. A failure will result in trying SKIP:4 continuing to exhaust all possibilities with any subsequent failures.

The Warehouse Proxy does require firewall access and should be coded with KDC\_FAMILIES=IP.PIPE COUNT:1 (port 6014).

If the Warehouse Proxy fails to open port 6014, start up fails.

---

## Multiple network interface cards

Whenever an IBM Tivoli Monitoring, V6.1 component starts up, it will by default discover all available network interfaces on the system and will actively use them. This may not always produce the desired results.

Let us take the example of a TEMS with two networking interface cards (NIC): one interface connected to the main production network and a second interface connected to a limited network that is only used for server backup.

When a TEMA on another system starts up and makes the first connection to the TEMS using the Global Location Broker, it connects to the TEMS first interface. Also, assume the TEMA does not have a interface connected to the limited backup network segment. The TEMS will send a reply to the TEMA, containing the network address on which the TEMS wants the TEMA to connect. This network address may be the NIC that is connected to the backup network. This results in the TEMA not being able to successfully connect even though the initial handshake succeeded.

To avoid this problem, you can specify a environment parameter on all the IBM Tivoli Monitoring, V6.1 components to force it to use a specific network interface rather than using any available.

This can be accomplished by passing either of these keywords:

- ▶ **KDCB0\_HOSTNAME:** you can either specify the hostname, corresponding to the NIC to be used, or its IP address in dotted decimal format. If specified, it will take priority over the KDEB\_INTERFACELIST parameter.  
KDCB0\_HOSTNAME should only be used in an environment without NAT

(Network Address Translation), since it will also inactivate the use of the Ephemeral Pipe.

- ▶ KDEB\_INTERFACELIST: the NIC must be specified as dotted decimal IP addresses. This keyword is recommended when IBM Tivoli Monitoring, V6.1 is installed in a environment with NAT.

Regardless, this technique is still a good practice to use to make sure that the Tivoli Enterprise Management Agents connect back to proper interface on the TEMS.

## Installations with firewalls

The best practice with Tivoli Enterprise Management Agents on the less secure zone of the firewall would be to deploy a Remote TEMS on the same firewall side. This will allow all TEMA to connect to the Remote TEMS and only have the Remote TEMS connect through the firewall.

This will minimize the number of systems which need firewall access, and keep port restrictions in place. Refer to Figure 2-13 on page 45 and Figure 2-14 on page 46 for a visual diagram.

### *Special case*

- ▶ Firewall with NAT - Ephemeral pipe

Today, many firewall implementations include Network Address Translation, which further protects the systems behind the firewall by making them “invisible” using a different set of IP addresses. If the configuration includes a firewall with NAT, the easiest way to configure TEMA, TEPS, or TEMS to connect to another TEMS would be the Ephemeral pipe. When an Ephemeral pipe is active, it acts as a *virtual tunnel* that funnels all connections between two components through one single port. The Ephemeral pipe is not explicitly started when using the standard installation scripts or tools, but will be activated by default under following conditions:

- KDC\_PARTITION definition file is not present. If KDC\_PARTITION is used, it inactivates the Ephemeral pipe.
- KDCB0\_HOSTNAME parameter should not be specified, instead use the KDEB\_INTERFACELIST variable.
- The initial communication must come from the agents, not by the TEMS. Older configurations may still have a KDSSTART LBDAEMON command for the Location Broker at the TEMS. This command should be removed to active the Ephemeral pipe.

If these conditions are met, TEMA to TEMS communication will automatically try to create an Ephemeral pipe connection and no further configuration actions are required. The main advantage of using Ephemeral pipe is that no special

configuration is required, so you do not have to *manually* update the configuration parameters at possibly hundreds of TEMA that run outside of the firewall.

The Ephemeral pipe can be explicitly configured by setting this parameter:

```
KDC_FAMILIES=IP.PIPE PORT 1928 EPHEMERAL:Y
```

This will force the client to use outbound ephemeral connections. This kind of configuration should be used, if you encounter duplicate pipe setup failure messages in the TEMS log – which will occur if you run multiple agents on the same system as the TEMS, and all connect to that particular TEMS using the same pipe. In this case, EPHEMERAL:Y will force the agents to use the Ephemeral pipe.

While Ephemeral pipe is the first choice for firewall environments with NAT, it may not communicate successfully across firewalls in all environments. If communication failures occurring between the TEMA and the TEMS, a more detailed communications trace will be required. Set the KDC\_DEBUG=Y variable to generate the required level of detail trace.

If the output of the KDC\_DEBUG=Y trace contains IP addresses with 0.0.0.0, this indicates correct use of Ephemeral pipe. However if communications is still failing, you will have to use the alternative technique which requires partition definitions. This can happen if the connections between TEMA and TEMS have to cross multiple firewalls or if NAT has been set up without using generic patterns.

#### ► Firewall with NAT – Partitioning

If Ephemeral pipe fails to establish a connection between the agents and the Hub TEMS, the only alternative with this IBM Tivoli Monitoring, V6.1 release is to use partition files. This is fully documented in the *IBM Tivoli Monitoring, V6.1.0 Installation and Setup Guide*, GC32-9407.

## Large installation with firewall architectures

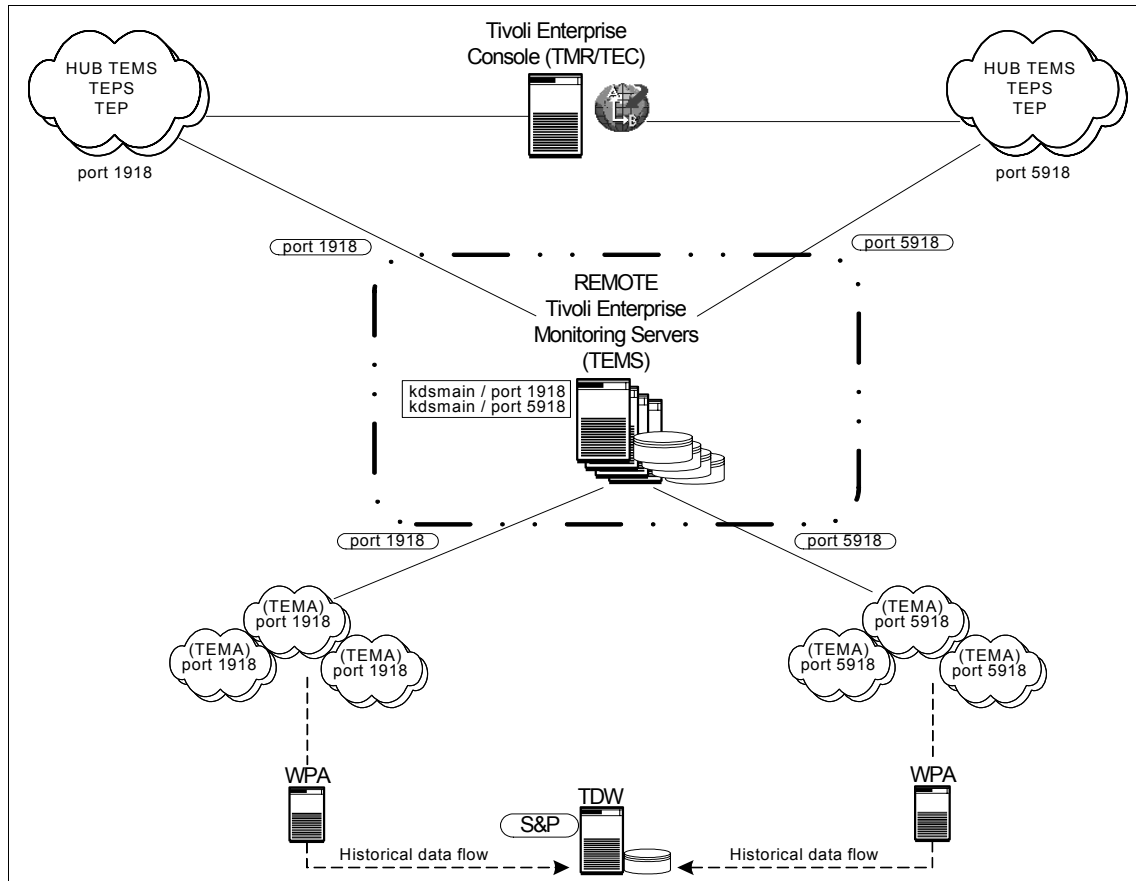
Keep in mind, security guidelines in a specific environment may be inflexible when dealing with the location of some of the IBM Tivoli Monitoring, V6.1 components. Accurate comprehension of the communication flows and ports will allow any installation to be customized to meet the underlying security policies.

The following recommended architectures provide visual guidance in assisting to understand the communication flow among the IBM Tivoli Monitoring, V6.1 components. Mastery of IBM Tivoli Monitoring, V6.1 communication protocol provides the architect control over the entire network topology. The following only presents two common designs.

### ***Warehouse Proxy agent in less secure zone***

This scenario is based on less restrictive firewall rules concerning the traffic flow for the historical data collection. Here the Warehouse Proxy Agent is located in the less secure zone.

Figure 2-13 depicts one recommended architecture for a IBM Tivoli Monitoring, V6.1 installation with firewall restrictions enabled, and the WPA located in the less secure zone.



*Figure 2-13 Advanced Installation with firewalls, warehouse proxy agent on less secure side*

This scenario keeps the TEMA warehousing traffic on the same side of the firewall, and the actual database repository on the more secure side. It is unnecessary to keep track of the WPA listening port for firewall rules. A specific port will have to be opened on the firewall to allow the WPA to perform a ODBC connection to the Tivoli Data Warehouse on the more secure side. The port for

the ODBC connection is unique to each RDBMS. Please consult the database product manuals or your local database administrator.

### ***Warehouse Proxy agent in more secure zone***

In this second scenario, the firewall restrictions are expanded to not allow any warehousing traffic to be on the less secure side of the firewall.

Figure 2-14 depicts the recommended architecture for a IBM Tivoli Monitoring, V6.1 installation with firewall restrictions increased, and the WPA located in the more secure zone.

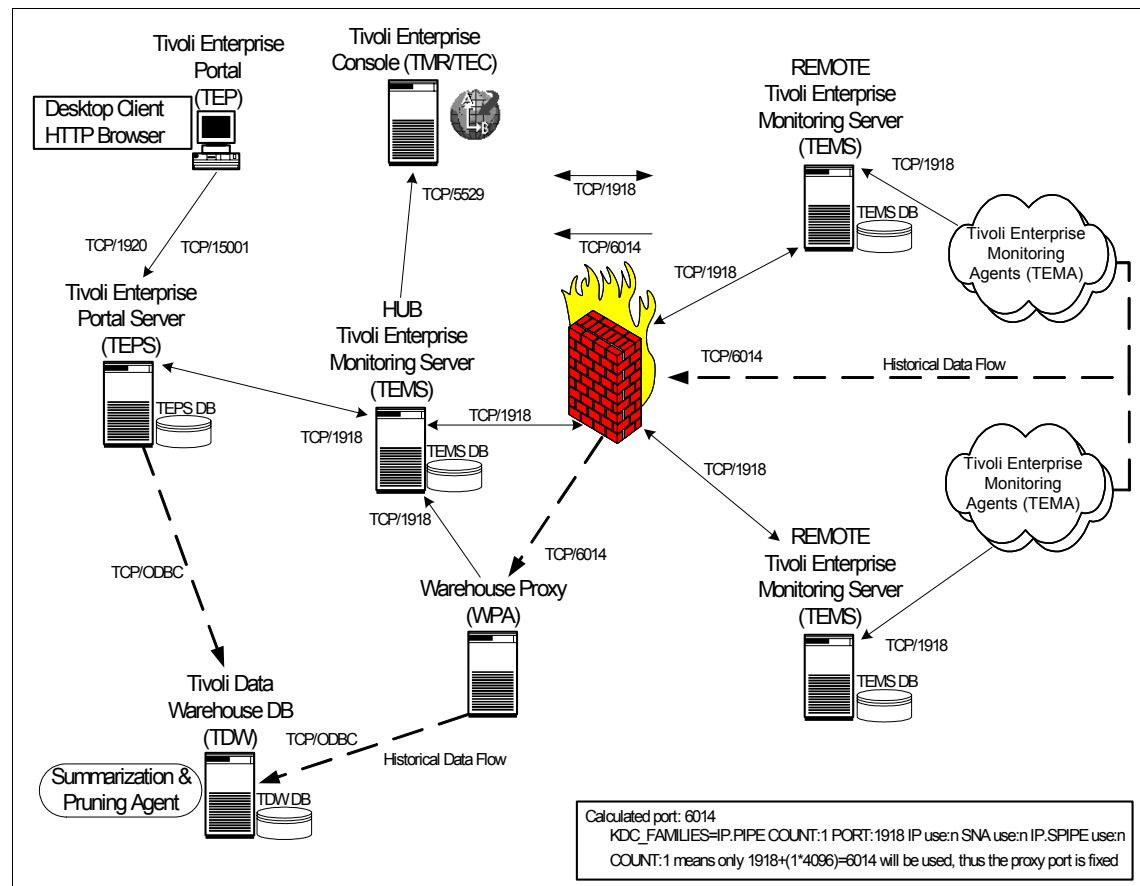


Figure 2-14 Advanced Installation with firewalls, warehouse proxy agent on more secure side

This scenario forces the TEMA to warehouse traffic through the firewall. The Warehouse Proxy Agent and the Tivoli Data Warehouse repository are both located in the more secure zone. This design increases the complexity for the Warehouse Proxy Agent but also increases the security of the warehouse data.

In order to open the proper ports so that the TEMA can warehouse the historical data through the firewall, the Warehouse Proxy Agent must establish a well-known listening port. This well known port is calculated through the KDC\_FAMILIES mechanism.

**Tip:** The Warehouse Proxy Agent calculated port is significant only when:

- ▶ the TEMA are warehousing data directly to the WPA, instead of storing on the Remote TEMS.
- ▶ firewall policies do not allow ODBC connections to be made from less secure to the more secure infrastructure, and the WPA must be located behind the firewall from the agents.
- ▶ the TEMA must go through a firewall to connect to the WPA.

When warehousing data in a large installation especially within the boundaries of firewalls, keep these tips handy:

- Accurately calculate the collection amount of historical data. Firewall traffic can increase excessively when historical data collection is enabled.
- Only collect the critical attribute groups, be careful not to turn on unnecessary attribute groups.
- Historical data roll-up can be stored on the Remote TEMS. However, it is severely limited to 250 TEMA per Remote TEMS.
- There is a Windows platform limitation of a maximum 2,000 sockets open simultaneously. Within a firewall environment, IP.PIPE is required. This limits the warehousing of historical data to only 1,500 TEMA (500 sockets are reserved for internal processing) per IBM Tivoli Monitoring, V6.1 installation.

**Important:** If you are familiar with the functions of Tivoli Firewall Security Toolbox (TFST), IBM Tivoli Monitoring, V6.1 firewall support currently does not provide all the functions the TFST, particularly to be able to start the connection from the secure site and proxying between multiple firewalls (to be able to use different ports between multiple firewalls). These functions are expected to be available with a Fix Pack post GA of IBM Tivoli Monitoring, V6.1.

## 2.2.6 Advanced huge installation - multiple TEMS processes

This advance deployment scenario illustrates the power, flexibility, and capabilities of IBM Tivoli Monitoring, V6.1. This deployment strategy requires double the recommended hardware specifications, but less physical hardware

deployment. This deployment exposes the technical capacity of running multiple monitoring server (TEMS) processes on one physical system. It certifies the adaptability of IBM Tivoli Monitoring, V6.1, but acknowledges the extreme complexity which can occur within an installation.

Exceptional planning and assessment must precede this implementation, it can be very easy to allow this strategy to become a maintenance dilemma.

This installation still requires multiple Hub TEMS, but leverages unused hardware capacity to run additional Remote TEMS processes (configured to listen on different ports) connecting to the separate Hub TEMS.

The installation consists of the following components:

- ▶ Tivoli Enterprise Monitoring Server
- ▶ Tivoli Enterprise Portal Server
- ▶ Tivoli Enterprise Portal
- ▶ Tivoli Warehouse Proxy Agent
- ▶ Tivoli Data Warehouse
- ▶ Summarization and Pruning Agent
- ▶ Tivoli Enterprise Console

This design strives to highlight the potential strategic deployment using multiple TEMS processes configured on different listening ports. It is architectural similar to the large installation. However, there are multiple Remote TEMS processes running on one physical system.

Keep in mind that Figure 2-15 on page 49 demonstrates a simple architecture to present the underlying theory. IBM Tivoli Monitoring, V6.1 is expandable further and can run more than two kdsmain processes per system. This technique accomplishes a larger implementation with less physical hardware. To keep the diagram intelligible, the Remote TEMS have been stacked for brevity. Even though this strategy is similar to the large installation (the implementation is exactly the same), we do not recommend loading this IBM Tivoli Monitoring, V6.1 installation to its maximum throughput.



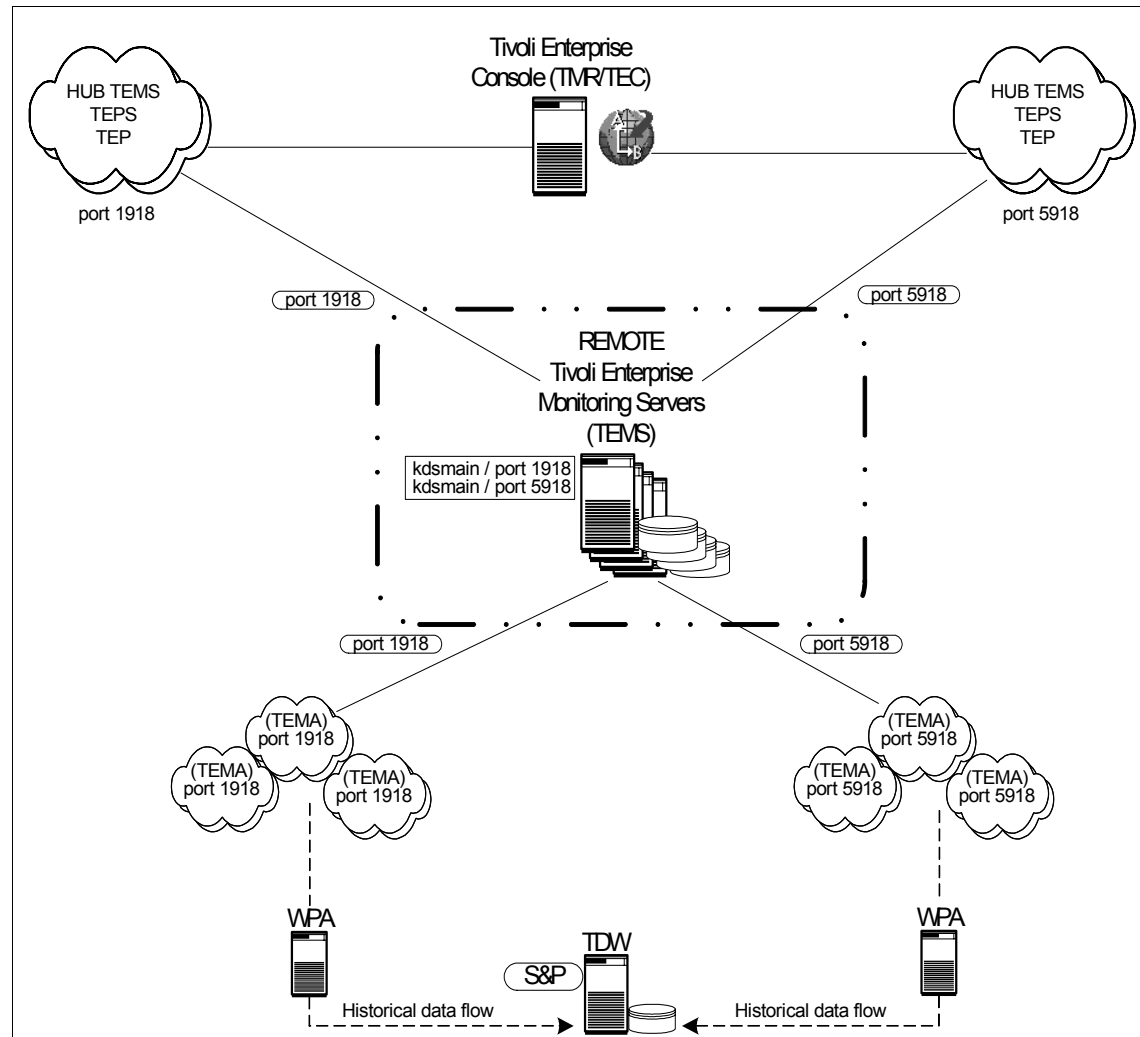


Figure 2-15 Large installation with multiple TEMS processes running on single system

Essentially, this large installation is capable of having up to 10 Remote TEMS, each running two or more Tivoli Enterprise Monitoring Server processes within one system boundary.

IBM Tivoli Monitoring, V6.1 has a software limitation which only permits a single Tivoli Enterprise Monitoring Server process to listen on the well-known port (default port 1918). In order to achieve this design, any additional TEMS processes on the exact system must be configured to use an unused port. This process essentially doubles the IBM Tivoli Monitoring, V6.1 capacity, without

additional hardware. We advise only running one Hub TEMS per physical system. Multiple TEMS processes on a single system all configured as (\*HUB) is supported, but not suggested.

To accomplish this installation, separate IBM Tivoli Monitoring, V6.1 install directories are necessary. These installations will be completely separate despite the binaries existing on the same physical system. Follow the normal installation procedures for a single large installation environment. The only necessary installation procedure change is the configuration of the well-known listening port for each running TEMS process. For historical data collection, it is exactly the same as a huge installation. One Tivoli Data Warehouse repository with multiple Warehouse Proxy Agents.

**Note:** A Warehouse Proxy Agent is required for each separate TEMS process instance. For example, TEMS process instances running on three different ports will require three Warehouse Proxy Agents.

One thought to keep in mind: these multiple TEMS processes are still logically independent installations which still require separate maintenance for each. The infrastructure systems will have distinct CANDLEHOME installation directories. The IBM Tivoli Monitoring, V6.1 code on every system will require maintenance to every separate installation directory.

**Attention:** Running multiple TEMSs on a single system is technically supported by IBM Tivoli Monitoring, V6.1. However, all alternatives should be given careful consideration. The total cost of ownership to maintaining this complex environment can be higher than the cost of additional hardware capacity.

## 2.3 Scalability

A distributed networking infrastructure inherits scalable characteristics by design. After all, a distributed system is built to expand and shrink through the increment and decrement in hardware capacity. It should be stated that scalability is not the same as performance tuning. Performance tuning deals with increasing output from current capacity without adding additional resources.

No single analysis of scalability and performance can determine the absolute hard limits of a distributed product. A distributed system in theory should extend to infinity. However, as distributed systems increase in scalability, performance loss may increase to an un-sustainable boundary. IBM Tivoli Monitoring, V6.1 follows the basic scalable characteristic within this design. Adding hardware capacity in the form of remote TEMS will distribute the load and allow a larger

amount of connected agents. This methodology represents a foundation which is built upon using the actual calculated values from the physical environment. It should be noted that IBM Tivoli Monitoring, V6.1 constitutes vast improvements in scalability and performance from OMEGAMON XE. It highlights the union between the mature code of Candle Corporation and the Enterprise qualification of IBM Tivoli Software.

Figure 2-16 depicts a great universal example of many unique sources of information pertaining to scalability and performance metrics. It exposes the issues revolving around scalability and performance expectations.

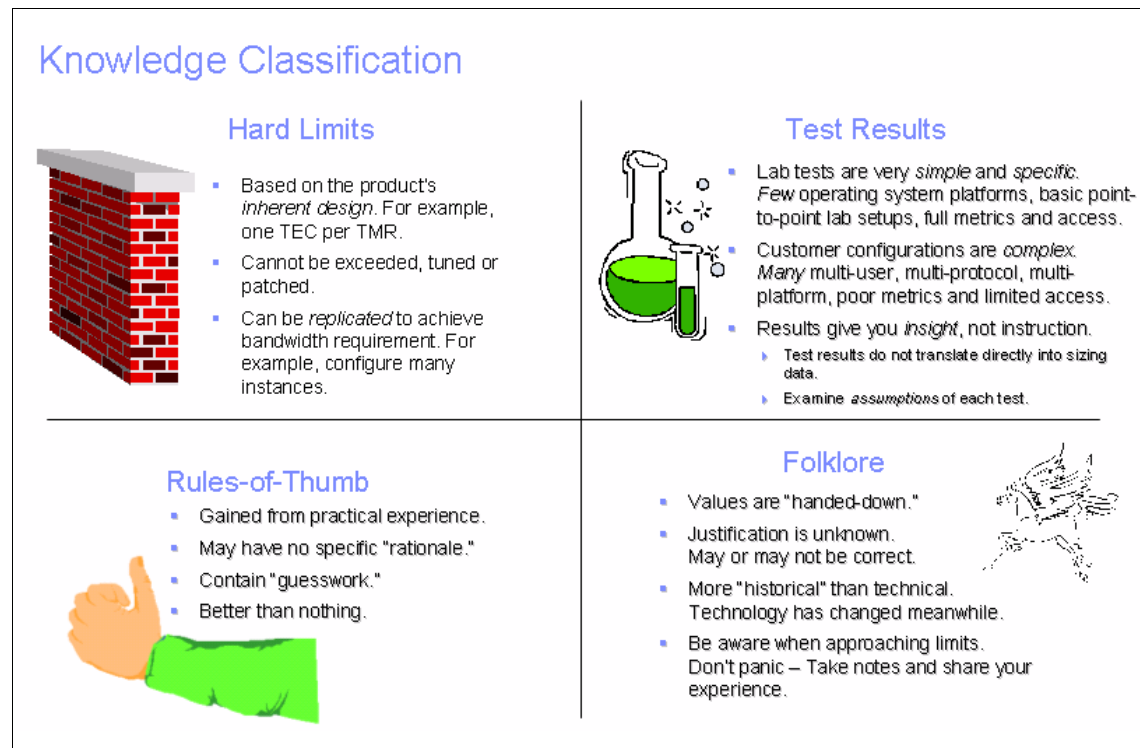


Figure 2-16 Universal sources of scalability and performance numbers

For example:

- ▶ User Guide says "unlimited"
- ▶ Support said "no more than n ..."
- ▶ Development said "n\*3 ..."
- ▶ Early Support Program said "n^3 ..."
- ▶ Services said "n/3 ..."
- ▶ Performance said "we didn't test that."

A decision must be carefully chosen because different sources have their own reasons for providing sizing metrics.

For IBM Tivoli Monitoring, V6.1, analysis of all these sources including an in-depth knowledge of the monitoring environment will assist in scaling the installation properly. Understanding the limitations of IBM Tivoli Monitoring, V6.1, and strategically working through them will facilitate obtainable goals.

From a scalability standpoint, the TEMS plays the key role. As the architect of an IBM Tivoli Monitoring, V6.1 implementation, the following factors need to be considered:

- Number of physical hosts and platforms types included.
- Number and type of applications and operating systems per host.
- Geographical topology of the environment, particularly in relation to where the managed systems shall reside.
- Estimated number of events generated and/or thresholds that will be deployed.
- The degree of automation that is required or planned – both reflex and workflow.
- Estimated number of TEP users and the expected type of usage (heavy reporting, frequent real time updates, etc.)
- Network topology and firewall considerations.

The information generated from these points above can then be combined with the scalability guidelines that have been established for the initial release of IBM Tivoli Monitoring, V6.1.

The following scalability metrics are from verification testing performed on IBM Tivoli Monitoring, V6.1 (GA). These numbers represent actual test synopsis validation. These numbers are not definitive declarations of scalability and performance. This data displays achievable goals which have been proven in a test/development environment. All IBM Tivoli Monitoring, V6.1 installations are unique, and require surveillance during the deployment.

Table 2-2 classifies the extensive metrics for IBM Tivoli Monitoring, V6.1. These metrics measure the apex for the IBM Tivoli Monitoring, V6.1 components with respect to load quantity. All these metrics represent one installation instance.

*Table 2-2 Extensive metrics*

IBM Tivoli Monitoring, V6.1 Component	Verified Metric
Remote TEMS	15 (Windows and UNIX)

IBM Tivoli Monitoring, V6.1 Component	Verified Metric
Managed Systems	5,000
Managed Systems per Remote TEMS	500
Heartbeating agents per TEMS	500
Simultaneous agent startup/logins to a TEMS	1,000
Agents storing historical data at Remote TEMS	250
Consoles per TEPS	50
Total situations	1,500 (30/agent)

**Important:** These metric values do not represent actual hard limits in IBM Tivoli Monitoring, V6.1. These numbers are derived from what was actually tested, not necessarily product limitation.

The Tivoli Data Warehouse scalability and metrics are out of scope within this chapter. For detailed information on performance and planning guidance, please refer to <xref - john's chapter>.

## 2.4 Agent deployment architecture

There are several techniques to install the Tivoli Enterprise Management Agents. This section summarizes three common practices which can be employed to install managed systems with an installation.

All three scenarios contain pros and cons as an established solution. Proper assessment of the physical environment will assist in the decision of which solution best fits.

Tips to keep in mind:

- Total number of physical systems, and the total amount of agents deployed to each of those systems.
- Network bandwidth and latency between TEMS and TEMA.
- Size of the IBM Tivoli Monitoring, V6.1 installation.
- Connectivity to the managed systems

## 2.4.1 IBM Tivoli Monitoring, V6.1 built-in Deployment Controller

IBM Tivoli Monitoring, V6.1 offers a easy, efficient deployment mechanism to push Operating System Agents, and Applications Agents to remote systems. Furthermore, this mechanism offers agent upgradability. IBM Tivoli Monitoring, V6.1 provides a powerful built-in tool allowing for intelligent agent upgrades via the GUI or command-line.

Figure 2-17 shows the architecture of IBM Tivoli Monitoring, V6.1 agent components. The functionality of the agent components are divided among the TEPS, TEMS and the OS Agent respectively.

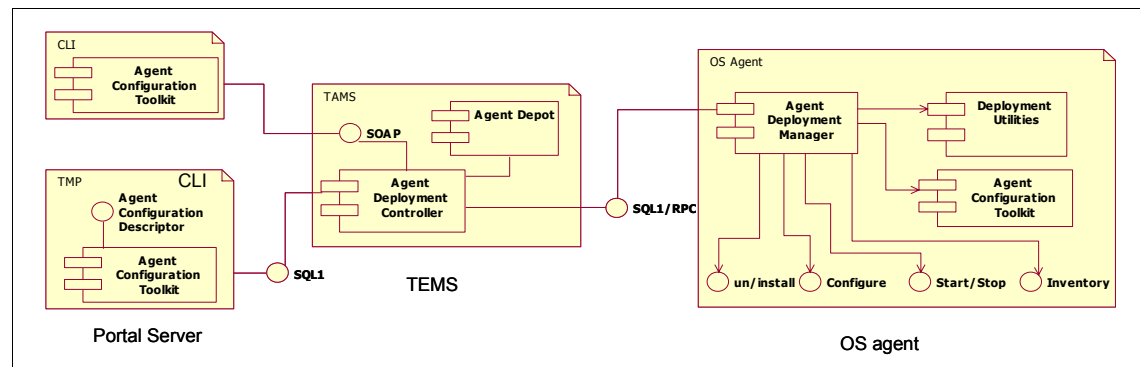


Figure 2-17 Agent deployment architecture

IBM Tivoli Monitoring, V6.1 OS Agents, implemented as a DLL, can handle agent deployment activities at the agent end.

The Agent Depot is an installation directory on the monitoring server from which you deploy agents and maintenance packages across your environment. The Agent Depot must reside on a local TEMS or on a remote file system configured as its depot home directory. Before you can deploy any agents from a monitoring server, you must first populate the Agent Depot with bundles. A bundle is the agent installation image, as well as any prerequisites.

Agents can be loaded into the Agent Depot at install time. Installer on Windows and UNIX has a “populate depot” option.

**Note:** No transfer of packages from one TEMS to another is provided.

Each agent bundle in the Agent Depot can be determined by its product id and platform characteristics. The Agent Depot can also contain MDL files and scripts used in the deployment of the Universal Agent. You can customize the Agent

Depot based on the types of bundles that you want to deploy and manage from that monitoring server.

The Deployment Controller is a service on the Management Server whose role is to act as the driver for the deployment. The Deployment Controller queries the contents of the Agent Depot and transfers agent bundles using Remote Procedure Calls (RPC). All other tasks are initiated by making SQL1 calls. Agent deployment requests are made using SQL1 calls to a Management Server. The Deployment Controller provides the ability to initiate deployment commands from a SQL1 interface.

**Notes:**

- ▶ In order to allow remote deployment, the target system must support (and configured for) at least one of these protocols:
  - SMB (server message block)
  - SSH (secure shell protocol)
  - REXEC (remote execution protocol)
  - RSH (remote shell)

By default, Deployment Controller attempts all these protocols until a connection is successfully established on one of them.

- ▶ Remote Procedure Call (RPC) is a protocol that one program can use to request a service from a program located in another computer in a network without having to understand network details. (A procedure call is also sometimes known as a function call or a subroutine call.)
- ▶ SQL1 is the implementation of SQL that is based on ANSI-1989 SQL1 standard.

Deployment Controller commands can be targeted to a specific system or to a managed system list. The deployment controller manages the interaction with the management agent (OS Agent); it manages receiving and aggregating results from multiple targets and provides forwarding of requests to the appropriate TEMS as well as queuing of requests for scalability. The following processes can be initiated: install, uninstall and upgrade.

**Note:** Deployment requests are asynchronous; once a request is received it is queued up for processing.

Agents vary greatly in how they are configured depending on the agent type and the OS platform. The Agent Configuration Toolkit collects and transfers configuration data. It provides a set of utilities to allow the agent deployment to

configure agents. The communication between the Agent Configuration Toolkit and the Deployment Controller is via SOAP.

SOAP (Simple Object Access Protocol) is a way for a program running in one kind of operating system (such as Windows 2000) to communicate with a program in the same or another kind of an operating system (such as Linux) by using the World Wide Web's Hypertext Transfer Protocol (HTTP) and its Extensible Markup Language (XML) as the mechanisms for information exchange. Since Web protocols are installed and available for use by all major operating system platforms, HTTP and XML provide an already at-hand solution to the problem of how programs running under different operating systems in a network can communicate with each other. SOAP specifies exactly how to encode an HTTP header and an XML file so that a program in one computer can call a program in another computer and pass it information. It also specifies how the called program can return a response.

An advantage of SOAP is that program calls are much more likely to get through firewall servers that screen out requests other than those for known applications (through the designated port mechanism). Since HTTP requests are usually allowed through firewalls, programs using SOAP to communicate can be sure that they can communicate with programs anywhere.

## 2.4.2 IBM Tivoli Configuration Manager, V4.2

Most IBM Tivoli Software customers already have an investment in Tivoli Management Framework, V4.1.1, and IBM Tivoli Configuration Manager, V4.2 IBM Tivoli Monitoring, V6.1 Agents can be deployed using IBM Tivoli Configuration Manager, V4.2 as the delivery mechanism.

It is cost effective to leverage IBM Tivoli Configuration Manager, V4.2 as a solution to deliver IBM Tivoli Monitoring, V6.1 Agents. IBM Tivoli Configuration Manager, V4.2 is robust and designed for large volume software pushes, which dominates over IBM Tivoli Monitoring, V6.1 Deployment Controller.

For information on deploying IBM Tivoli Monitoring, V6.1 Agents via IBM Tivoli Software, you can refer to Chapter 11 “Agent deployment using IBM Tivoli Configuration Manager Software Distribution” in *Getting started with IBM Tivoli Monitoring Version 6.1 on Distributed environments*, SG24-7143 redbook.

## 2.4.3 Operating system image deployment

It is possible to extract *manually* the package files to generate a customized image to transfer to an operating system image for replication. The technique is similar to the Tivoli Configuration Manager, V4.2 method. The only difference is software distribution is not used to push the install packages.



The install packages are built and then transferred to a pristine operating system image which gets deployed to many systems using a third party method.

Once the operating system is built from the image, the silent install can be leveraged to install the product binaries via the standard silent install mechanism.

Operating system imaging is out of scope for this book. This is an alternate method which can be employed and is another recommended deployment solution.





# Demonstration, proof of concept and small size installation

This chapter describes how to install IBM Tivoli Monitoring, V6.1 and related components for PoC (proof of concept) and demonstration purposes. You can also use this type of installation for small size environments.

The following topics are covered:

- ▶ “DB2 Workgroup Server Edition installation and configuration” on page 60
- ▶ “IBM Tivoli Monitoring, V6.1 components installation” on page 70

## 3.1 DB2 Workgroup Server Edition installation and configuration

Before we install IBM Tivoli Monitoring, V6.1, we need to install a database. The *Tivoli Enterprise Portal Service (TEPS)* requires one Relational Database to store all user data, user IDs, workspaces, links, queries. The *Tivoli Data Warehouse (TDW)* requires another Relational Database to store the historical data. The IBM Tivoli Monitoring V6.1 is shipped with IBM DB2 Workgroup Server Enterprise Server Edition for demonstration and installation purposes, so we are going to install that version. Please refer to *IBM Tivoli Monitoring, Version 6.1.0, Installation and Setup Guide*, GC32-9407, for supported databases and hardware and software requirements.

The following steps describe how to install DB2 Workgroup Server Edition in Windows 2000 and how to setup the required database components.

### 3.1.1 Installing DB2 Workgroup Server Edition

Use the following steps to install the IBM DB2 Workgroup Server Enterprise Server Edition.

1. Log on to the system with the Administrator account.
2. To start the installation, go to the installation image location. In our case this was C:\ITM61\_image\db2\_image.
3. Launch **Setup.exe**.
4. In IBM DB2 Setup Launchpad, click **Install Product**.
5. Click **Next** in DB2 Workgroup Server Edition to start the DB2 Setup Wizard.
6. Read and accept the terms in the license agreement, selecting **I accept the terms in the license agreement**, click **Next**.
7. Select **Typical** and click **Next** in Select the installation type as shown in Figure 3-1.

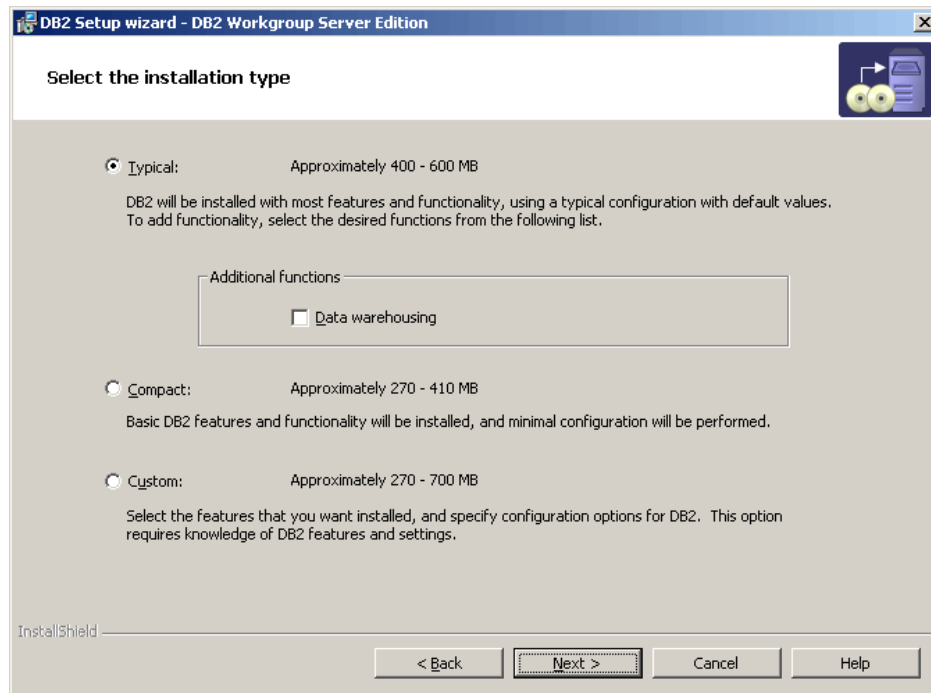


Figure 3-1 DB2 Setup wizard- Select the installation type

8. Type where the DB2 will be installed and click **Next** as shown in Figure 3-2.

**Note:** Here we leave the directory as default: c:\Program Files\IBM\SQLLIB.

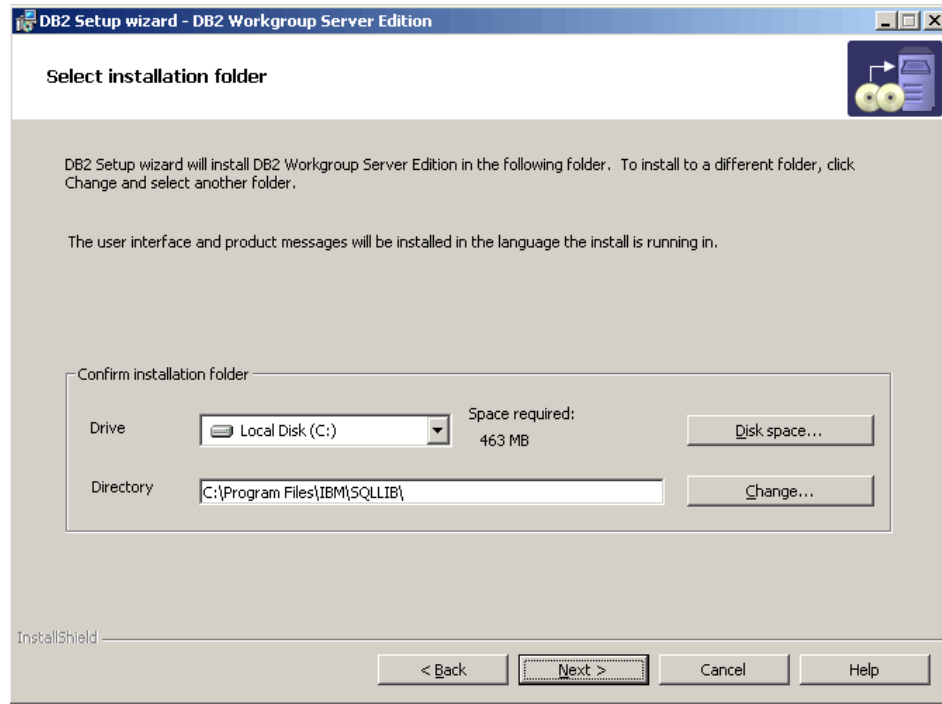


Figure 3-2 DB2 Setup wizard - Select installation folder

9. The DB2 Setup wizard creates a user for DB2 administration purposes. Select **Local user or Domain user account**, in Set user information for the DB2 Administration Server, also select **Use the same user name and password for the remaining DB2 services**. For User Information do the following:
  - a. Domain, leave blank unless you are using domain user.
  - b. User name db2admin;
  - c. Password itm61dgrb;
  - d. Confirm password itm61dgrb;
  - e. Click **Next**.

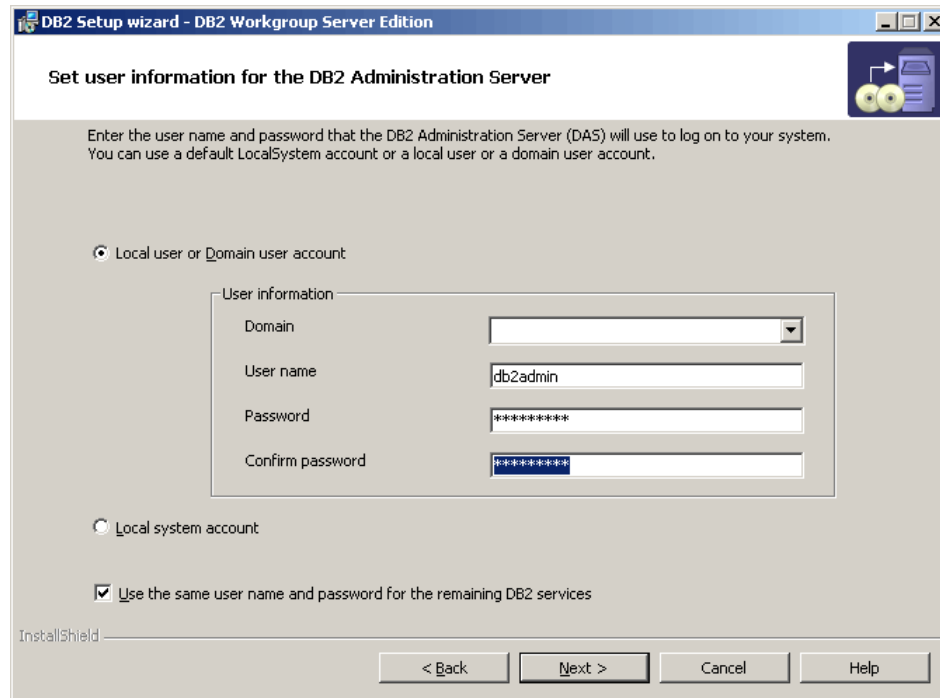


Figure 3-3 Set user information for the DB2 Administration Server

10. Click **Next** in Set up the administration contact list. We did not configure this for that installation.
11. Click **OK** in the Warning window.
12. Click **Next** in Configure DB2 instances.
13. In Prepare the DB2 tools catalog, select **Do not prepare the DB2 tools catalog on this computer** and click **Next**.
14. Select **Defer the task until after installation is complete** in Specify a contact for health monitor notification.
15. The last window shows the current settings, click **Install** to start copying files as shown in Figure 3-4.

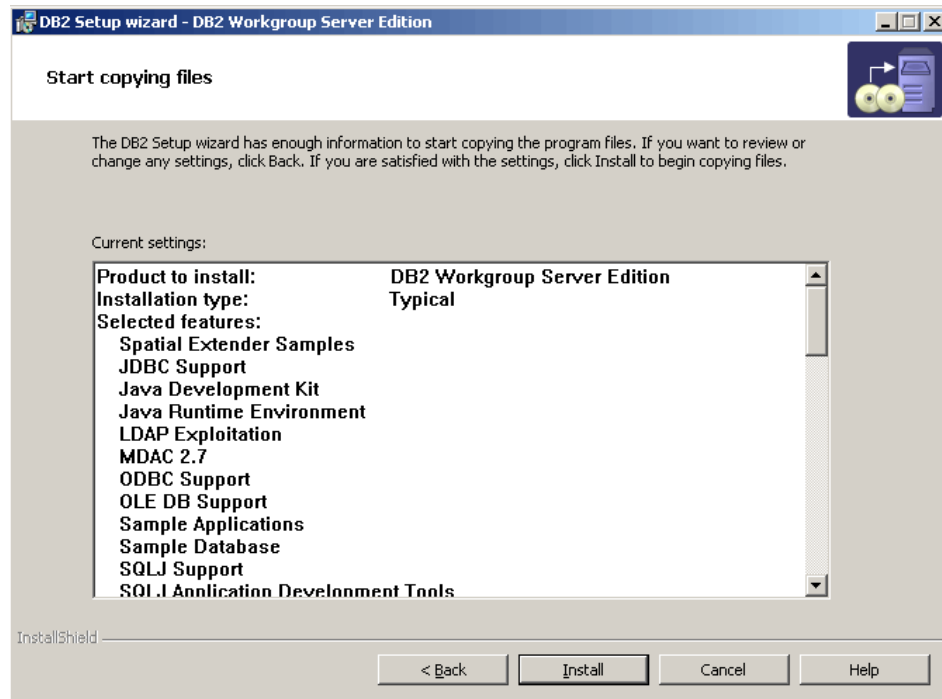


Figure 3-4 DB2 Setup wizard - Start copying files

16. Click **Finish** to complete the DB2 installation.

**Note:** After finishing the DB2 installation, the DB2 Setup starts IBM DB2 First Steps Launchpad and check for DB2 updates. You can defer this task clicking **No** and **Exit First Steps**.

### 3.1.2 Creating the Tivoli Datawarehouse database

In this section, we will show you how to create the database for Tivoli Enterprise Portal Server.

First we should verify if database server is running, checking the DB2 services states.

Click **Start** → **Setting** → **Control Panel** → **Administrative Tools** → **Services**.

Verify that services Started with DB2 are running, DB2 Governor Service and DB2 License Server do not start automatically, these both are Off by default as shown in Figure 3-5.



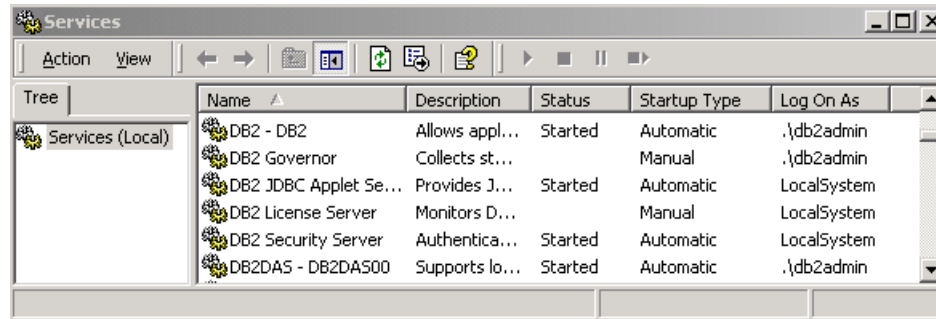


Figure 3-5 Services management console

Now we can create the database. Click **Start** → **Run** type **db2cmd** in the Open box and click **OK**. This opens DB2 command line prompt, where we run DB2 commands.

To create the DB2 database types the following command in DB2 CLP:

```
db2 create database tdw21 using codeset utf-8 territory US
```

This takes some time to create the tdw21 database, the following message shows the database creation ending:

```
DB20000I The CREATE DATABASE command completed successfully.
```

### 3.1.3 Creating the database user

When we created the tdw21 database logged as Administrator account, we gave DB2 administration rights to Administrator account. Now we need to create another account. This account will be used by Tivoli Enterprise Portal Server and Tivoli Data Warehouse for database access.

Use the following steps to create the user:

1. Click **Start** → **Settings** → **Control Panel** → **Administrative Tools** → **Computer Management** expand Local Users and Groups and click **Users**.
2. In the Menu Bar, click → **Action** → **New User...** as shown in Figure 3-6.

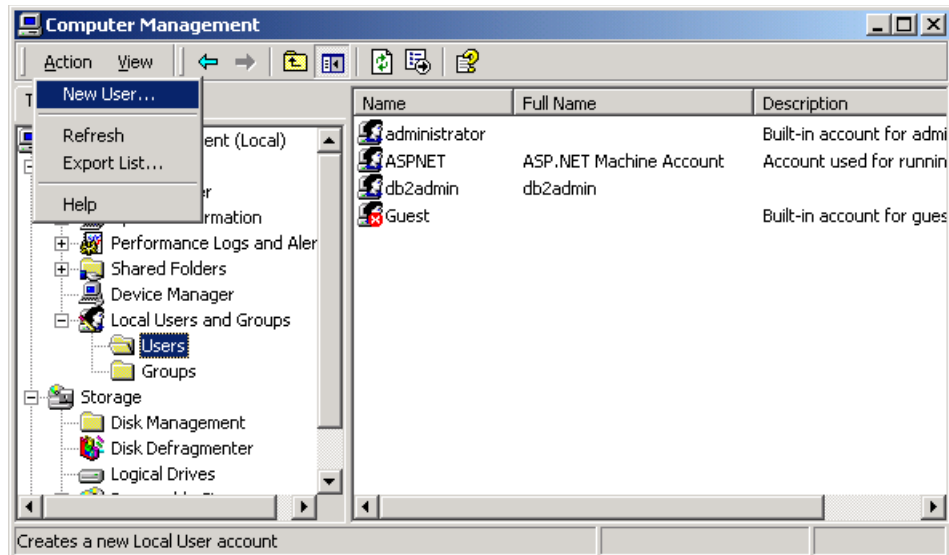
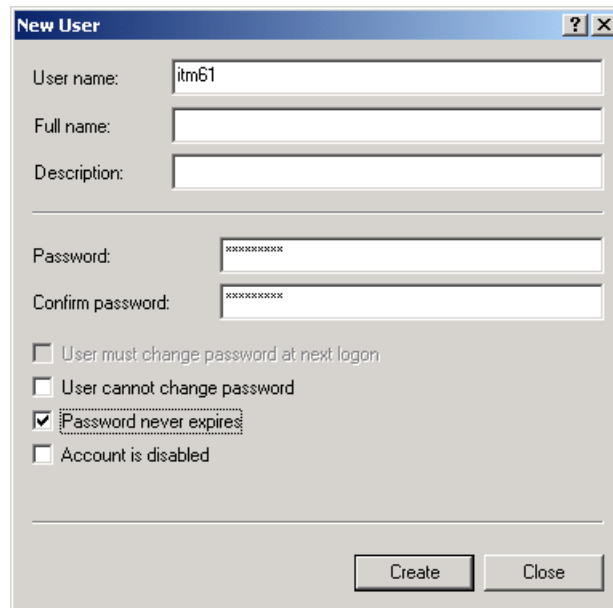


Figure 3-6 Computer Management, adding a New User

3. Fill up the New User information as following:
  - a. **User name** itm61;
  - b. **Password** itm61dgrb;
  - c. **Confirm Password** itm61dgrb.
4. Uncheck the **User cannot change password** and check **Password never expires**.
5. Click **Create** and then **Close** as shown in Figure 3-7.

A Windows-style dialog box titled "New User" with a blue header bar containing a question mark icon and a close button. The dialog contains several input fields and checkboxes. The "User name:" field is filled with "itm61". The "Full name:" and "Description:" fields are empty. The "Password:" and "Confirm password:" fields are filled with "XXXXXXXXXX". Below these fields are four checkboxes: "User must change password at next logon" (unchecked), "User cannot change password" (unchecked), "Password never expires" (checked), and "Account is disabled" (unchecked). At the bottom right are two buttons: "Create" and "Close".

User name: itm61

Full name:

Description:

Password: XXXXXXXXXXXX

Confirm password: XXXXXXXXXXXX

☐ User must change password at next logon

☐ User cannot change password

☒ Password never expires

☐ Account is disabled

Create Close

Figure 3-7 New User interface

Follow these steps to add this user to the Administrator Group:

1. In Computer Management, expand the **Local Users and Groups** then expand **Users**.
2. In the right plane, select the **itm61** user.
3. In the Menu Bar, click **Actions** → **Properties**.
4. Select the **Member Of** tab and click **Add** as shown in Figure 3-8.

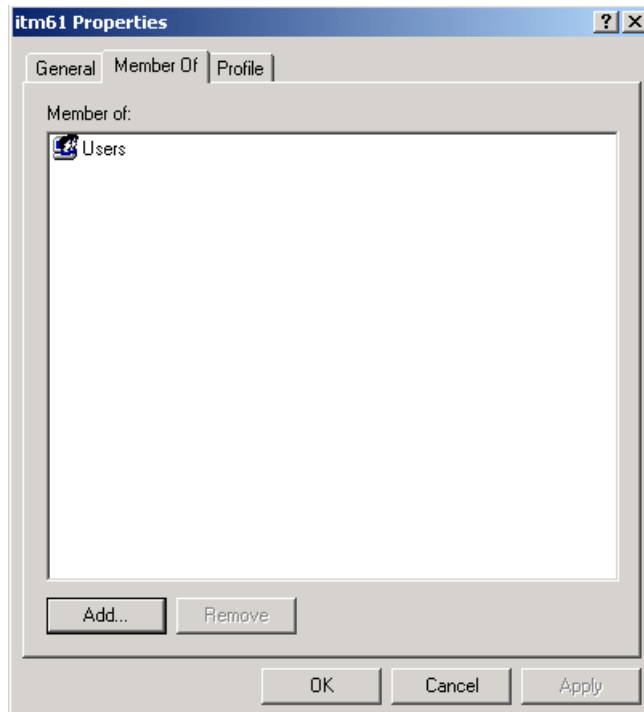


Figure 3-8 Adding Groups to itm61 user

5. Select the **Administrators** in the top pane and click **Add**. Notice that Administrators group goes to the bottom pane (Figure 3-9), click **OK**, and **OK** again to close the itm61 Properties window.

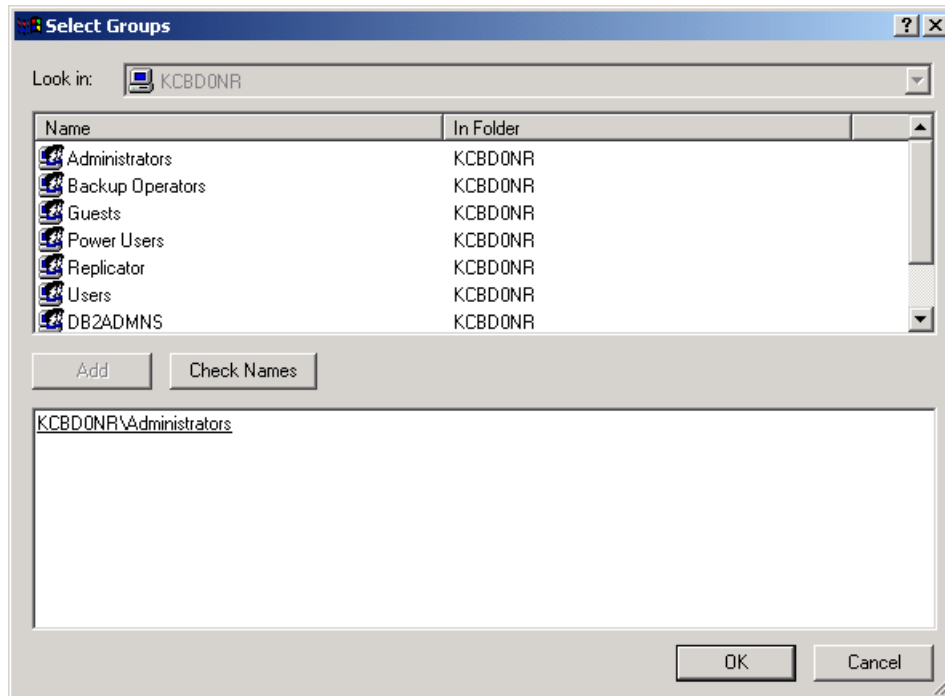


Figure 3-9 Adding Administrators group.

6. Close the Computer Management console.

### 3.1.4 Setting up ODBC connection for Tivoli Data Warehouse Proxy

In order to move data from Tivoli Enterprise Portal Server to Tivoli Data Warehouse, IBM Tivoli Monitoring, V6.1 uses Warehouse Proxy agent. This agent uses an ODBC connection to transfer historical data collected from agents to a database. The next steps show how to create this ODBC connection.

In order to create an ODBC connection, perform the following steps:

1. Click **Start** → **Settings** → **Control Panel** → **Administrative Tools** → **Data Sources (ODBC)**.
2. Select **System DNS** tab and click **Add**.
3. Select **ODBC IBM DB2 DRIVER** and click **Finish** as shown in Figure 3-10.

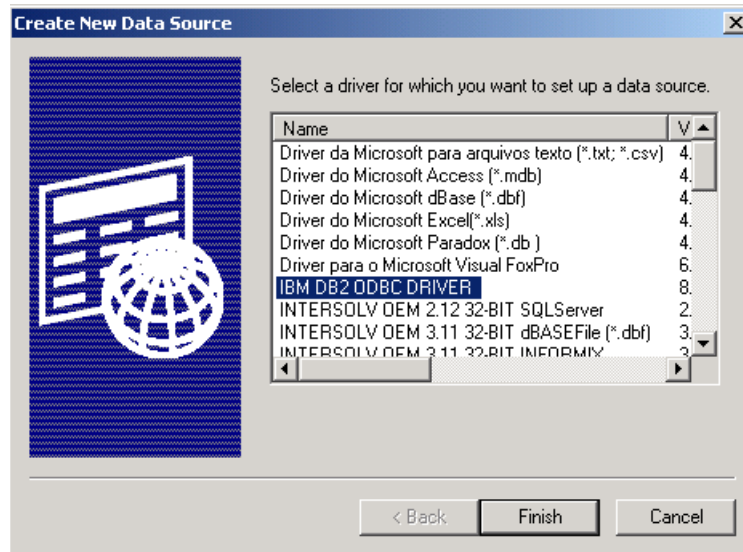


Figure 3-10 Create New Data Source

4. In the ODBC IBM DB2 Driver - Add window, perform the following steps:
  - a. Enter ITM Warehouse in Data source name.
  - b. Select **TDW21** in Database Alias.
  - c. Click **OK**.
5. In order to test the ODBC database connection, you can do the following:
  - a. In the ODBC Data Source Administrator window, select **ITM Warehouse**.
  - b. Click **Configure**.
  - c. Enter User ID and Password (user itm61) in the CLI/ODBC Settings - ITM Warehouse window and click **Connect**.
  - d. A connection test successful message is displayed.
  - e. Click **OK**.
  - f. Click **OK** to close the window.

## 3.2 IBM Tivoli Monitoring, V6.1 components installation

This topic describes the installation process of several components as:

- ▶ Tivoli Enterprise Monitoring Server
- ▶ Tivoli Enterprise Portal Server

- ▶ Tivoli Enterprise Monitoring Agents
- ▶ Tivoli Enterprise Portal

### 3.2.1 Installing IBM Tivoli Monitoring, V6.1

Following the next steps to install IBM Tivoli Monitoring, V6.1:

1. Log on to the system with the Administrator account.
2. Access IBM Tivoli Monitoring, V6.1 installation image. In our case, it was under C:\ITM61\_image\itm61\_image.

**Note:** You can also install IBM Tivoli Monitoring, V6.1 from the CD image.

3. Open Windows folder and launch **setup.exe**. This launch IBM Tivoli Monitoring - InstallShield Wizard.
4. In Welcome to IBM Tivoli Monitoring (Figure 3-11) click **Next**.

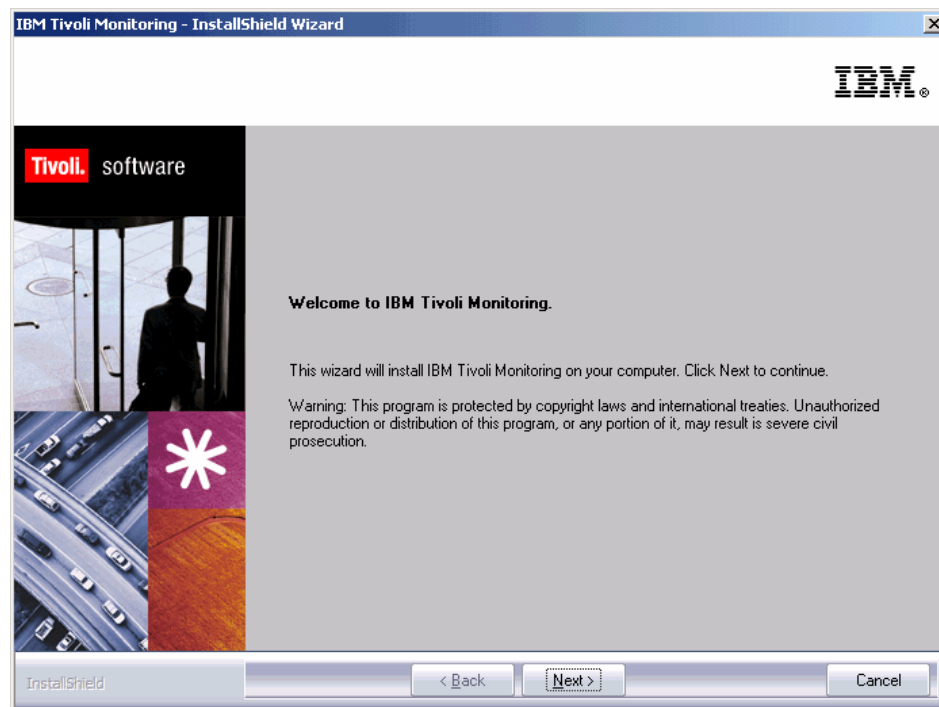


Figure 3-11 Welcome to IBM Tivoli Software

5. In Software License Agreement window, click **Accept** to accept the License Information.

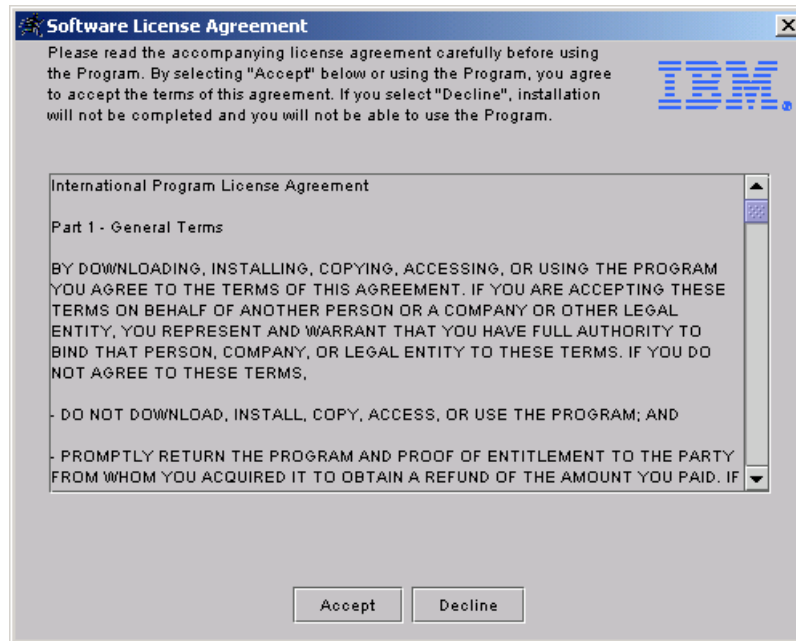


Figure 3-12 Software License Agreement

6. After accepting the License Agreement, IBM Tivoli Monitoring - InstallShieldWizard checks for a valid database installation and existence of a specific version of JRE as shown in Figure 3-13. In our case, the JRE was installed as part of the installation process. Click **Next** to continue with the installation process.

**Note:** If you have the correct JRE installed and a valid database installation, the Figure 3-13 will not show up.



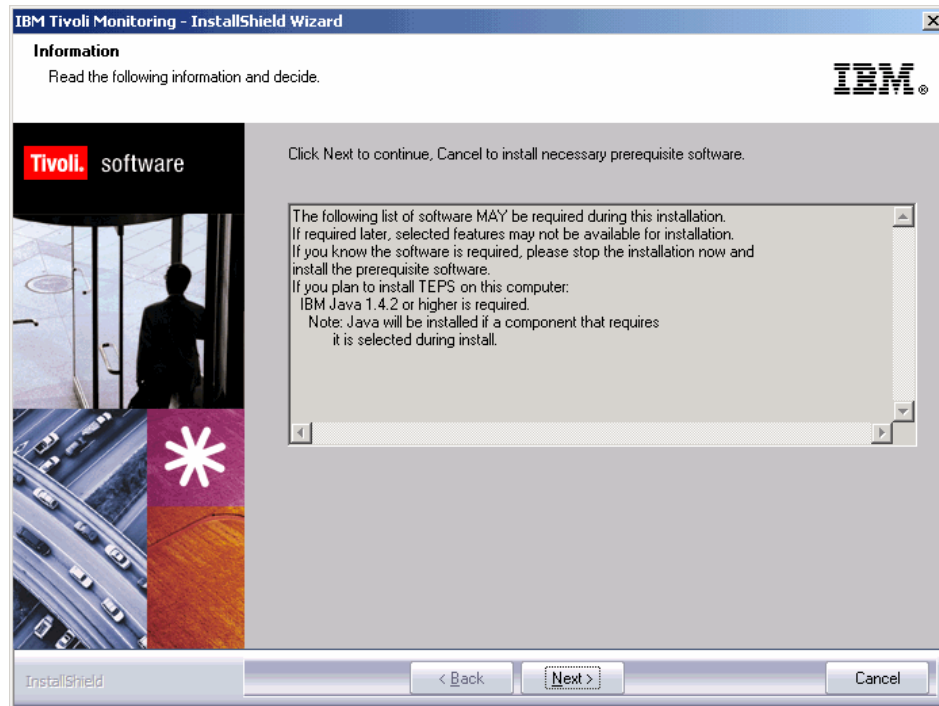


Figure 3-13 Checking necessary prerequisite software

7. In Choose Destination Location (Figure 3-14), accept the default directory selecting **Next**.

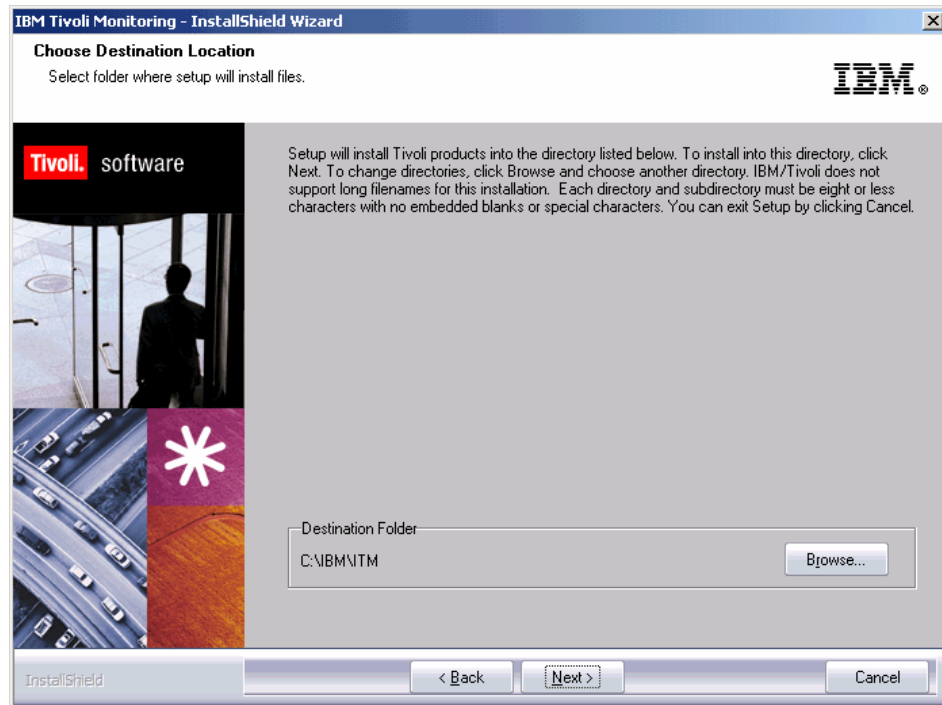


Figure 3-14 Choose Destination Location

8. Now we have to set up a SSL encryption key. Click **Next** to leave the default key IBMTivoliMonitoringEncryptionKey as shown in Figure 3-15.

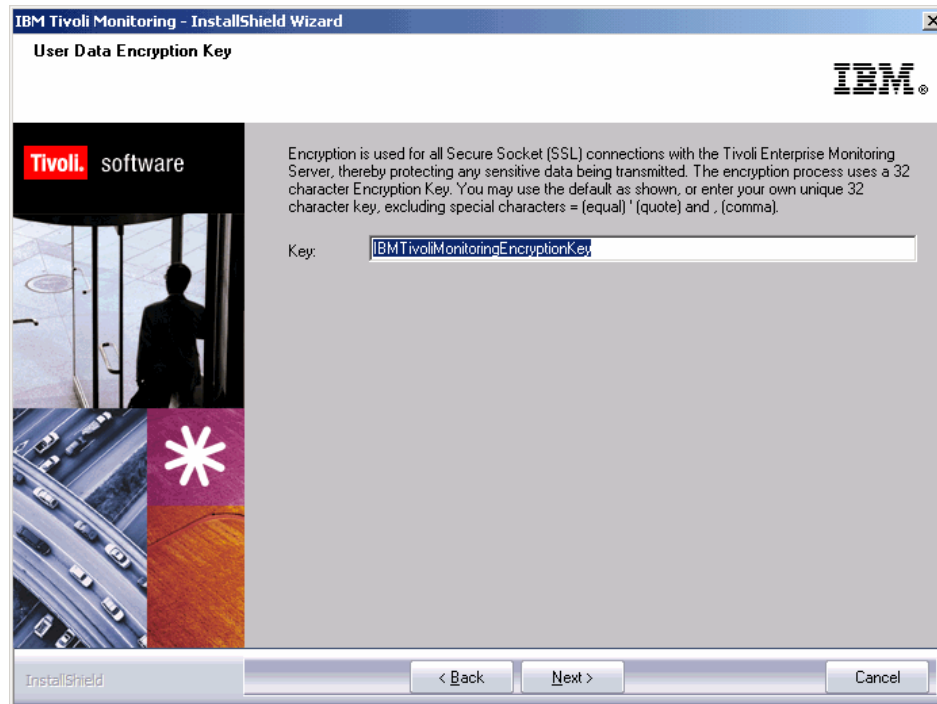


Figure 3-15 User Data Encryption Key

9. Click **OK** in Encryption Key as shown in Figure 3-16.

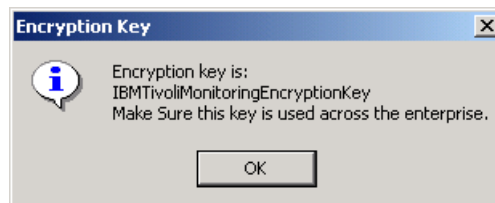


Figure 3-16 Encryption Key

**Attention:** You can change the Encryption Key, but save this information to be used later.

10.) Next screen (Figure 3-17) we select the components that we want to install.

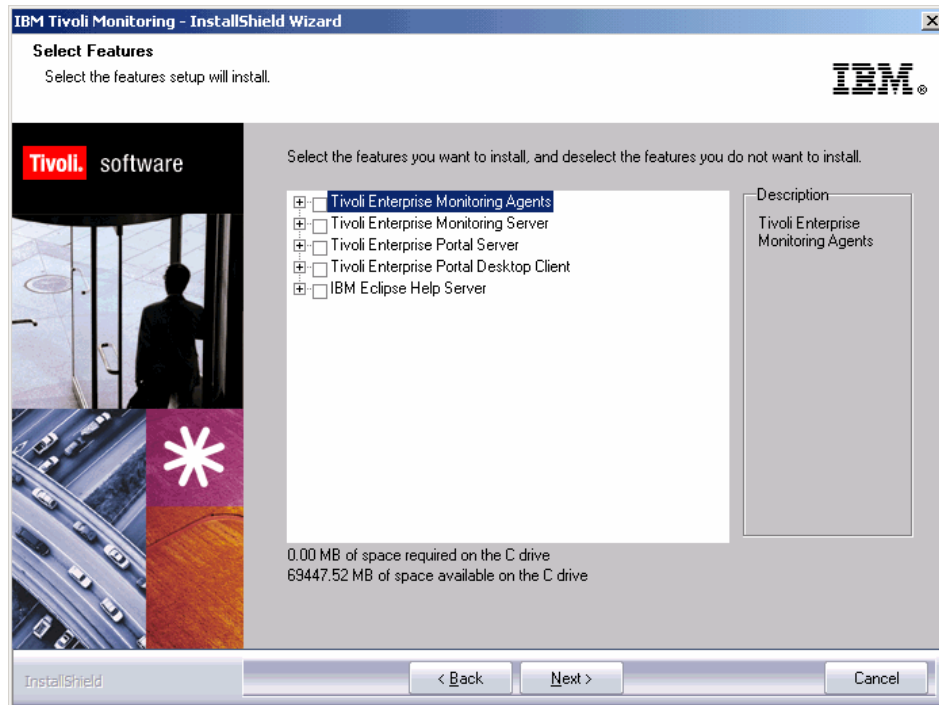


Figure 3-17 Selecting IBM Tivoli Monitoring, V6.1 components

11. Click in plus (+) sign to expand Tivoli Enterprise Monitoring Agents, select **Warehouse Proxy** and **Summarization and Pruning Agent** as shown in Figure 3-18. *Do not* click **Next** yet.

**Important:** Do not check the box next to Tivoli Monitoring Agents, otherwise this will would install *all* the available agents. Tivoli Enterprise Monitoring Agent Framework is selected when we selected the others Agents.

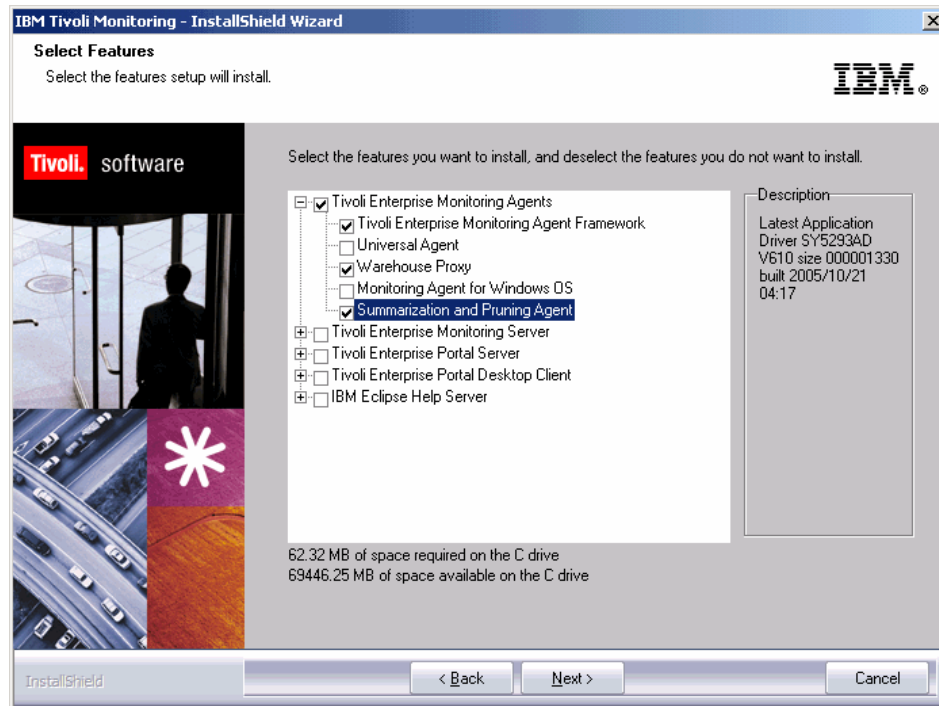


Figure 3-18 Selecting Tivoli Enterprise Monitoring Agents

12. Put a check box mark in **Tivoli Enterprise Monitoring Server**, **Tivoli Enterprise Portal Server** and **Tivoli Enterprise Portal Desktop Client**, as shown in Figure 3-19.

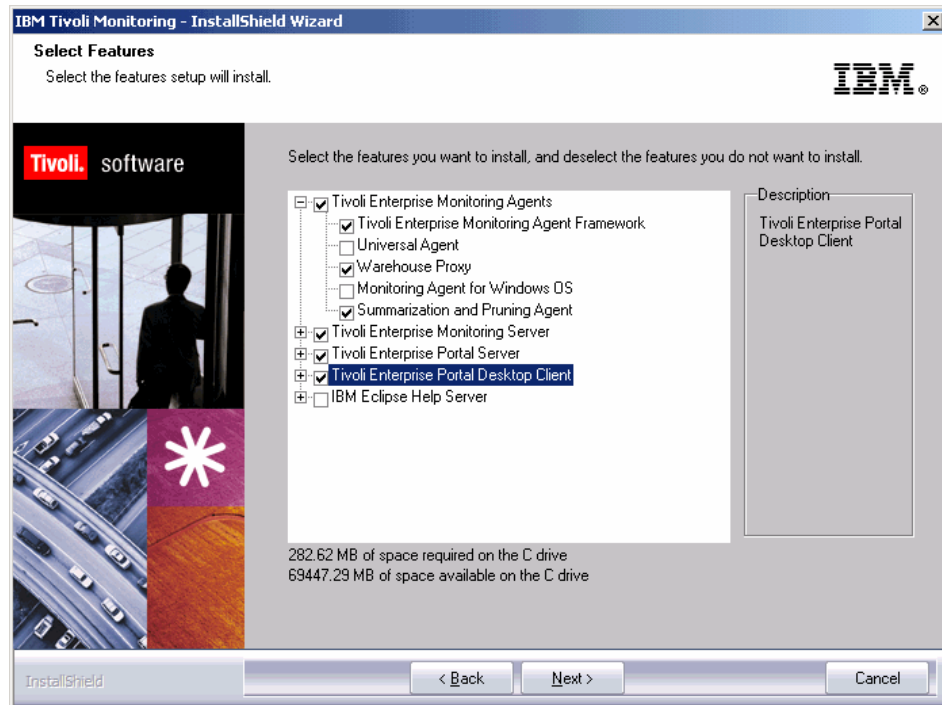


Figure 3-19 Selecting other IBM Tivoli Monitoring Components.

**Note:** Selecting the entire component as we did, we are installing the support for all different agents. Doing that we are enabling the Tivoli Enterprise Monitoring Server to work with data from several kinds of Agents.

13. Select **Next** to continue.

14. In Agent Deployment select **Universal Agent** and **Monitoring Agent for Windows OS** (Figure 3-20) and click **Next**, this allow this agents be deployed to a remote location.

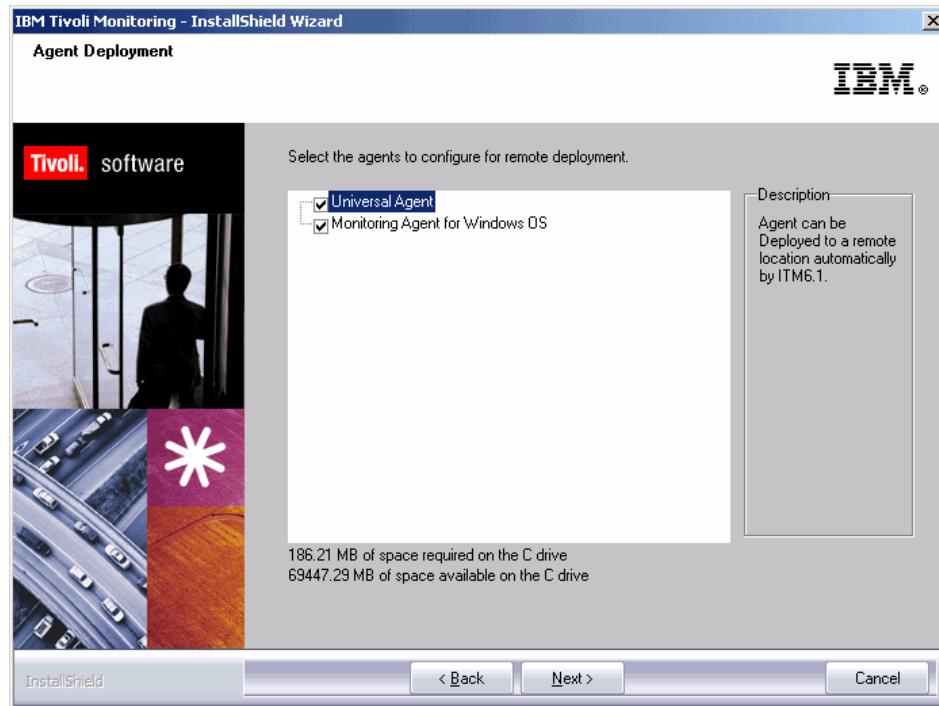


Figure 3-20 Agent Deployment

15. Click **Next** In Select Program Folder.
16. The next window (Figure 3-21) shows the Current Settings, click **Next** in Start Copying Files. The IBM Tivoli Monitoring - InstallShieldWizard installs the IBM Java2 Runtime Environment 1.4.2 and starts to copy files.

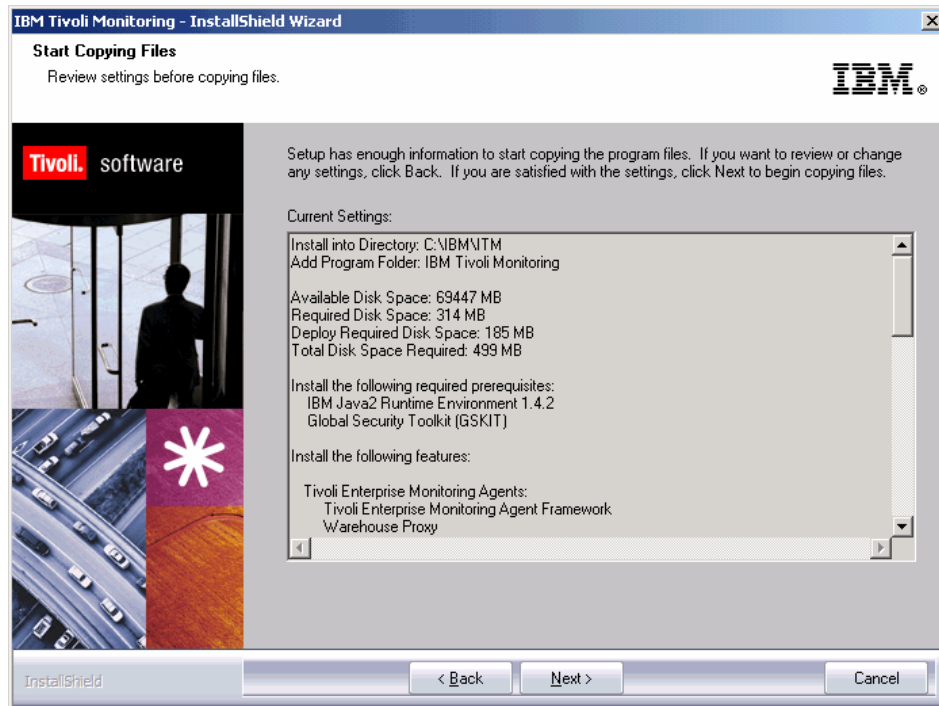


Figure 3-21 Start Copying Files

17. The Setup Type window is prompted (Figure 3-22) when the copy files have finished. Keep all check boxes selected and click **Next** to begin configuring the IBM Tivoli Monitoring components.



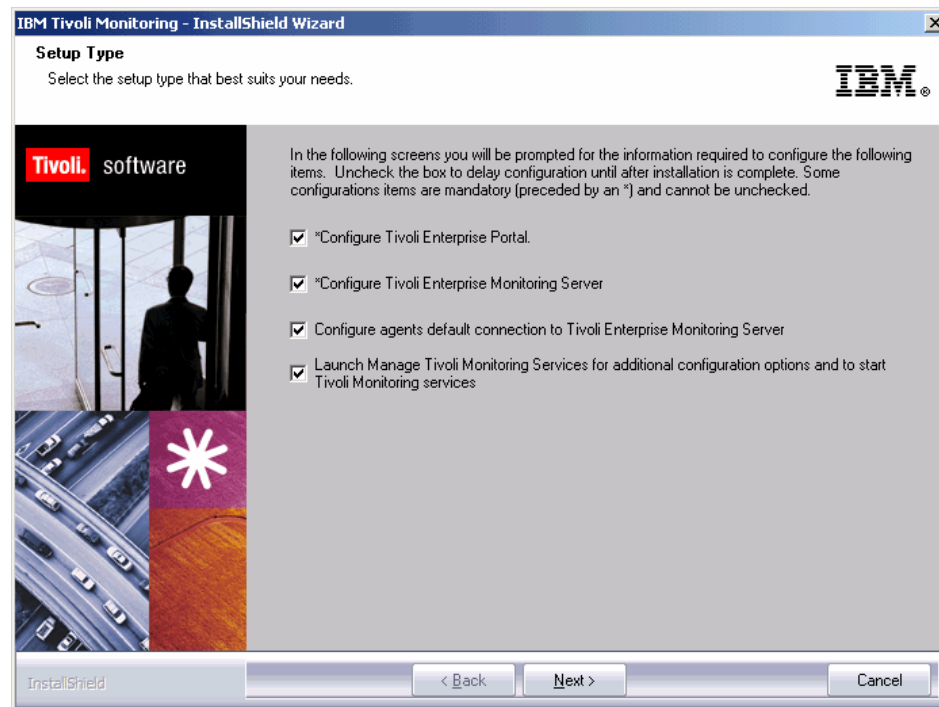


Figure 3-22 Setup Type

18. Click **Next** in Define TEP Host Information (Figure 3-23) to accept the hostname detected.

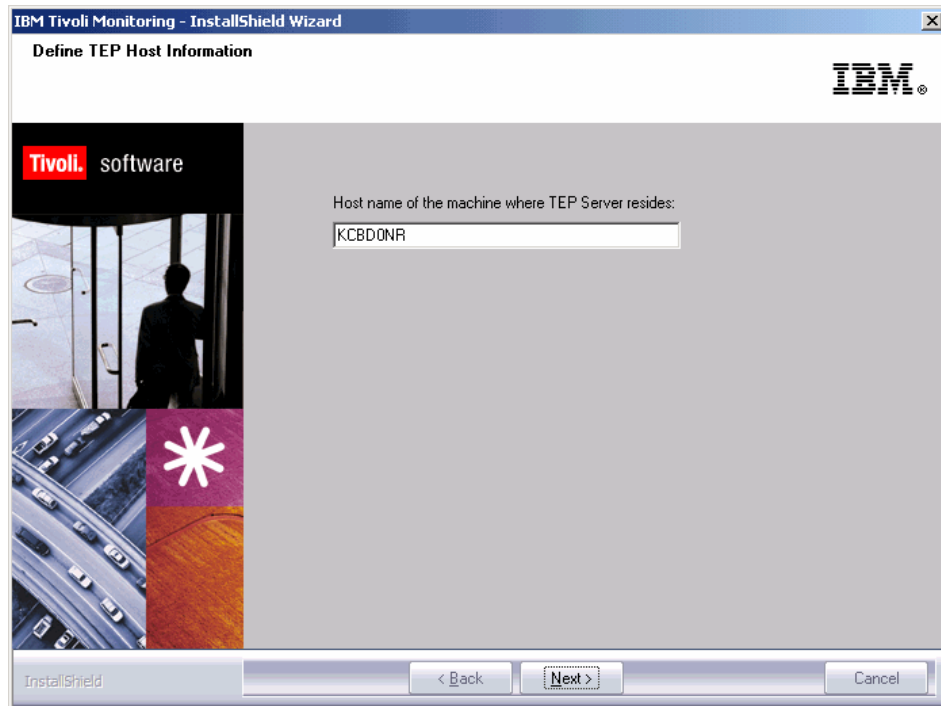
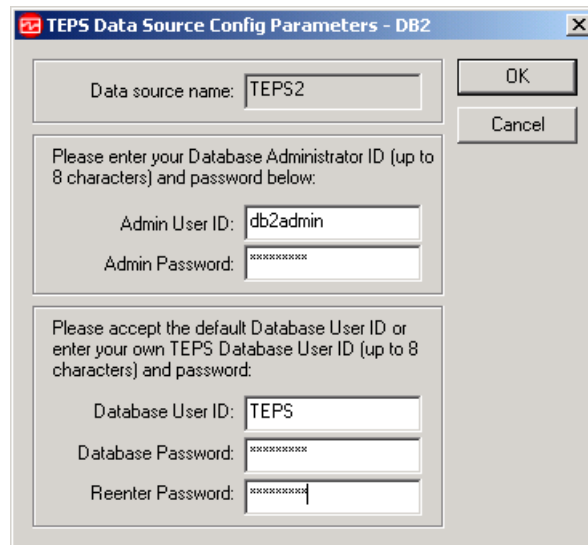


Figure 3-23 Define TEP Host Information

19. Configure the TEPS Data Source Config Parameters - DB2 as shown in Figure 3-24. Fill up the fields as follow:

- a. Admin User ID db2admin;
- b. Admin Password itm61dgrb;
- c. Database User ID TEPS;
- d. Database Password itm61dgrb;
- e. Reenter Password itm61dgrb;
- f. Click **OK**.



The dialog box is titled "TEPS Data Source Config Parameters - DB2". It contains three main sections:

- Data source name:** A text field containing "TEPS2".
- Database Administrator ID and password:** A section with the instruction "Please enter your Database Administrator ID (up to 8 characters) and password below:". It contains two fields: "Admin User ID" with "db2admin" and "Admin Password" with masked characters "XXXXXXXXXX".
- Database User ID and password:** A section with the instruction "Please accept the default Database User ID or enter your own TEPS Database User ID (up to 8 characters) and password:". It contains three fields: "Database User ID" with "TEPS", "Database Password" with masked characters "XXXXXXXXXX", and "Reenter Password" with masked characters "XXXXXXXXXX".

Buttons for "OK" and "Cancel" are located on the right side of the dialog.

Figure 3-24 TEPS Data Source Config Parameters - DB2

20. Click **OK** (Figure 3-24) and **OK** to finish Tivoli Enterprise Portal Server configuration.

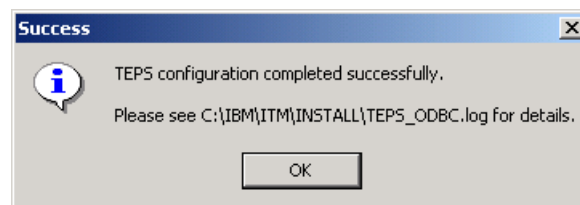


Figure 3-25 TEPS configuration completes successfully

**Attention:** The Tivoli Enterprise Portal Server configuration could take a while to finish, do not panic.

21. In Warehouse ID and Password for TEP Server (), we configure the credentials for Tivoli DataWarehouse database. Type the user created in ODBC connection in page 66, as follows:

- a. **ID** itm61;
- b. **Password** itm61dgrb;
- c. **Confirm Password** itm61dgrb;
- d. Click **Next**.

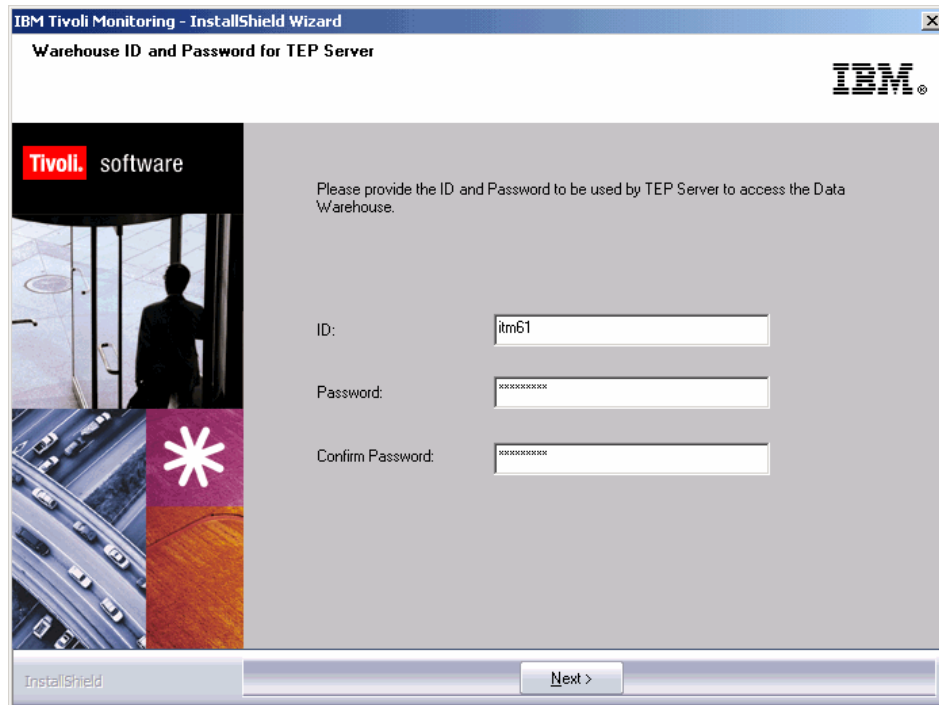


Figure 3-26 Warehouse ID and Password for TEP Server

22. Click **OK** to accept the default values in TEP Server Configuration windows.

**Note:** You can specify whether you want to go through a firewall or not. Also you can specify the communications parameters:

- ▶ **IP.PIPE** uses unsecured TCP communications
- ▶ **IP.SPIPE** uses SSL secure TCP communications
- ▶ **SNA** uses SNA for mainframes environments
- ▶ **IP.UDP** uses unsecured UDP communications

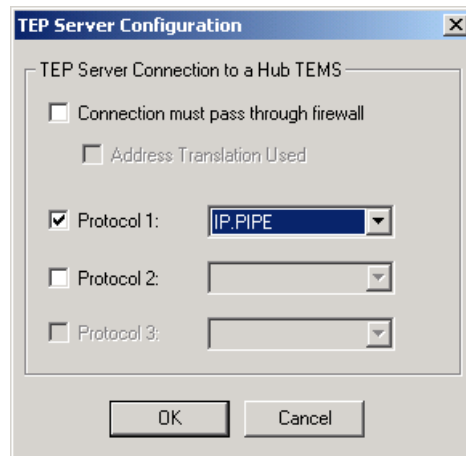


Figure 3-27 TEP Server Configuration

23. Click **OK** to accept the default settings of Tivoli Enterprise Monitoring Server as shown in Figure 3-28.

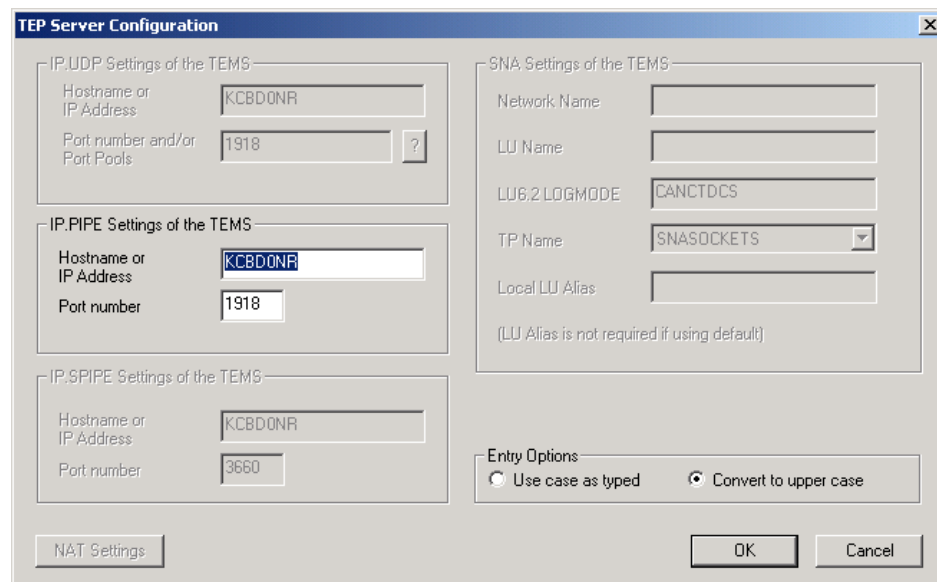


Figure 3-28 TEP Server Configuration

24. Click **Yes** in Do you want to reconfigure the warehouse connection information for the Tivoli Enterprise Portal Server as shown in Figure 3-29.

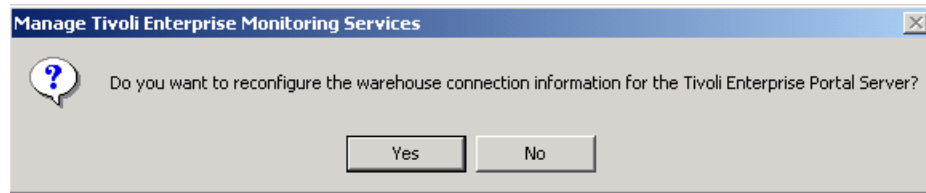


Figure 3-29 Reconfigure warehouse connection information

25. Select **DB2** in Configure DB2 Data Source for Warehouse Proxy as shown in Figure 3-30.

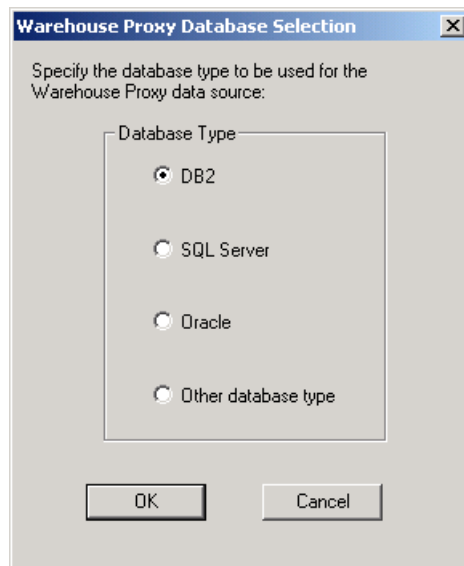


Figure 3-30 Warehouse Proxy Database Selection

26. Fill up the fields as describe below in Configure DB2 Data Source for Warehouse Proxy (Figure 3-31 on page 87)

- a. Data Source Name: ITM Warehouse;
- b. Database Name: tdw21;
- c. Admin User ID: db2admin;
- d. Admin Password: itm61dgrb;
- e. Database User ID: itm61;
- f. Database Password: itm61dgrb;
- g. Reenter Password: itm61dgrb;

h. Click **OK**.

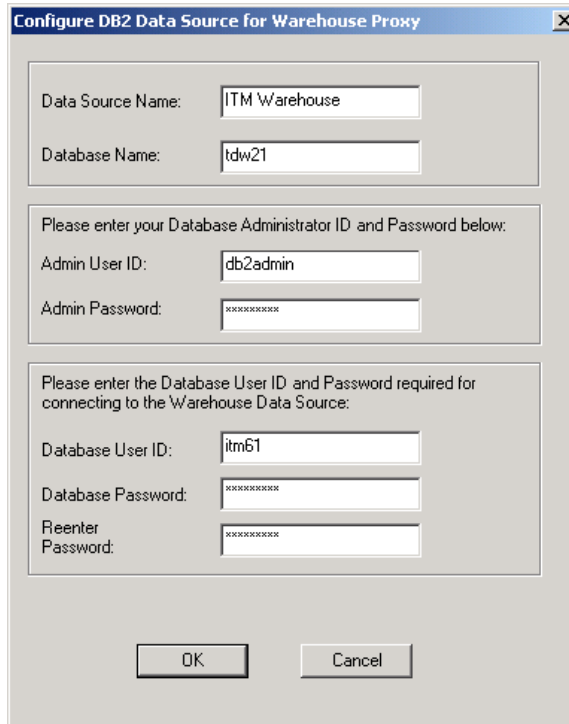
A Windows-style dialog box titled "Configure DB2 Data Source for Warehouse Proxy". It contains three sections of input fields. The first section has "Data Source Name:" with the value "ITM Warehouse" and "Database Name:" with the value "tdw21". The second section is titled "Please enter your Database Administrator ID and Password below:" and contains "Admin User ID:" with the value "db2admin" and "Admin Password:" with a masked password "xxxxxxxx". The third section is titled "Please enter the Database User ID and Password required for connecting to the Warehouse Data Source:" and contains "Database User ID:" with the value "itm61", "Database Password:" with a masked password "xxxxxxxx", and "Reenter Password:" with a masked password "xxxxxxxx". At the bottom are "OK" and "Cancel" buttons.

Figure 3-31 Configure DB2 Data Source for Warehouse Proxy

27. Click **OK** to finish the warehouse data source configuration as shown in Figure 3-32.



Figure 3-32 Manage Tivoli Enterprise Monitoring Services

28. After some time the IBM Tivoli Monitoring builds the Tivoli Enterprise Portal presentation files as shown in Figure 3-33.

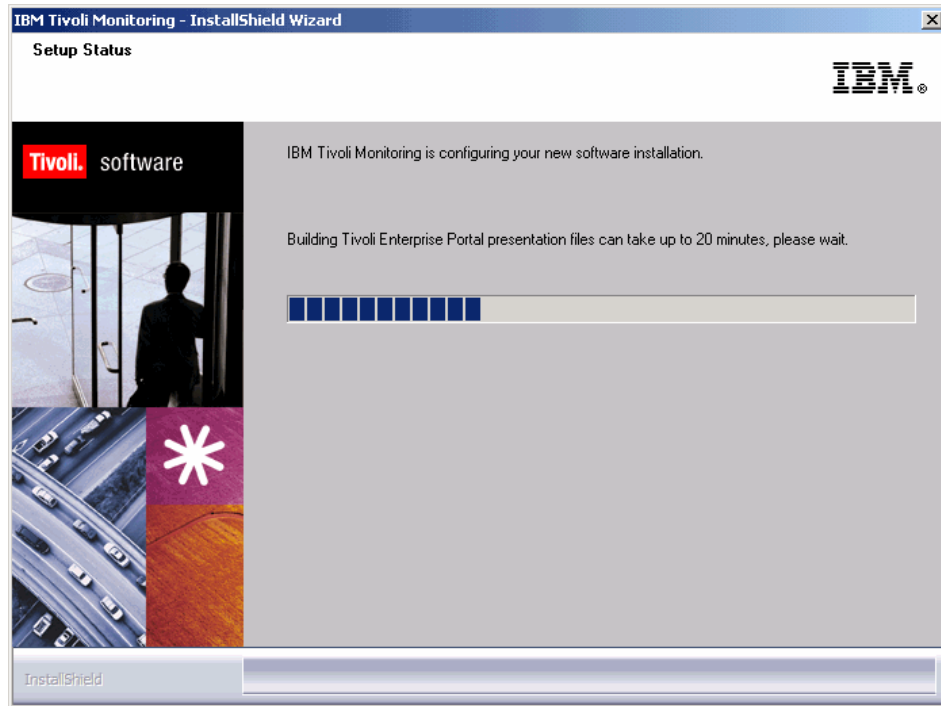
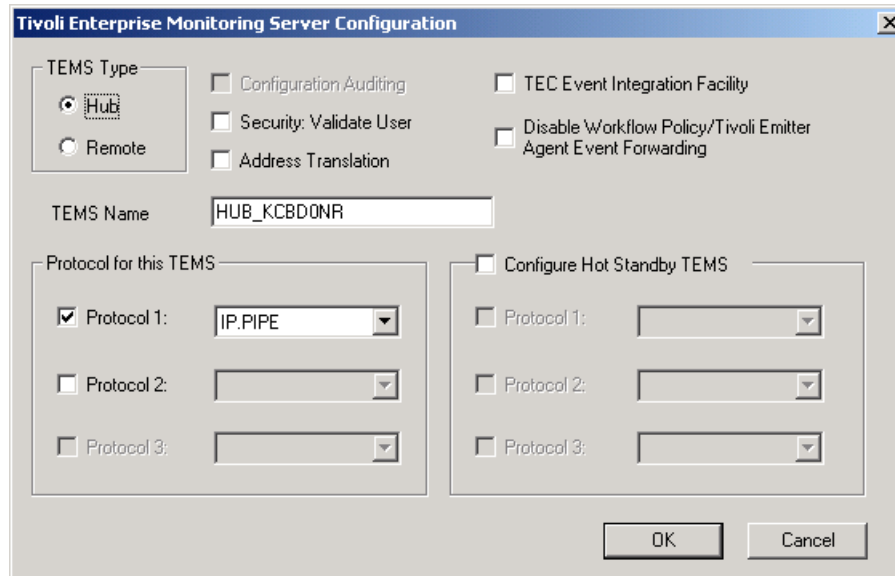


Figure 3-33 Tivoli Enterprise Portal presentation files

29..In the next window, we configure the Tivoli Enterprise Monitoring Server, select the TEMS Type **Hub**, check the **TEMS Name**, check the protocol for this TEMS has **Protocol 1** selected and **IP.PIPE** configured, click **OK** as shown in Figure 3-34.





**Tivoli Enterprise Monitoring Server Configuration**

TEMS Type  
☒ Hub  
☐ Remote

☐ Configuration Auditing  
☐ Security: Validate User  
☐ Address Translation

☐ TEC Event Integration Facility  
☐ Disable Workflow Policy/Tivoli Emitter Agent Event Forwarding

TEMS Name:

Protocol for this TEMS

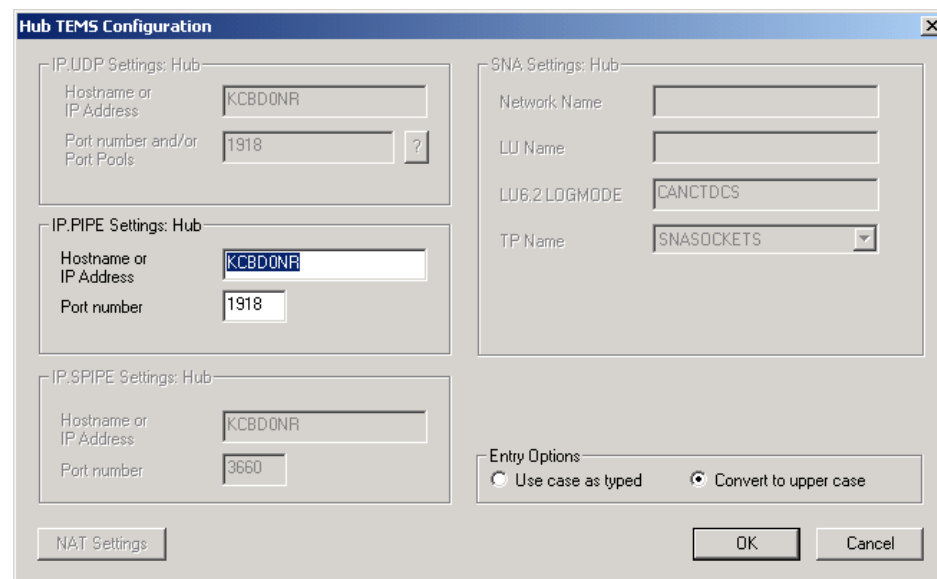
☒ Protocol 1:   
☐ Protocol 2:   
☐ Protocol 3:

☐ Configure Hot Standby TEMS  
☐ Protocol 1:   
☐ Protocol 2:   
☐ Protocol 3:

OK Cancel

Figure 3-34 Tivoli Enterprise Monitoring Server Configuration

30. In Hub TEMS Configuration click **OK** to accept the default configuration for IP.PIPE Settings: Hub as shown in Figure 3-35.



**Hub TEMS Configuration**

IP,UDP Settings: Hub  
 Hostname or IP Address:   
 Port number and/or Port Pools:  ?

IP.PIPE Settings: Hub  
 Hostname or IP Address:   
 Port number:

IP,SPIPE Settings: Hub  
 Hostname or IP Address:   
 Port number:

SNA Settings: Hub  
 Network Name:   
 LU Name:   
 LU6.2 LOGMODE:   
 TP Name:

Entry Options  
☐ Use case as typed ☒ Convert to upper case

NAT Settings OK Cancel

Figure 3-35 Hub TEMS Configuration

31. IN the next step we add application support to the monitoring server, such as the workspaces and situations for agents. Select the TEMS Location as **On this computer** and click **OK** as shown in Figure 3-36.

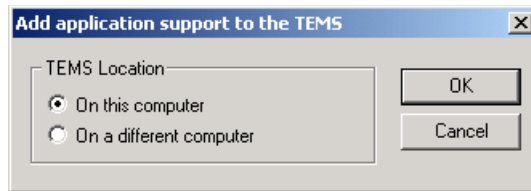


Figure 3-36 TEMS Location

32. Because the monitoring server is currently not running, it is started automatically before the process begins. Click **OK** to start it and perform the application support operation as shown in Figure 3-37



Figure 3-37 Manage Tivoli Enterprise Monitoring Services

33. The next step (Figure 3-38) you select the data that you want to add to the monitoring server. Verify that all available application support is selected and click **OK**.

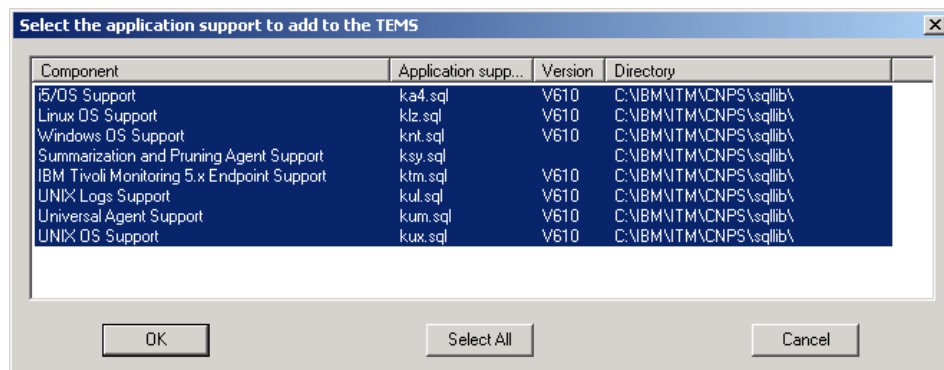


Figure 3-38 Select the application support to add to the TEMS

34. Click **Next** on Application support addition complete box.

35. This step we configure the communication between any IBM Tivoli Monitoring component and the hub monitoring server, verify that **Protocol 1** is selected and configured as **IP.PIPE** and click **OK** as shown in Figure 3-39.

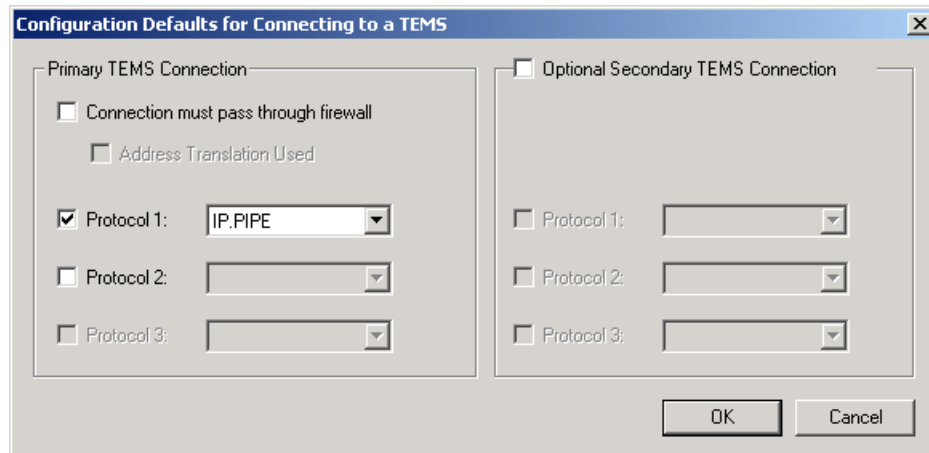


Figure 3-39 Configuration Defaults for Connecting to a TEMS

36. Click **OK** in Configurations Defaults for Connecting to a TEMS to accept the default configurations for IP.PIPE Settings: Hub as shown in Figure 3-39 on page 91.
37. After a while, the IBM Tivoli Monitor - InstallShield Wizard prompts a window informing that services are being recycled and then the final completion screen pops up as shown Figure 3-40. Click **Finish** to ends IBM Tivoli Monitoring, V6.1 components install.

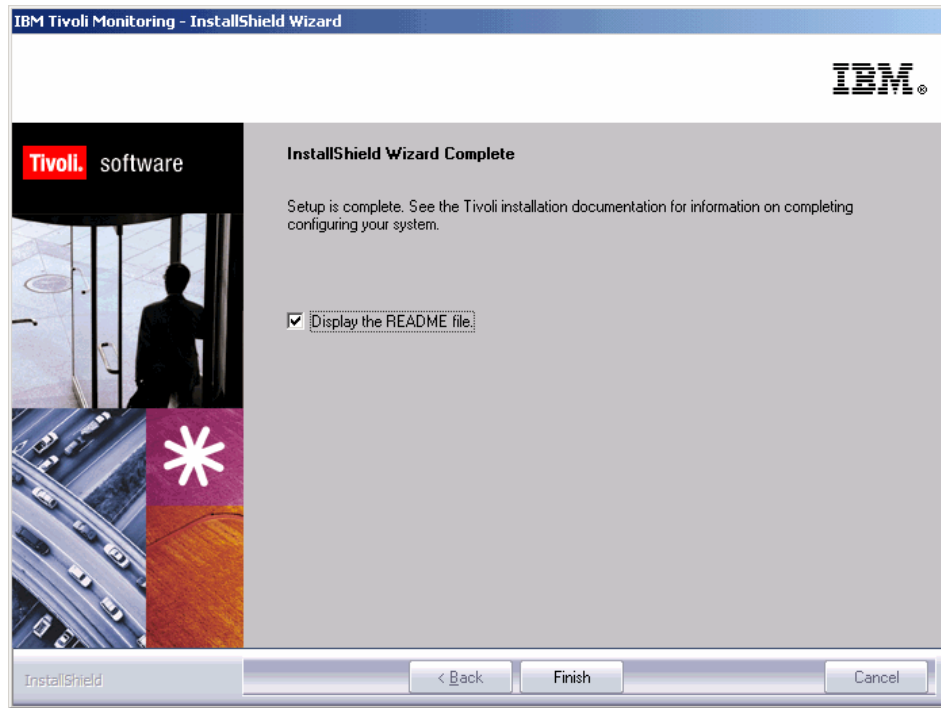


Figure 3-40 InstallShield Wizard Complete

Two text files open, one is the IBM Tivoli Monitoring Readme.txt and Post\_Install\_Info.txt. The most important thing to note is the warning about Java™ 2 v1.4.2, as shown below.

*Example 3-1 Readme.txt*

---

If you will be viewing the help for the TEP Server or TEP Client in Internet Explorer, be sure to clear the "Use Java 2 v1.4.2 for <applet> (requires restart)" checkbox under Tools->Internet Options->Advanced->Java (IBM). Otherwise, you will not be able to enter Index or Search text.

---

Finally, the Manage Tivoli Enterprise Monitoring Services - TEMS Mode - [Local Computer] opens as show in Figure 3-41.

This console allows you work with the IBM Tivoli Monitoring , you can:

- ▶ see the services status;
- ▶ recycle the services;
- ▶ reconfigure the services

- Launch Tivoli Enterprise Portal.

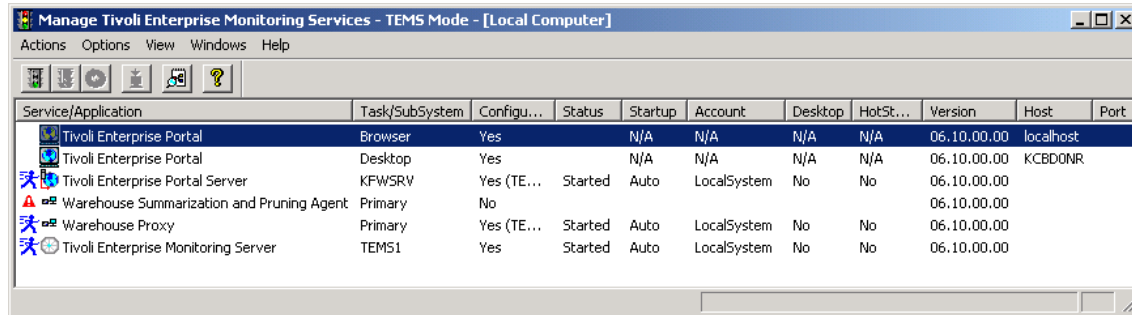


Figure 3-41 Manage Tivoli Enterprise Monitoring Services

**Note:** Warehouse Summarization and Pruning Agent is not configured, the topic shows how to configure it

### 3.2.2 Launching Tivoli Enterprise Portal

In order to check if our installation is running fine, we need to launch Tivoli Enterprise Portal Client, you can launch Tivoli Enterprise Portal Client either as a desktop or Web-based application.

#### Launching Tivoli Enterprise Portal from Internet Explorer

Following the instructions to launch Tivoli Enterprise Portal using a browser.

1. Click **Start** → **Programs** → **Internet Explorer**.
2. Type <http://kcbd0nr:1920/client/client>.
3. Click **Yes** to accept the Warning - Security message as shown in Figure 3-42.



Figure 3-42 The security certificate message

4. In Logon window, for User Credentials use:
  - a. Logon ID sysadmin;
  - b. Password <blank>.

**Note:** Since we do not have security enable, we do not need to enter the password.

5. Click **OK** as shown in Figure 3-43.

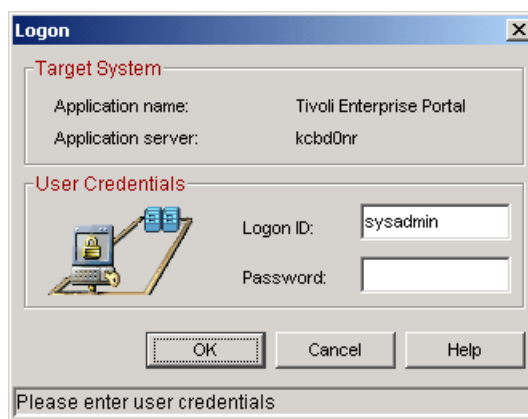


Figure 3-43 Logon window

6. In Security Alert window (Figure 3-44 on page 95), click **Always Accept** to accept the certificate.

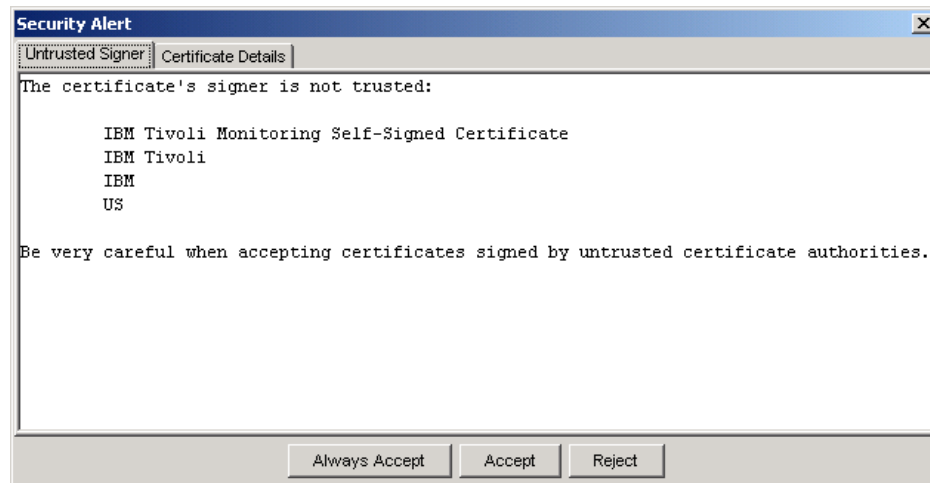


Figure 3-44 Security Alert

We have two Internet Explorer windows: Welcome to IBM Tivoli Monitoring and Tivoli Enterprise Portal. Since we have not configured and installed any agent, you can only see the Enterprise Navigator with no agent running.

7. Click **Exit** to close Welcome to IBM Tivoli Monitoring Window and **File** → **Exit** and **Yes** to close Tivoli Enterprise Portal. You can also close the Internet Explorer.

### Launching Tivoli Enterprise Portal Client desktop application

When we install Tivoli Enterprise Portal Client, it creates a menu item and a desktop icon. We can launch Tivoli Enterprise Portal Client (Figure 3-45) launching its icon or we can go **Start** → **Programs** → **IBM Tivoli Monitoring** → **Tivoli Enterprise Portal**.

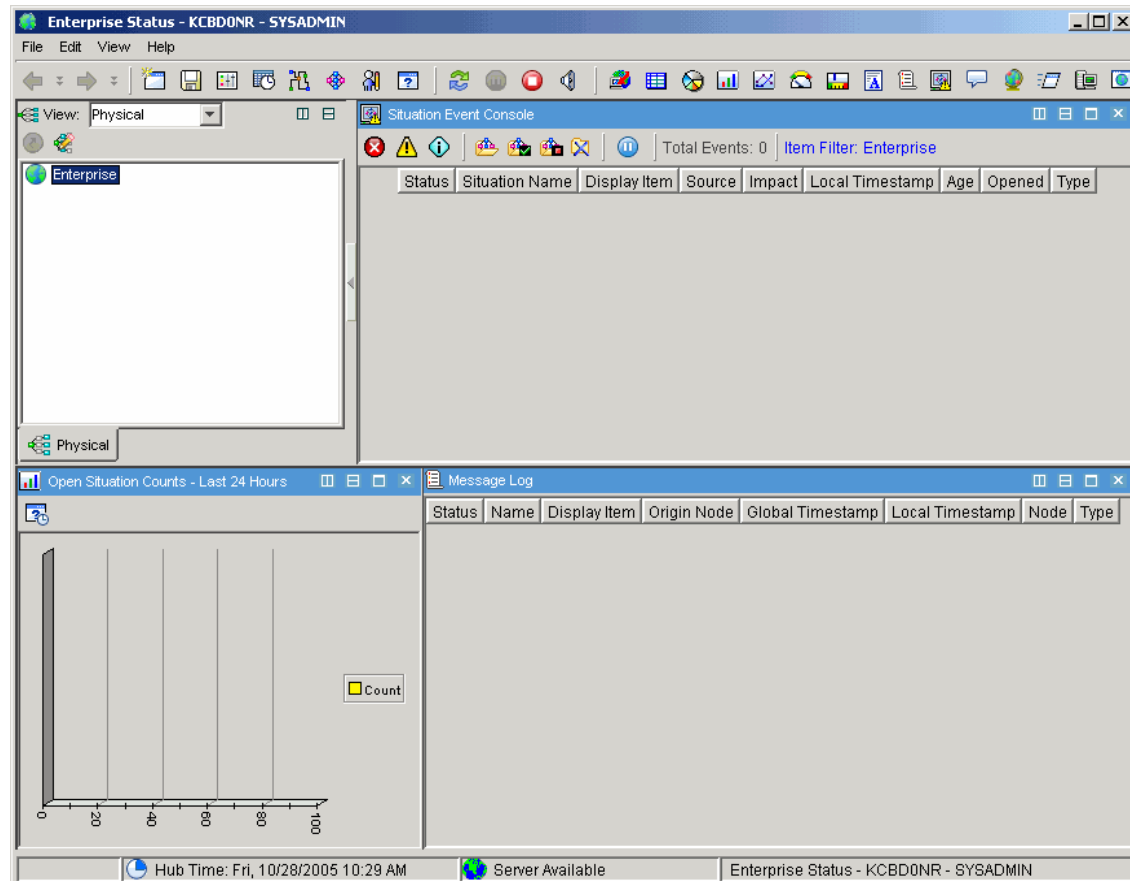


Figure 3-45 Tivoli Enterprise Portal Client Desktop

**Note:** Before you run the client version, you need to install its application from ITM 6.1 image. In the browser version, we just need to have network access and a web browser as Internet Explorer.

### 3.2.3 Configuring Warehouse Summarization and Pruning Agent

The Warehouse Summarization and Pruning Agent moves data from monitoring agents and monitoring server to Tivoli Data Warehouse database. We have already installed the Warehouse Summarization and Pruning Agent. Now, we need configure it.

To configure the Warehouse Summarization and Pruning Agent do the following:



1. Click **Start** → **Programs** → **IBM Tivoli Monitoring** → **Management Tivoli Enterprise Services**.
2. Right Click **Warehouse Summarization and Pruning Agent** and click **Configure Using Defaults** as shown in Figure 3-46.

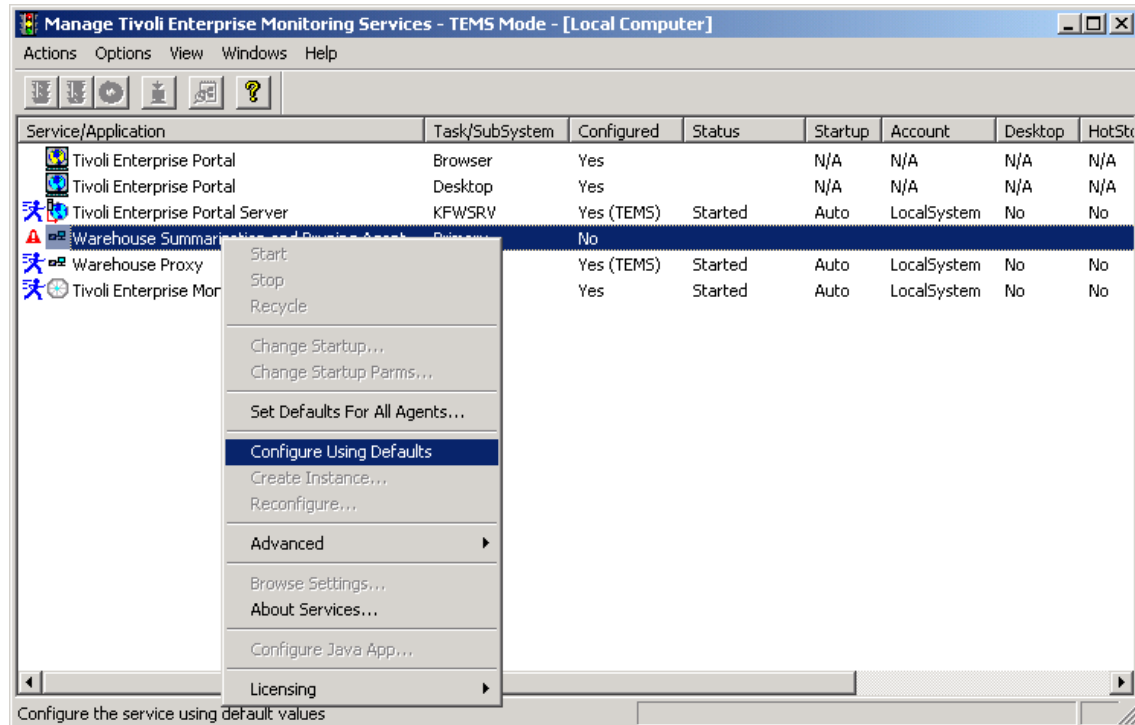




Figure 3-46 Warehouse Summarization and Pruning Agent configuration

3. Click **Yes** in the Would you like to configure this Summarization and Pruning Agent window.
4. In the Source tab of Configure Summarization and Pruning Agent java application, you can see the database settings. You can leave it as is.
5. Click in **Defaults** tab and select **Apply settings to default tables for all agents checkbox**.
6. Click in **Scheduling** tab. In this tab you can specify how often and when the agent runs. Leave it as is.
7. Next click **Work Days**. Here you can differ the working hours and non-working hours, also you can include the vacations settings, leave it as is.
8. Click the last tab **Additional Parameters**, you can use this tab to configure some others database parameters. You can leave it as is.

9. Click **Save** and **Close**.
10. Now that Warehouse Summarization and Pruning Agent is configured we can start it. Right click **Warehouse Summarization and Pruning Agent** and select **Start** as shown in Figure 3-47.

**Note:** The left icon on service side has changed to a  green check symbol but the service is still stopped. When we start the service this icon will change to a blue .

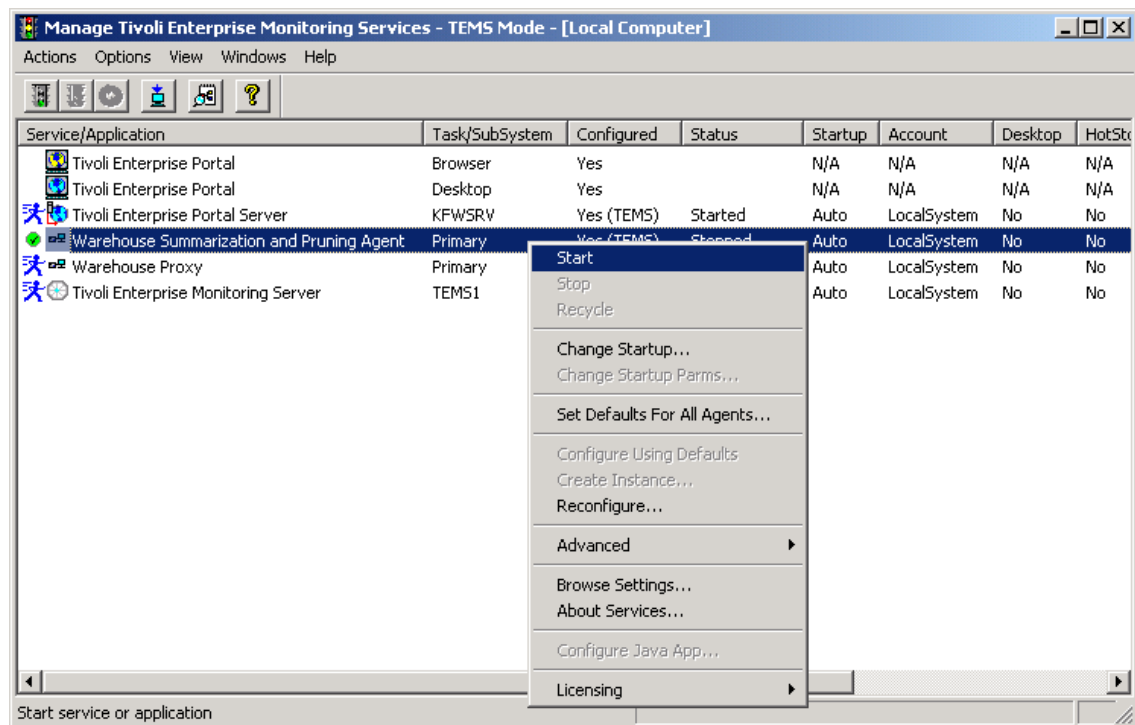


Figure 3-47 Starting Warehouse Summarization and Pruning Agent

So we finished the Warehouse Summarization and Pruning configuration. In the next section, we will configure what components logs data to Tivoli Data Warehouse.

### 3.2.4 Installing IBM Tivoli Monitoring Agents

Following the next steps to install IBM Tivoli Monitoring, V6.1:

1. Log on to the system with the Administrator account.

2. Access IBM Tivoli Monitoring, V6.1 installation image. In our case, it was under C:\ITM61\_image\itm61\_image.
3. Open **Windows** folder and launch **setup.exe**. This launch IBM Tivoli Monitoring - InstallShield Wizard,
4. In Modify, repair, or remove program window (Figure 3-48 on page 99), select **Modify** and click **Next**.

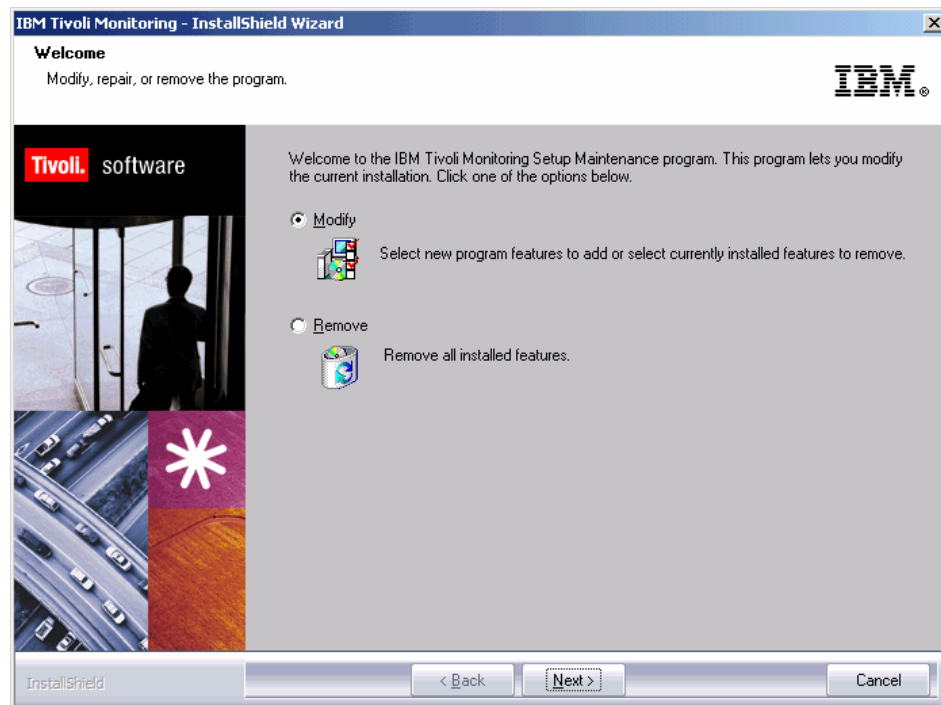


Figure 3-48 Welcome Modify, repair, or remove program

5. Click **OK** in information windows as shown in Figure 3-49 on page 99.



Figure 3-49 Information window.

6. Click + sign to expand the Tivoli Enterprise Monitoring Agents and check **Monitoring Agent for Windows OS** as shown in Figure 3-50.

**Attention:** Do not deselect anything that we installed so far. Deselecting any item uninstall that item.

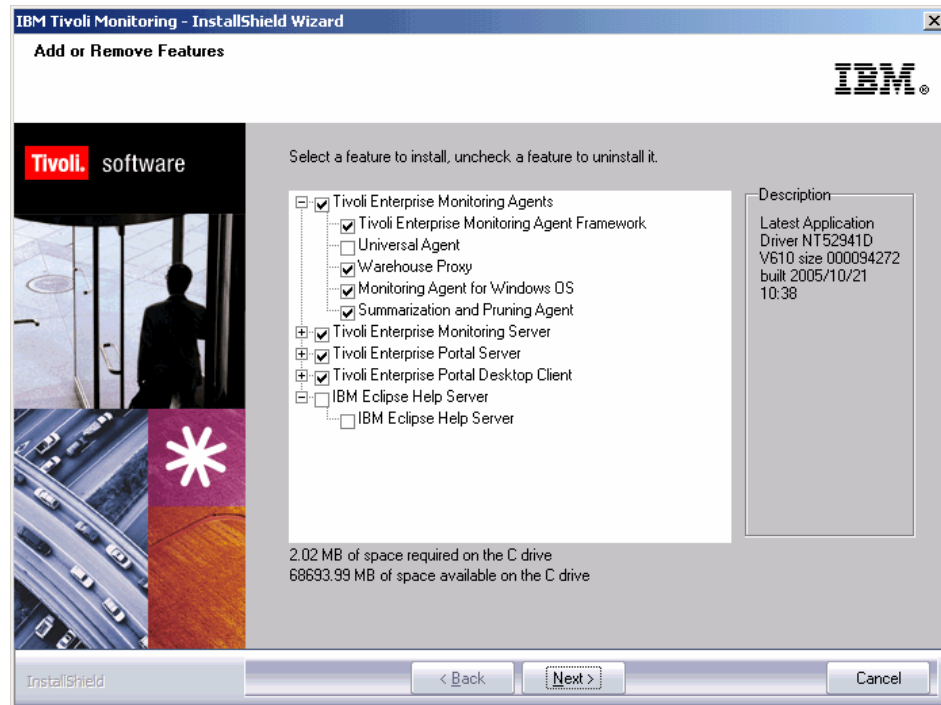


Figure 3-50 Selecting Monitoring Agent for Windows OS

7. Since we have Tivoli Enterprise Monitoring Server installed on that computer, this next step (Figure 3-51 on page 101) is to populate the depot. Leave **Universal Agent** and **Monitoring Agent for Windows OS** selected and click **Next**.

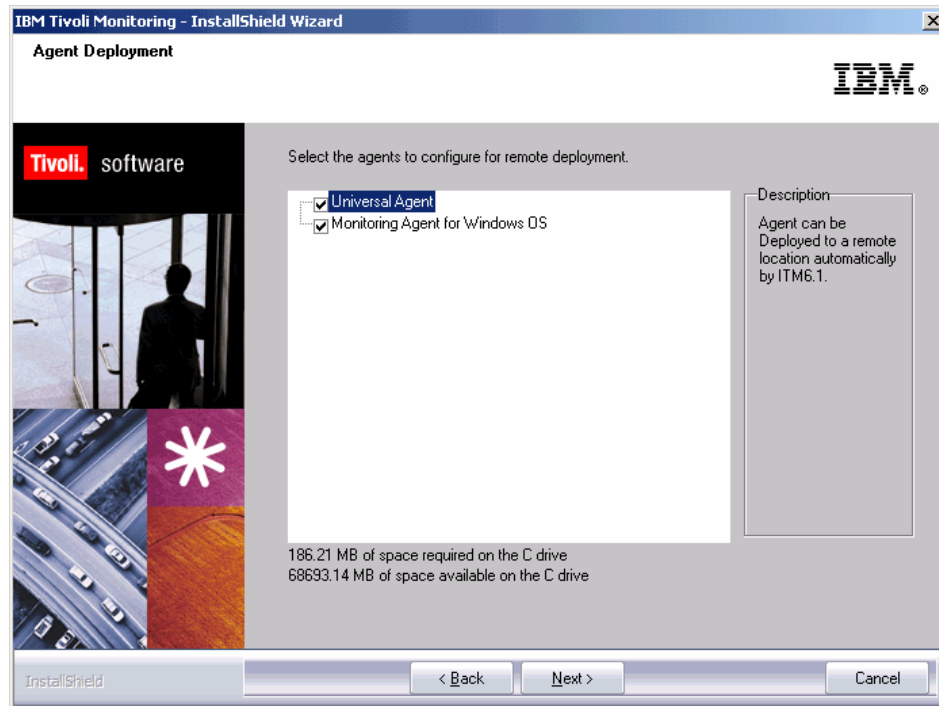


Figure 3-51 Selecting the Agents to depot.

8. Select **Next** in Start Copying Files.
9. In Setup Type window we select only Configure agents default connect to Tivoli Enterprise Monitoring Server and click **Next** as shown in Figure 3-52 on page 102.

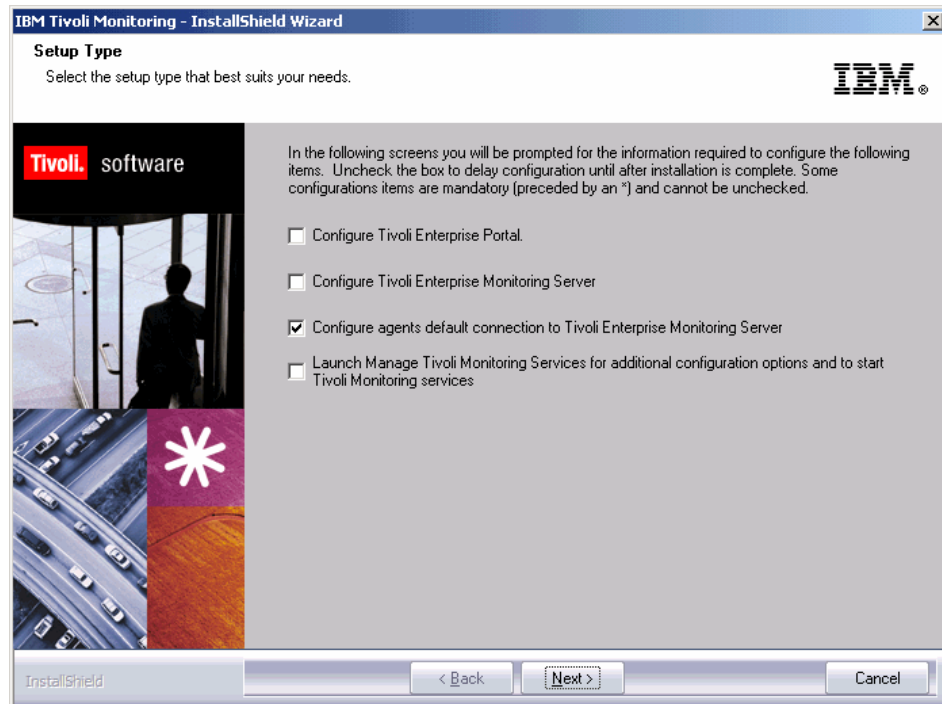


Figure 3-52 Configure agents default connection to Tivoli Enterprise Monitoring Server

10. Click **OK** to accept the TEMS connections configuration and click **OK** to accept Configuration Defaults for Connecting to a TEMS.
11. Click **Finish** to complete the InstallShield Wizard Complete and **Finish** to complete Maintenance Complete.

Now that we finish Tivoli Monitoring Agent installation, we need start Manage Tivoli Enterprise Monitoring Services to see its service status. Click **Start** → **Programs** → **IBM Tivoli Monitoring Manage** → **Tivoli Monitoring Services**. We can see (Figure 3-53) that Monitoring Agent for Windows is installed and Started.

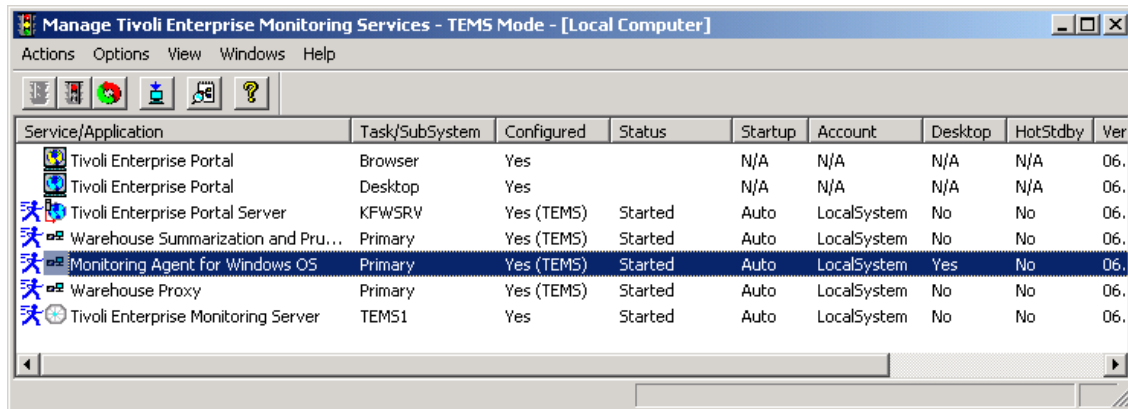


Figure 3-53 Monitoring Agent for Windows OS status

We can also launch (3.2.2, “Launching Tivoli Enterprise Portal” on page 93) Tivoli Enterprise Portal Client to see this Windows OS agent installed. You can navigate through the workspace to see that monitoring is already working.







## Chapter 4.

## Medium and large environment installation

In Chapter 3, “Demonstration, proof of concept and small size installation” on page 59, we have seen how you can install IBM Tivoli Monitoring, V6.1 on one Windows system for demonstration or proof of concept purposes. This type of installation may also be used for a small environment, for example 100 agents or less. For larger size environments, it is better to spread out IBM Tivoli Monitoring, V6.1 server components on more than one systems.

In this chapter, we will cover two different scenarios: Windows TEMS and UNIX TEMS based. We will also give some best practices guidelines in terms of machine sizing and configurations.

The following are covered in this chapter:

- ▶ “Lab environment” on page 106
- ▶ “Installing IBM Tivoli Monitoring, V6.1” on page 110
- ▶ “Uninstalling IBM Tivoli Monitoring, V6.1” on page 228

## 4.1 Lab environment

The following section describes the software and hardware components used during the implementation of IBM Tivoli Monitoring, V6.1 in our lab environment. It also outlines the architecture used to build that environment.

In order to simulate real time environments as much as possible, we setup two different scenarios: Windows TEMS and UNIX TEMS based.

- ▶ Section 4.2.5, “Installing and configuring the scenario-1 environment” on page 117 covers a typical IBM Tivoli Monitoring, V6.1 implementation with two Windows TEMS serves with second server used for Hot Standby
- ▶ Section 4.2.16, “Installing and configuring the scenario-2 environment” on page 218 discusses an implementation with two UNIX TEMS servers, with second server again used for Hot Standby

Apart from the TEMS servers all IBM Tivoli Monitoring, V6.1 components remain the same in both scenarios. You can use one of these scenarios depending on the TEMS platform of your choice.

If you install your TEMS server on one platform (such as Windows), and then decide to migrate it to another platform (such as UNIX), you can follow the instructions given in Section 4.2.17, “Replacing a Hub TEMS server with a new one” on page 225.

### Notes:

- ▶ Both of these configurations can be achieved with one TEMS server instead of two, if you don't plan to use the Hot Standby functionality. For fault tolerance reasons, we recommend that you use the Hot Standby function.
- ▶ It is also possible to use one Windows and one UNIX TEMS server, since Hot Standby functionality also works between Windows and UNIX servers. We have tested this scenario successfully in the Redbook.

### 4.1.1 Hardware and software configuration

Table 4-1 on page 107 shows the hardware and software configuration of our lab environment.

Table 4-1 Lab hardware and software configuration

Server	OS	CPU	Memory	Hard Disk	Main Components	Specific Applications
amsterdam	W2K/SP4	P4 3Ghz	514MB	32GB	TEMA	
berlin	W2K/SP4	P4 3Ghz	2GB	32GB	TEPS	DB2 8.2
cairo	W2K3	Xeon™ 3Ghz	3.5GB	32GB	Hub TEMS	
copenhagen	W2K/SP4	P4 1.8Ghz	1GB	37GB	Remote TEMS	
as20	AS/400®	E Series G170	512MB	68GB	TEMA	
izmir	W2K/SP4	P4 1.8Ghz	260MB	22GB	WPA & SPA	DB2 8.2
lizbon	W2K/SP4	P4 1.8Ghz	391MB	27GB	TEMA	
london	W2K/SP4	P4 3Ghz	512MB	74GB	TEP	
dakar	W2K/SP4	P4 1.8Ghz	260MB	27.9GB	TEMA	Exchange Server 2000
istanbul	AIX 5.3.0	F80 RS6K	1GB	24GB	Event Synchronization	TEC
madrid	AIX 5.3.0	F80 RS6K	1GB	36GB	Event Synchronization	
milan	AIX 5.3.0	F80 RS6K	2GB	222GB	Event Synchronization	
ankara	RHEL4U1	P3 900Mhz	1GB	37GB	TEMA	
edinburg	RHEL4U1	P4 1.8Ghz	512MB	40GB	Remote TEMS	
oslo	SLES9	P4 1.8Gz	1GB	40GB	TEMA	

## 4.1.2 Lab architecture

The following sections describe the architecture on the two different scenarios.

### Lab architecture of scenario-1

Figure 4-1 on page 108 shows the first scenario with two Windows Hub TEMS servers and two Remote TEMS servers, one UNIX server and one Windows server™.

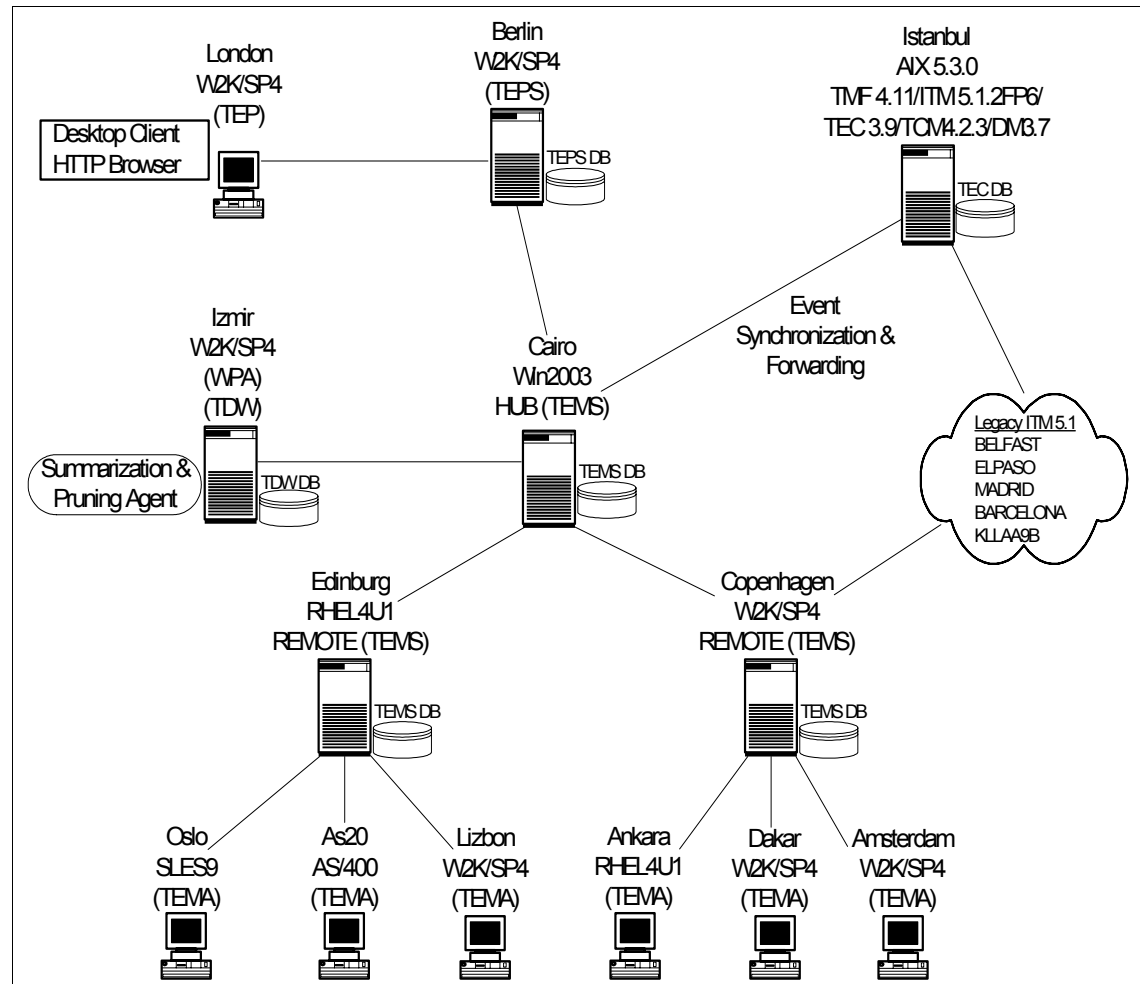


Figure 4-1 Lab architecture of a large scale enterprise scenario-1

**Note:** For simplicity, the Hot Standby node is not shown in the topology diagram. In a large installation, it is strongly recommended to implement the Hot Standby node.

## Lab architecture scenario-2

Figure 4-2 on page 109 on the other side shows the second scenario with two AIX Hub TEMS servers and the same configuration for the rest of the components as scenario-1.

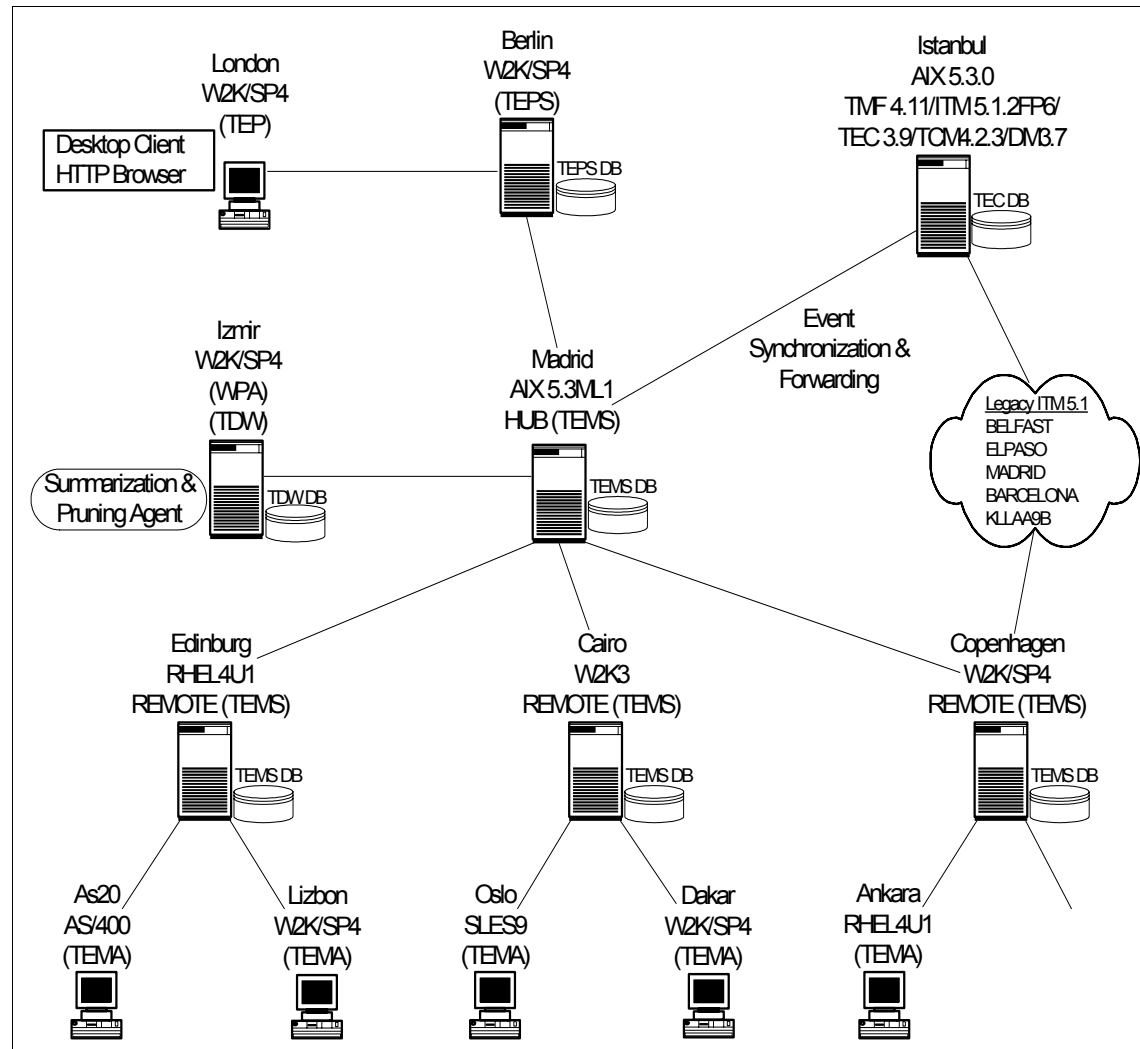


Figure 4-2 Lab architecture for a large scale enterprise scenario-2

This architecture is scalable and can be extended to contain more than 4000 agents. Please refer to Section 2.2.4, “Huge installation - (greater than 4000 agents)” on page 33 for more details on how to extend this architecture to handle more than 4000 agents.

To build the second scenario and reconfigure cairo as a Remote TEMS, we performed the steps described in Table 4.2.17 on page 225.

## 4.2 Installing IBM Tivoli Monitoring, V6.1

This section describes step by step the installation process of the different IBM Tivoli Monitoring, V6.1 components. We will show you examples for both GUI and command line interface (CLI) installation.

The following table provides an overview of the steps required to fully install and deploy an IBM Tivoli Monitoring, V6.1 environment.

Table 4-2 Installation steps

Steps	References
Planning the Installation	"Planing the installation" on page 110
Install the Tivoli Enterprise Monitoring Server	"Installing and configuring a Hub TEMS on a Windows server" on page 117 and "Installing a Hub TEMS on a UNIX server" on page 218
Install the Tivoli Enterprise Remote Monitoring Server	"Installing a Remote TEMS on a Windows and UNIX server" on page 131
Install the Tivoli Enterprise Portal Server.	"Tivoli Enterprise Portal Server - TEPS" on page 135
Install Tivoli Management Agent	"Tivoli Enterprise Monitoring Agent - TEMA" on page 143
Install the portal desktop client on any system where you want to use it	"Tivoli Enterprise Portal - TEP" on page 174
Install Warehouse Proxy	"Installing the Warehouse Proxy Agent" on page 179
Install TEC Event Synchronization	"Event Synchronization installation" on page 196

### 4.2.1 Planing the installation

This section will outline the specific information you need to have ready before starting the installation.

We will discuss the following topics in this section:

- ▶ "Expertise required" on page 111
- ▶ "Naming the monitoring server" on page 113
- ▶ "Creating an IBM Tivoli account on UNIX servers" on page 114
- ▶ "Import the images" on page 115

- ▶ “Host name for TCP/IP network services” on page 115
- ▶ “Use of fully qualified path names” on page 116
- ▶ “File descriptor (maxfiles) limit” on page 116
- ▶ “Hardware and software prerequisites” on page 116

## **Expertise required**

Installing IBM Tivoli Monitoring, V6.1 requires expertise on several areas. In this section, we describe some of the general expertise required to do the above listed tasks. We take each phase of the installation down to the operating system level. In most cases, it is not necessary for one person to have all the expertise, but if the person designated as the Tivoli administrator possesses some knowledge of these different products, it will be easier to deploy and maintain the product.

It is not unusual to have different people with expertise in these technologies all working together. The workload of the Tivoli administrator will be significantly more than the workload of, for example, the DB2 administrator in most cases.

### ***Database administrator***

The database administrator must possess an understanding of how databases work. If there is a database administrator in the organization, they need to possess the needed knowledge to perform most of the work to be done with the chosen database. A thorough knowledge of the RDBMS is not needed in most instances, but will greatly enhance the IBM Tivoli Monitoring, V6.1 experience.

### ***Operating systems administrator***

The UNIX administrator should possess advanced knowledge of administering a UNIX server. The UNIX administrator will be called upon at times to upgrade the operating system software and any other software that is resident on the server. The UNIX administrator must also be able to add and delete users and be able to change permissions on directories. There is also a need to be able to do some debugging at the operating system level and a need to know about TCP/IP, networks, Domain Name System (DNS), host files, file systems, cron jobs, ports, adding additional space for a growing processes, and any other assignments that a UNIX administrator would do in the normal course of business.

The Microsoft Windows administrator should possess the advanced knowledge of administering Microsoft Windows computers, both server classes, such as Microsoft Windows 2000 Servers or Microsoft Windows 2003 Servers, and workstation classes such as Microsoft Windows XP. This administrator will be called upon to keep the operating system software updated and secure. The administrator must be able to give certain security rights to the Tivoli administrator that will allow the software to operate normally.

## 4.2.2 Define the architecture

Chapter 2, “Architecture and planning” on page 15 gives an complete and detailed description on the best practices to define an architecture that fits into your organization. We setup our lab architecture based on those best practices. The two scenarios resulting from those suggestions are described in Figure 4-1 on page 108 and Figure 4-2 on page 109.

**Note:** Although IBM Tivoli Monitoring, V6.1 can be setup using two hubs with different platforms (Windows and UNIX for example), if you are planning to implement the Hot Standby feature, it is advisable-but not mandatory-to have them of the same platform.

## 4.2.3 Creating a deployment plan

Creating a deployment plan is essential to creating and installing an IBM Tivoli Monitoring, V6.1 environment. The basic considerations for creating a deployment plan for a Tivoli environment are provided in *IBM Tivoli Monitoring, V6.1.0 Installation and Setup Guide*, GC32-9407.

At a minimum, you need to gather the following information before installing any software:

- ▶ Base hardware and software requirements for IBM Tivoli Monitoring, V6.1. This information is provided in *IBM Tivoli Monitoring, V6.1.0 Installation and Setup Guide*, GC32-9407, Chapter 3.
  - Whether the computer systems in your distributed network can support this new software, whether these systems can be upgraded to meet your business needs, or whether new systems need to be obtained.
  - Which IBM Tivoli Monitoring, V6.1 components to install on which computer systems in your distributed network to support your business needs and whether they have additional third-party software requirements. This information is provided in 2.1.1, “Platform Support Matrix - IBM Tivoli Monitoring, V6.1 (GA)” on page 22.
- ▶ For each system where you plan to install components of IBM Tivoli Monitoring, V6.1, gather the following information:
  - Name of the monitoring server you are installing or that the agent will connect to
  - Operating system
  - Available memory and available disk space
  - Host name of the system where the product (a monitoring server or one instance of an agent) will execute.



- Whether the monitoring server being installed will be configured as a hub or remote monitoring server
- Hub hostname
- Port number

## Naming the monitoring server

In general, the names selected should be short, but meaningful within the environment. Use the following mandatory guidelines when selecting the names of monitoring servers:

- ▶ Each name must be unique. One name cannot match another monitoring server name for its entire length.
- ▶ Each name must begin with an alpha character. No blanks or special characters (.\$#@.) can be used.
- ▶ Each name must be between 2 and 32 characters in length.
- ▶ Management server naming is case-sensitive on all platforms.

Table 4-3 and Table 4-4 describe the various TEMS configuration on our 2 environments:

*Table 4-3 Scenario-1 lab TEMS description*

Monitoring server	Hostname	Architecture	Description
HUB_HELSINKI	helsinki	W2K3	TEMS Hub
HUB_CAIRO	cairo	W2K3	TEMS Hub
REMOTE_COPENHAGEN	copenhagen	W2K	TEMS Remote
REMOTE_EDINBURG	edinburg	Redhat 4	TEMS Remote

*Table 4-4 Scenario-2 lab TEMS description*

Monitoring server	Hostname	Architecture	Description
HUB_MADRID	madrid	AIX F80	Hub TEMS
HUB_MILAN	milan	AIX F80	Hub TEMS
REMOTE_CAIRO	CAIRO	W2K3	Remote TEMS
REMOTE_COPENHAGEN	copenhagen	W2K	TEMS Remote
REMOTE_EDINBURG	edinburg	Redhat 4	TEMS Remote

## Creating an IBM Tivoli account on UNIX servers

We created an IBM Tivoli account for installing and maintaining the installation directory. For best performance, follow these guidelines:

- ▶ You can use any valid name. You can install the IBM Tivoli Monitoring software as the root user on UNIX, but you do not have to. If you do not install IBM Tivoli Monitoring, V6.1 as root, you must use the following procedure to create the user and set correctly the permission. We created a user called *itmuser* in *itusers* group. IBM recommends using the Korn shell for your IBM Tivoli account; however, you can use any shell that is shipped with the UNIX operating system.
  - a. Create the *itusers* group using the following procedures  
For Linux, Solaris, and HP-UX computers, run the following command:  

```
groupadd itusers
```

  
For an AIX computer, run the following command:  

```
mkgroup itusers
```
  - b. Create the *itmuser* user belonging to *itusers* group; *itusers* will be the primary *itmuser* group:  
For AIX, Solaris and Linux computers run the following command to create the *itmuser* account  

```
useradd -g itusers -s /usr/bin/ksh itmuser
```
- ▶ Use the same user to install all components.
- ▶ If you are using NFS or a local file system, you should establish your installation directory according to the guidelines used in your environment.

**Note:** IBM Tivoli products do not support third-party vendor shells such as BASH and TCSH.

Once the user properly created, use the following procedure to set the permissions:

- a. Set the CANDLEHOME directory. You better set it in the *itmuser* user profile.  

```
export CANDLEHOME=/opt/IBM/ITM
```
- b. Run the following command to ensure that the CANDLEHOME environment variable correctly identifies IBM Tivoli Monitoring installation directory:  

```
echo $CANDLEHOME (default is /opt/IBM/ITM)
```

**Note:** Running the following steps in the wrong directory can change the permissions on every file in every file system on the computer.

- c. Change to the directory returned by the previous step:

```
cd $CANDLEHOME
```

- d. Run the following command to ensure that you are in the correct directory:

```
pwd
```

- e. Run the following commands:

```
chgrp itmusers .  
chgrp -R itmusers .  
chmod o-rwx .  
chmod -R o-rwx .
```

**Important:** If you did this operation after the agent installation, run the following command to change the ownership of additional agent files: `bin/SetPerm` and select the option: All of the above to set the proper permission on all installed agent.

## Import the images

Import the IBM Tivoli Monitoring, V6.1 images to the server where you will perform the installation

You can create a separated file system where you will download the images and install IBM Tivoli Monitoring, V6.1. To install IBM Tivoli Monitoring, V6.1 on Windows system, create a separate drive other than the C: drive (or the drive where the operating system reside).

## Host name for TCP/IP network services

TCP/IP network services such as NIS, DNS, and the `/etc/hosts` file should be configured to return the fully qualified host name (for example: `hostname.ibm.com`). Define the fully qualified host name after the dotted decimal host address value and before the short host name in the `/etc/hosts`.

Execute the following command line from the TEMS:

```
nslookup hostname
```

where `hostname` is hostname of the servers in the IBM Tivoli Monitoring, V6.1 environment (for example the second Hub TEMS, the Remote TEMS, the TEPS, and so on.). Once the command line successfully performed on those servers, proceed with the reverse lookup executing the following command:

```
nslookup -querytype=PTR
```

At the prompt, enter the IP address of the server previously tested. Fix any inconsistencies contacting your System or Network Administrator before proceeding to the next steps.

### Use of fully qualified path names

Because of the wide variety of UNIX operating systems and possible user environments, use fully qualified path names when entering a directory during the installation process (no pattern-matching characters). IBM scripts use the Korn shell - when a new process or shell is invoked, use of symbolic links, environmental variables, or aliases can potentially cause unexpected results.

### File descriptor (maxfiles) limit

The monitoring server requires a minimum of 256 file descriptors (maxfiles) for the operating system. For the monitoring server to function properly, we set the maximum file descriptor (MAX\_FILES parameter of the configurable kernel parameter) to 256.

To determine the number of per process file descriptors (maxfiles), run one of the following commands:

```
sysdef | grep maxfiles  
ulimit -a
```

For AIX computers, run the following command:

```
ulimit -d
```

Notice that the *-d* option specifies the size of the data area, in number of KB. If the settings returned are less than 256 MB, increase the maxfiles limit to 256 MB.

If 256 MB is not sufficient (for example, as evidenced by the malloc failures in the monitoring server log file), contact IBM Software Support regarding a Memory Upgrade Patch. This patch enables you to use multiple user segments of 256 MB. This patch must be applied to the KDSMAIN module at every product or maintenance installation.

### Hardware and software prerequisites

All information regarding software and hardware prerequisites can be found in the *IBM Tivoli Monitoring, V6.1.0 Installation and Setup Guide*, GC32-9407. Read carefully this document to check if your environment complies with the IBM Monitoring 6.1 prerequisites.

## 4.2.4 Backup strategies

This section describes several of the backup strategies that should be deployed when using IBM Tivoli Monitoring, V6.1. Without a good backup strategy, the enterprise can be vulnerable to outages of undeterminable lengths of time.

### Tivoli backups

If the IBM Tivoli Monitoring, V6.1 is being installed in an already existing Tivoli server, we suggest you to backup the Tivoli database just in case, even though IBM Tivoli Monitoring, V6.1 does not update the Tivoli Framework database. There are two ways to back up the Tivoli server and Managed Nodes. The **wbkupdb** command is available to back up the pertinent files in the \$DBDIR directory. This will not back up any custom scripts that you might have or anything outside of \$DBDIR. But, this is sufficient to restore a Tivoli server back to running state if there is some corruption in the database.

### System-level backups

The other method is to do a system level backup, or back up everything under the ../Tivoli directory. This will capture all the scripts that were built for tasks and any other custom scripts that might be in that environment.

If you are installing IBM Tivoli Monitoring, V6.1 in a TMR, make sure that you have a “clean” system before backing up. Use the **wchkdb** command with the appropriate parameters of either -ux for interconnected Tivoli regions or -u for all managed nodes, and -ut for just the Tivoli server. A “clean” **wchkdb** command result will allow better backup and restore capabilities.

One of the steps that is almost always forgotten is to check the backups for validity. Too often there are backups that are not validated, and when necessary, they might not be good candidates for restore purposes. A good plan is to have a machine that you can use to restore the backup. Then, use a set of tests to make sure that the backup is valid. If it is not, debug the problem to make sure that you can back up successfully. One debugging tip is to back up individual Managed Nodes and not the whole Tivoli region at a time. If there is a failure, you can see which Managed Node has the failure and further debug just that Managed Node.

## 4.2.5 Installing and configuring the scenario-1 environment

This section will describe the different IBM Tivoli Monitoring, V6.1 components installation and configuration on an Windows Hub TEMS environment.

### Installing and configuring a Hub TEMS on a Windows server

The following sections provide detailed information on how to install a Hub TEMS on a Windows server, and perform the initial configuration.

Use the following steps to install the hub monitoring server on a Windows computer

1. Launch the installation wizard by double-clicking the **setup.exe** file on the installation media.
2. Click **Next** on the welcome window.

**Note:** If you are running Windows 2003 or Windows XP and have security set to check the software publisher of applications, you might receive an error stating that the **setup.exe** file is from an unknown publisher. Click on **Run** to disregard this error message and continue.

3. Click **Accept** to accept the license agreement, as shown in Figure 4-3.

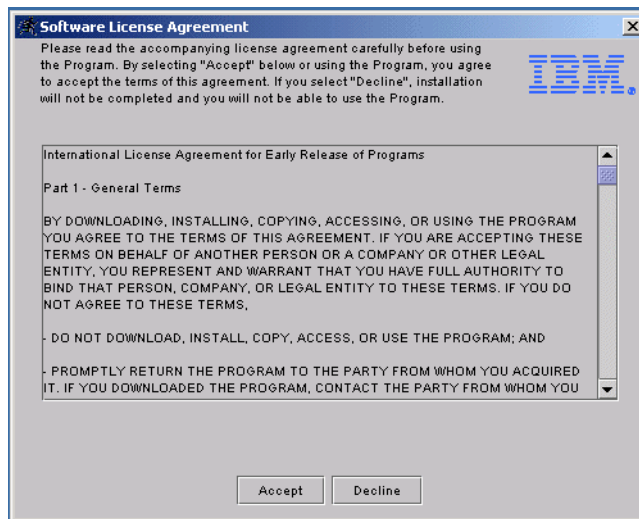


Figure 4-3 License agreement windows

4. Choose the directory where you want to install the product. The default directory is C:\IBM\ITM. You are strongly recommended to install IBM Tivoli Monitoring, V6.1 in a different drive from the operating system one. Click Next. Figure 4-4 on page 119 shows the windows with the installation directory.

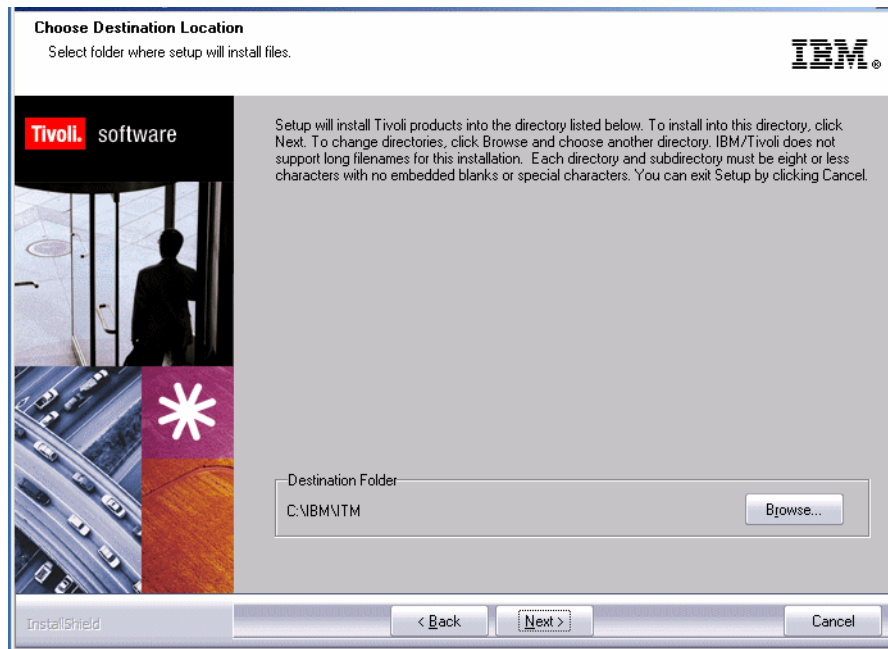


Figure 4-4 Installation windows

5. The next windows will ask you to type a 32-bit encryption key. You can use the default key.

#### Notes:

- This encryption key is used to establish a secure connection (using SSL protocol) between the Hub TEMS and the other components of the IBM Tivoli Monitoring, V6.1 environment as the Remote TEMS connected to the hub. Do not use any of the following characters in your key:
  - =
  - ’
  - |
- Ensure that you document the value you use for the key. Use this key during the installation of any components that communicate with this monitoring server.

6. Click Next and then **click OK** to confirm the encryption key.
7. Select the components that you want to install. Figure 4-5 on page 120 shows the components we selected for our installation.

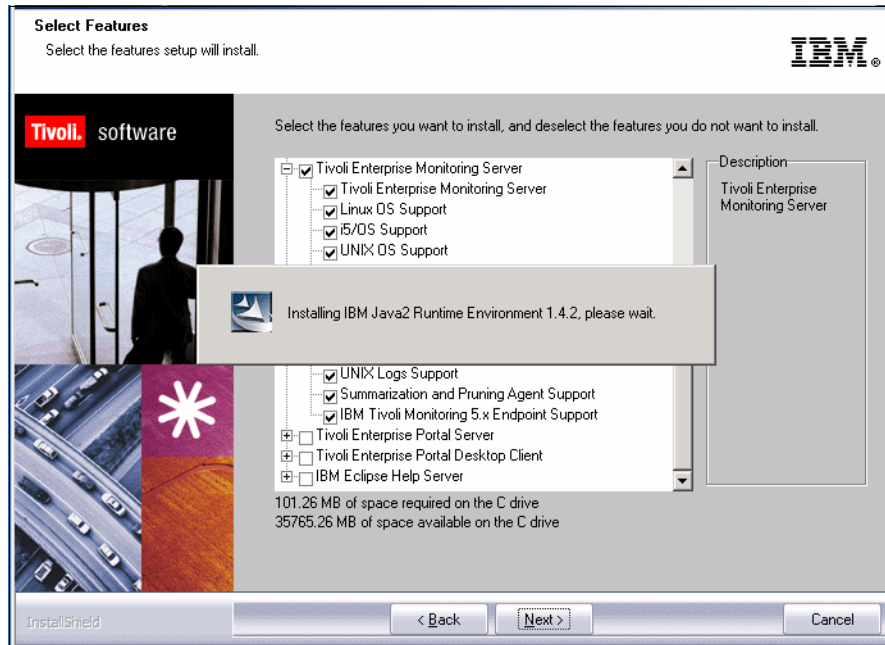


Figure 4-5 List of selected components to be installed

8. Click **Next**.
9. If you want to perform remote deployment of agent software, select those agents that you want to deploy, as shown in Figure 4-6 on page 121. This step creates and populates the deployment depot, from which you can deploy agents at a later time.



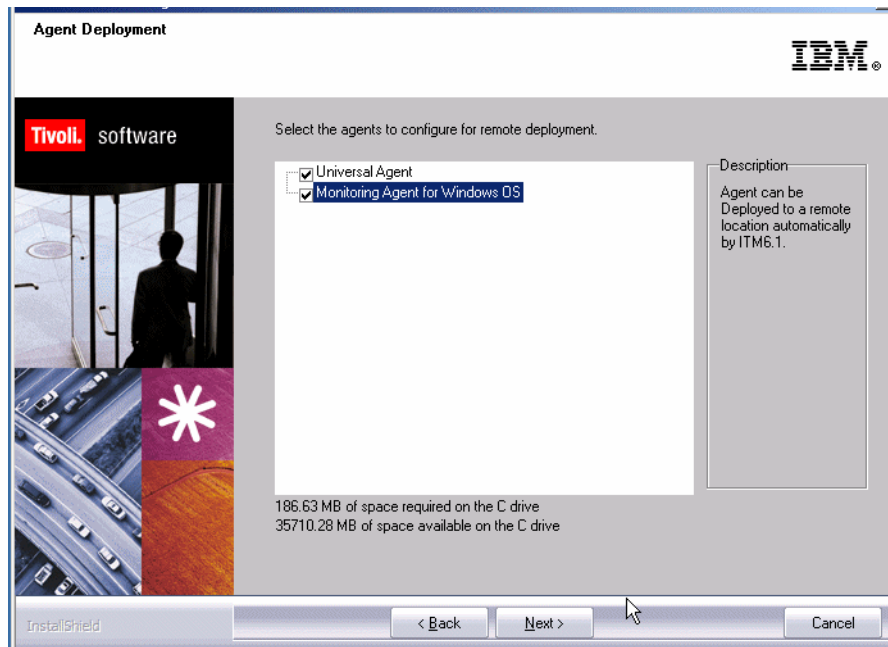


Figure 4-6 Agent list for remote deployment

10. Click **Next**.

**Note:** By default, the depot is located in the <itm\_installdir>/CMS/depot directory on Windows and <itm\_installdir>/tables/<ms\_name>/depot directory on Linux and UNIX. If you want to use a different directory, change the DEPOTHOME value in the kbb.env file.

11. Select a program folder as outlined in Figure 4-7 on page 122 and click **Next**.  
The default program folder name is IBM Tivoli Monitoring.

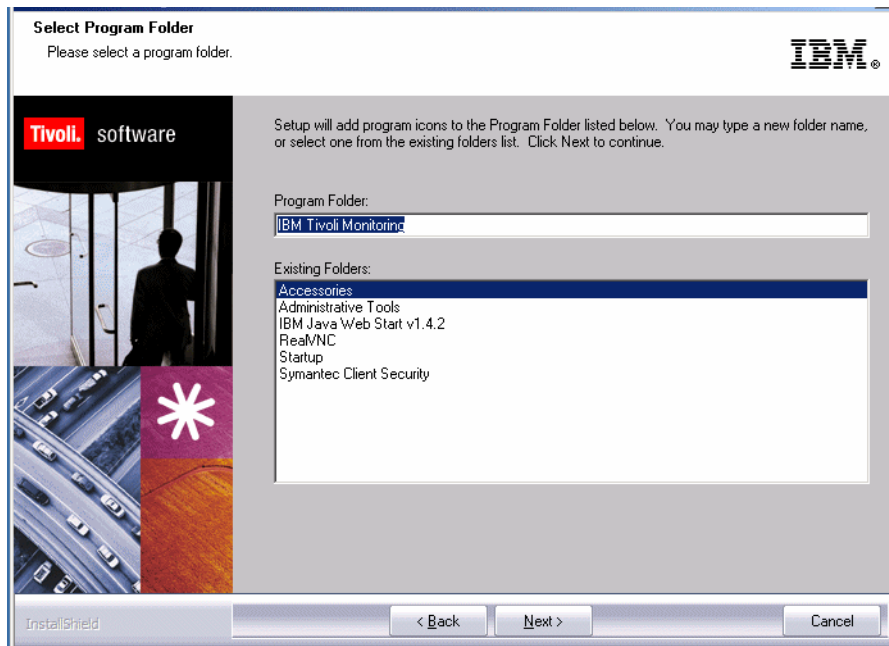


Figure 4-7 Program Folder for the IBM Tivoli Monitoring, V6.1 installation

12. Review the installation summary details. This summary identifies what you are installing and where you have chosen to install. Click **Next** to begin the installation of components (Figure 4-8 on page 123).

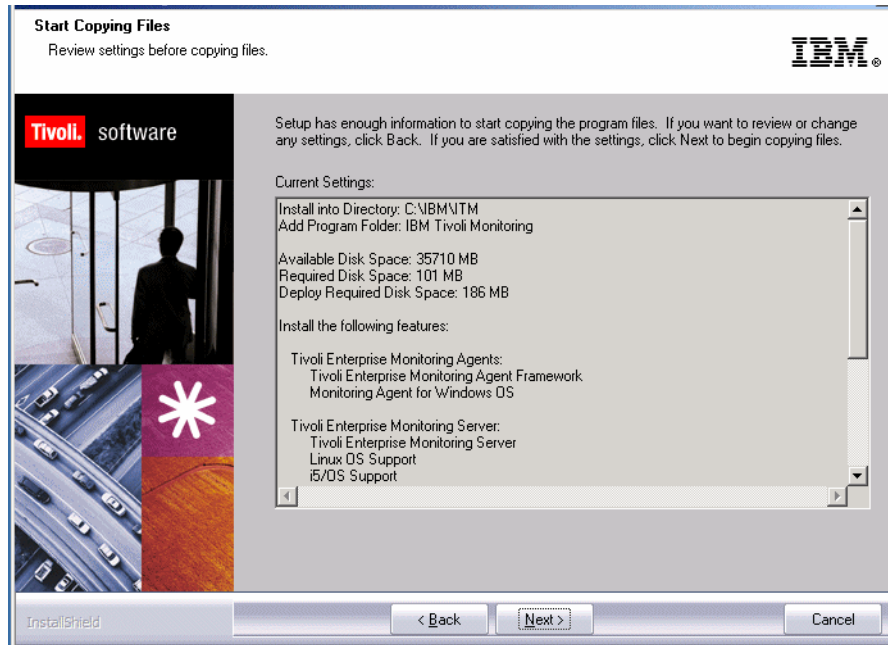


Figure 4-8 Installation summary details

13. After the components are installed, a configuration window (Figure 4-9 on page 124) is displayed with the list of components that can be configured. Select only those you want to configure and click **Next**. We selected all the three components.

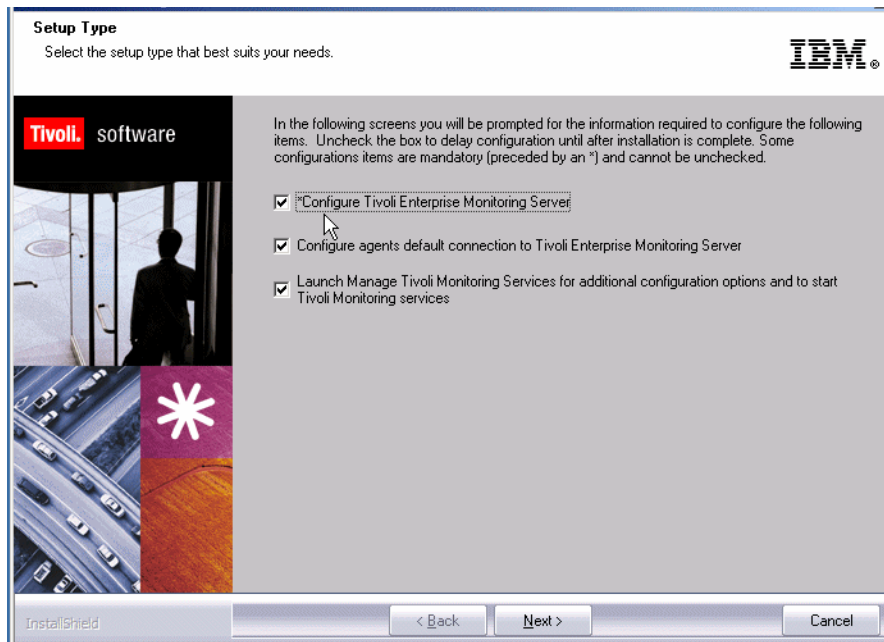


Figure 4-9 List of components that will be configured

14. Figure 4-10 shows the different options of monitoring server type that can be selected. Select **Hub**.

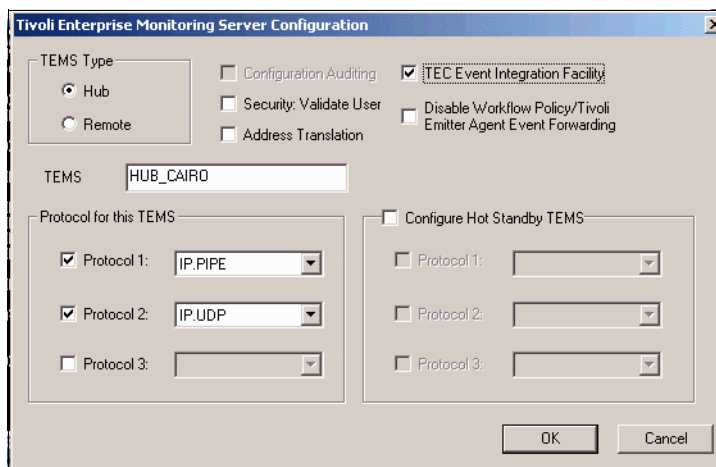


Figure 4-10 Monitoring server configuration window

15. Verify that the name of this monitoring server is correct in the *TEMS* field. If it is not, change it. The default name is `hub_hostname` for example, we chose `HUB_CAIRO` as our TEMS name.
16. Identify the communications protocol for the monitoring server. You have four choices: `IP.UDP`, `IP.PIPE`, `IP.SPIPE`, or `SNA`. You can specify three methods for communication - this enables you to set up backup communication methods. If the method you've identified as Protocol 1 fails, Protocol 2 is used. We selected `IP.PIPE` as our primary protocol and `IP.UDP` as secondary one.

**Note:** `IP.PIPE` protocol uses TCP, thus, permanent connection is established between the TEMS and the remote servers. This could have an impact on the server performance, because of the number of RPCs that it needs to handle. If using UDP will not cause security breaches in your environment, we recommend that you setup the first protocol as `IP.UDP`, otherwise use `IP.PIPE`. Note that if you have a firewall between your TEMS and your agents, you can not use `IP.UDP`.

Table 4-5 describes the communication protocols that can be used and their definitions. This information is valid for all components in the IBM Tivoli Monitoring, V6.1 environment. We will only outline Hub and Remote TEMS in this table.

Table 4-5 Communications protocol description

Field	Description
<b>IP.UDP Settings: Primary Hub TEMS</b>	
Hostname or IP address	The host name or IP address for the hub monitoring server.
Port # and/or Port Pools	The listening port for the hub monitoring server.
<b>IP.PIPE Settings: Primary Hub TEMS</b>	
Host name or IP Address	The host name or IP address for the hub monitoring server.
Port Number	The listening port for the monitoring server. The default value is 1918.
<b>IP.SPIPE Settings: Primary Hub TEMS</b>	

Field	Description
Host name or IP Address	The host name or IP address for the hub monitoring server.
Port Number	The listening port for the monitoring server. The default value is 3660.
<b>SNA Settings: Remote TEMS</b>	
Local LU Alias	The LU alias
TP Name	The transaction program name for this monitoring server.
<b>SNA Settings: Primary Hub TEMS</b>	
Network Name	The SNA network identifier for your location.
LU Name	The LU name for the monitoring server. This LU name corresponds to the Local LU Alias in your SNA communications software.
LU 6.2 LOGMODE	The name of the LU6.2 LOGMODE. The default value is .CANCTDCS.
TP Name	The transaction program name for the monitoring server.

17. If you want to forward situation events to IBM Tivoli Enterprise Console, select **TEC Event Integration Facility**.
18. We did not select Configure Hot Standby TEMS option, because we will set it up when all the TEMS are installed and properly configured. Neither did we select **Disable Workflow Policy/TivoliEmitter Agent Event Forwarding**. We suggest you do the same.
19. Click **OK**.
20. The next window will give you the options to configure the hub server name/ip address and communication port the communication protocol will use. Complete the fields as shown in Figure 4-11 on page 127.

The image shows a 'Hub TEMS Configuration' dialog box with several tabs and input fields. The 'IP.UDP Settings: Hub' tab is active, showing 'Hostname or IP Address' as 'CAIRO' and 'Port # and/or Port Pools' as '1918'. The 'IP.PIPE Settings: Hub' tab shows 'Hostname or IP Address' as 'CAIRO' and 'Port number' as '1918'. The 'IP.SPIPE Settings: Hub' tab shows 'Hostname or IP Address' as 'CAIRO' and 'Port number' as '3660'. The 'SNA Settings: Hub' tab shows 'Network Name' as an empty field, 'LUJ Name' as an empty field, 'LUJ6.2 LOGMODE' as 'CANCTDCS', and 'TP Name' as 'SNASOCKETS'. The 'Entry Options' section has two radio buttons: 'Use case as typed' (selected) and 'Convert to upper case'. The 'NAT Settings' tab is also visible at the bottom left. 'OK' and 'Cancel' buttons are at the bottom right.

Figure 4-11 Host and communication protocol configuration window

21. If you are certain that you have typed in the values for all of these fields with exactly the correct cases (upper and lower cases), you can select **Use case as typed**. However, because IBM Tivoli Monitoring is case-sensitive, consider selecting **Convert to upper case** to reduce the chance of user error.
- 22.. Click OK to continue. The next configuration step is to add application support to the monitoring server, such as the workspaces and situations for agents.
23. After the configuration is complete you'll be prompted to seed the TEMS. Specify the location of the monitoring server. You have two choices:
  - a. On this computer
  - b. On a different computer
 Chose the first option
24. Click **OK**.
25. Because the monitoring server is not currently running, it will start automatically before the process begins. Click **OK** when the following appears. (Figure 4-12 on page 128).



Figure 4-12 Monitoring server start confirmation windows

26. Select the data that you want to add to the monitoring server. By default, all available application support is selected. You are strongly recommended to leave all the components selected, so that they can be seeded. Click **OK**.

**Note:** Seeding adds product specific data from the monitored resources to the monitoring server. For Windows, you can seed the monitoring server both during install and through Manage Tivoli Monitoring Services.

During this process fields are created in the TEMS database (a flat file/Btrieve database not the relational database installed for the TEPS) for the agents you have chosen. This basically enables the TEMS to work with the data from these agents. The same goes for the TEPS, except here of course the necessary tables get created in the relational database of choice.

If the seed data is for an agent that reports to a remote monitoring server, complete this process for both the hub and the remote monitoring server. A hub monitoring server should be running before proceeding with a remote monitoring server seed.

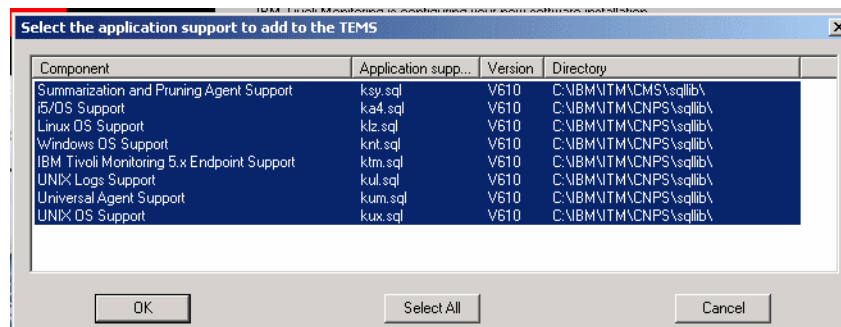


Figure 4-13 Application support to be added to TEMS

27. Verify that all Addition application support for the components have a return code (rc) equal to 0, as shown in Figure 4-14 on page 129 and then click **Next**.



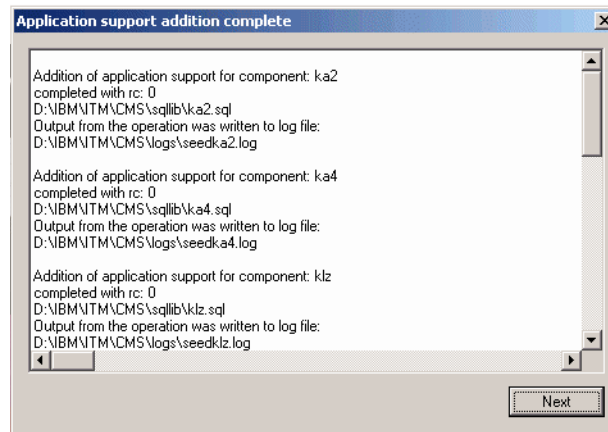


Figure 4-14 Application addition support window

The next configuration step (Figure 4-15 on page 130) configures the default communication between any IBM Tivoli Monitoring component and the hub monitoring server.

28. Specify the default values for any IBM Tivoli Monitoring component to use when they communicate with the monitoring server.
  - a. If agents must cross a firewall to access the monitoring server, select Connection must pass through firewall.
  - b. Identify the type of protocol that the agents use to communicate with the hub monitoring server. You have four choices: IP.UDP, IP.PIPE, IP.SPIPE, or SNA as describe in Table 4-5 on page 125. You can specify three methods for communication - this enables you to set up backup communication methods. If the method you've identified as Protocol 1 fails, Protocol 2 is used. If using UDP will not break your security rules, we suggest to use IP.UDP protocol.
  - c. Click **OK**.

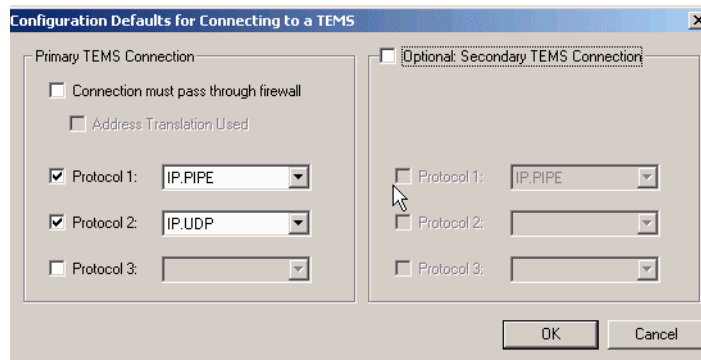


Figure 4-15 Communication protocol configuration to a TEMS

29. In the next window, click **Finish** to complete the installation.

The Manage Tivoli Enterprise Monitoring Services utility is opened. You can start, stop, and configure IBM Tivoli Monitoring components with this utility. See Figure 4-16.

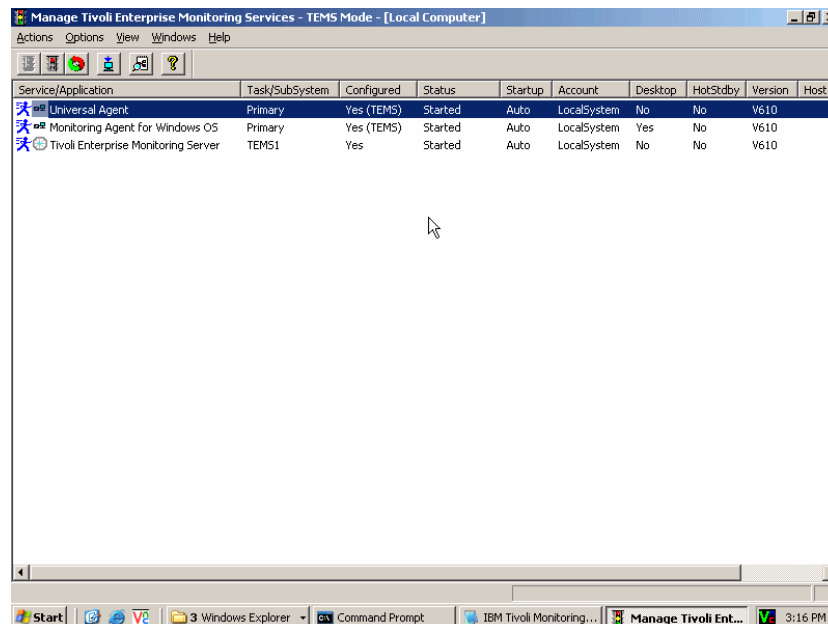


Figure 4-16 IBM Tivoli Monitoring, V6.1 services window

30. Use this same procedure to install the second Hub TEMS.

## 4.2.6 Installing a Remote TEMS on a Windows and UNIX server

The following sections provide detailed information for installing and configuring the remote monitoring server. The following procedures will be used on both the two scenarios:

### Installing a Remote TEMS on a Window server

The installation of a Remote TEMS is very similar with the installation of a Hub TEMS. Unless different from the Hub TEMS installation, the figures for the Remote TEMS installation will not be shown.

Use the following steps to install the remote monitoring server on a Windows computer:

1. Launch the installation wizard by double-clicking the **setup.exe** file on the installation media.

**Note:** If you are running Windows 2003 or Windows XP and have security set to check the software publisher of applications, you might receive an error stating that the setup.exe file is from an unknown publisher. Click **Run** to disregard this error message.

2. Click **Next** on the welcome window.
3. Click **Accept** to accept the license agreement.

**Note:** If you do not have a database (DB2 or MS SQL) installed on this computer, a message regarding potentially missing software is displayed. You do not need a database to use this computer as a monitoring server, so you can click **Next** and ignore this message.

4. If you are missing the IBM Java SDK, the installation program installs it automatically during a later step. Click **Next**.
5. Choose the directory where you want to install the product. The default directory is C:\IBM\ITM. Click **Next**.
6. Type a 32-bit encryption key or use the provided default key.

**Note:** Ensure that you document the value you use for the key. Use this key during the installation of any components that communicate with this monitoring server.

7. Click **Next** and then click **OK** to confirm the encryption key.

8. Select the components that you want to install: **Tivoli Enterprise Monitoring Server**.
9. If you want to install any agents on this remote monitoring server, expand Tivoli Enterprise Monitoring Agents and select the agent. Click **Next**.
10. If you want to do remote deployment of agent software from this remote monitoring server, select those agents that you want to deploy. This step creates and populates the deployment depot, from which you can deploy agents at a later time. Click **Next**.

**Note:** By default, the depot is located in the <itm\_installdir>/CMS/depot directory on Windows and <itm\_installdir>/tables/<ms\_name>/depot directory on Linux and UNIX. If you want to use a different directory, change the DEPTHOME value in the kbb.env file.

11. Select a program folder and click **Next**. The default program folder name is IBM Tivoli Monitoring.
12. Review the installation summary details. This summary identifies what you are installing and where you have chosen to install. Click **Next** to start the installation of components.

After the components are installed, a configuration window is displayed.

13. Select what you want to configure and click **Next**. The first step configures the monitoring server.
14. Select the type of monitoring server you are configuring: Hub or Remote. For this procedure, select **Remote** as shown in Figure 4-17.

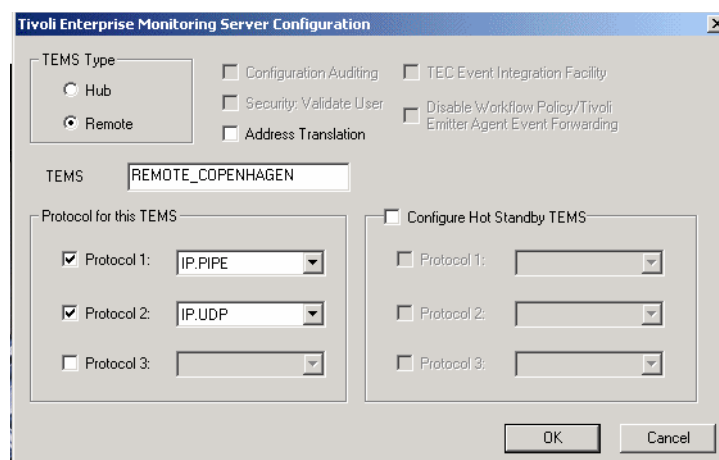


Figure 4-17 Remote TEMS configuration window

15. Verify that the name of this monitoring server is correct in the TEMS. If it is not, change it.
16. Identify the communications protocol for the monitoring server. You have four choices: IP.UDP, IP.PIPE, IP.SPIPE, or SNA. You can specify three methods for communication - this enables you to set up backup communication methods. If the method you have identified as Protocol 1 fails, Protocol 2 will be used. Click **OK**.
17. Complete the following fields for the communications protocol for the monitoring server. Table 4-5 on page 125 shows you the detailed description of all the protocols that can be used.
18. If you are certain that you have typed the values for all of these fields with exactly the correct casing (upper and lower cases), you can select **Use case as typed**. However, because IBM Tivoli Monitoring is case-sensitive, consider selecting **Convert to upper case** to reduce the chance of user error.
19. Click **OK** to continue. The next configuration step is to seed the monitoring server.
20. Specify the location of the monitoring server. You have two choices:
  - a. This computer
  - b. On a different computerSelect **This computer** and click **OK**.
21. Because the monitoring server is not currently running, it is started automatically before the seeding process begins. Click **OK** when you get the the message that tells you this.
22. Select the data that you want to add to the monitoring server. By default, all available product data is selected. Click **OK**.
23. Click **Next** on the message that provides information about the seeding. The next configuration step configures the default communication between any IBM Tivoli Monitoring component and the hub monitoring server.
24. Specify the default values for any IBM Tivoli Monitoring component to use when they communicate with the monitoring server.
  - a. If agents must cross a firewall to access the monitoring server, select **Connection must pass through firewall**.
  - b. Identify the type of protocol that the agents use to communicate with the hub monitoring server. You have four choices: IP.UDP, IP.PIPE, IP.SPIPE, or SNA. You can specify three methods for communication - this enables you to set up backup communication methods. If the method you have identified as Protocol 1 fails, Protocol 2 is used.
25. Click **OK**.

26. Complete the communication protocol fields for the monitoring server. See Table 4-5 on page 125 for definitions of these fields.
27. **Click Finish** to complete the installation.

## Installing Remote TEMS on a UNIX/Linux server

The Remote TEMS installation procedure is the same as the one for Hub TEMS. The differentiation will occur during the configuration. The Table 4-6 shows the different steps on installing, configuring and seeding a Remote TEMS.

Table 4-6 Steps for installing a Remote TEMS

Steps	Where to find information
Install the Remote TEMS using the same instruction as installing the Hub TEMS	Installing a Hub TEMS on a UNIX server
Configure the remote TEM	Configuring Remote TEMS on a UNIX/Linux server
Seeding the Remote TEMS	Installing agents support on (seeding) the hub monitoring

## Configuring Remote TEMS on a UNIX/Linux server

1. Use the following steps to configure the hub monitoring server:
2. At the command line change to the opt/IBM/ITM/bin directory (or the directory where you installed IBM Tivoli Monitoring).
3. Run the following command:  
`./itmcmd config -S -t tems_name`, where tems\_name is the name of your monitoring server (for example, REMOTE\_EDINBURG).
4. Type remote to indicate that this is a Remote TEMS.
5. Press Enter to accept the default host name for the monitoring server. This should be the host name for your computer. If it is not, type the correct host name and then press Enter. 5. Enter the type of protocol to use for communication with the monitoring server. You have four choices: ip, ip.pipe, sna or ip.spipe. Press Enter to use the default communications protocol (IP.PIPE).
6. If you want to set up a backup protocol, enter that protocol and press Enter. If you do not want to use backup protocol, press Enter without specifying a protocol.
7. Depending on the type of protocol you specified, provide the port number for each communication protocol and press Enter.
8. Press Enter to not specify the name of the KDC\_PARTITION.

9. Press Enter when prompted for the path and name of the KDC\_PARTITION.
10. If you want to use Configuration Auditing, type y or type n otherwise and press Enter.
11. Press Enter to accept the default setting for Hot Standby (NO). For best results, wait until after you have fully deployed your environment to configure Hot Standby for your monitoring server. See ““Configuring Hot Standby” on page 212 for information about configuring Hot Standby.
12. Press Enter to accept the default for the Optional Primary Network Name (none).
13. Press Enter for the default Security: Validate User setting (no). If you need to use security validation in your environment, you can enable it after initial configuration is complete.
14. If you will be using Event Synchronization to view situation events, type y and press Enter to enable TEC Event Integration. Complete the following additional steps:
  - a. Type the name of the IBM Tivoli Enterprise Console event server and press Enter.
  - b. Type the port number for the event server and press Enter.
15. Press Enter to not disable the Workflow Policy/Tivoli Emitter Agent.
16. Type S to save the default SOAP configuration and exit the configuration.

**Notes:**

- ▶ You can configure any SOAP information at a later time. The procedure is described in “Installing Event Synchronization on your event server” on page 198.
- ▶ A configuration file is generated in the install\_dir/config directory with the format host\_name\_ms\_tems\_name.config (for example, edinburg\_ms\_REMOTE\_EDINBURG.config).

## 4.2.7 Tivoli Enterprise Portal Server - TEPS

The following section will describe the detailed steps on how to install and configure a TEPS in a Windows server using DB2 8.2 as RDBMS.

**Note:** Our choice for the Windows server was driven by a limitation of the IBM Tivoli Monitoring, V6.1 beta version we were using. In the beta version of the code that we used for this project, it was not possible to connect to a Data Warehouse for long term historical data views using a Linux portal server. This limitation is expected to go away in the general availability version. Please refer the IBM Tivoli Monitoring, V6.1 general availability documentation or contact IBM support to verify if this issue has already been resolved, if you are considering changing your platform because of that limitation.

## Pre-installation steps

The Tivoli Enterprise Portal Server function require a database to store information. Please refer to *IBM Tivoli Monitoring, V6.1.0 Installation and Setup Guide*, GC32-9407, Appendix B to install and setup properly your RDBMS.

### ***Install the RDBMS***

Prior to installing the TEPS you have to install and setup correctly the DB2 database in your environment.

### ***ODBC connection for the TEPS***

TEPS access the created database using ODBC connection. ODBC TEPS2 will be created during TEPS installation, so it is not necessary to create it manually.

### ***Create a user on the DB2 server***

Create a DB2 user in the DB2 server. You can use whatever name you want but the user must belong to Administrators group. We created a user named *ITMUser*.

**Note:** This user will be used by TEPS to access the Data Warehouse.

## Installing the portal server on a Window server

Use the following steps to install the Tivoli Enterprise Portal Server on a Windows computer.

1. Launch the installation wizard by double-clicking the **setup.exe** file in the WINDOWS subdirectory of the installation media.
2. Click **Next** on the Welcome window to start the installation.
3. Read and accept the software license agreement by clicking **Accept**.
4. If you do not have a database (DB2 or MS SQL) or the IBM Java SDK installed on this computer, a message regarding potentially missing required software is displayed. If you are missing a database, stop the installation, install the required database, and begin the installation again. If you are



missing the IBM Java SDK, the installation program installs it automatically during a later step. Click **Next**.

**Note:** If your computer has all required software, you will not see this step.

5. Specify the directory where you want to install the portal software and accompanying files. The default location is C:\IBM\ITM. Click **Next**.
6. Type an encryption key to use. This key should be the same as what was used during the installation of the monitoring server to which this portal server will connect. Click **Next** and then **OK** to confirm the encryption key.
7. Select Tivoli Enterprise Portal Server from the list of components to install as shown in Figure 4-18.

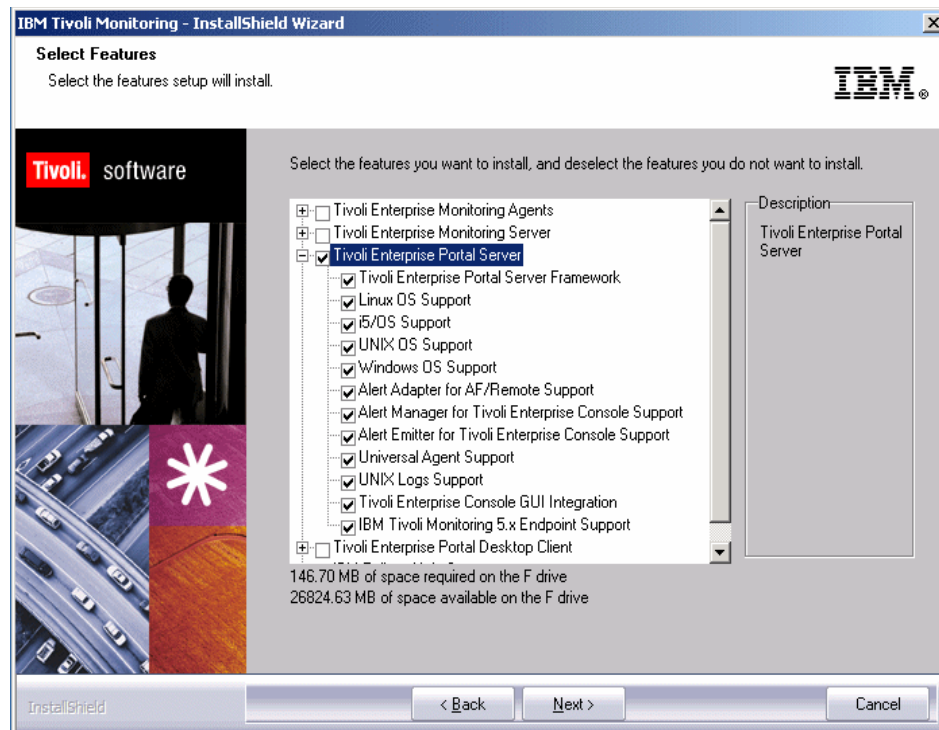


Figure 4-18 IBM Tivoli Monitoring, V6.1 Components List

**Note:** You might notice that it will begin installing the required JRE on the machine as soon as you select the TEPS for installation. This happens if you do not have the required JRE installed in your machine. The JRE is bundled with the installation media and you do not have to do anything but wait until the installation is finished.

8. If you want to view events from the IBM Tivoli Enterprise Console event server through the Tivoli Enterprise Portal, expand the **Tivoli Enterprise Portal Server** selection and ensure that Tivoli Enterprise Console GUI Integration is selected. Click **Next**.
9. Click **Next** on the Agent Deploy window. Do not select any agents.
10. Type a name for the program folder. The default is IBM Tivoli Monitoring. Click **Next**.
11. Click **Next** to start the installation. After installation is complete, a configuration window (Table 4-19) is displayed.

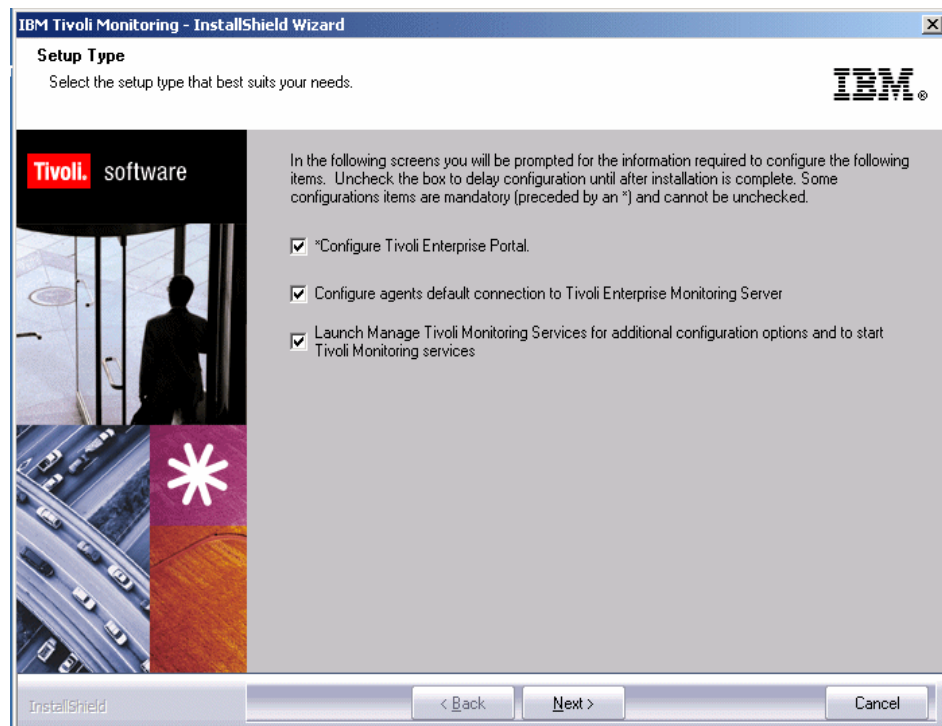


Figure 4-19 TEPS configuration option window

- 12.. Click **Next** to begin configuring the portal server and the connection to the monitoring server, and to open Manage Tivoli Monitoring Services.
13. In the next window (Table 4-20) type the host name of the computer where you are installing the portal server and click **Next**.

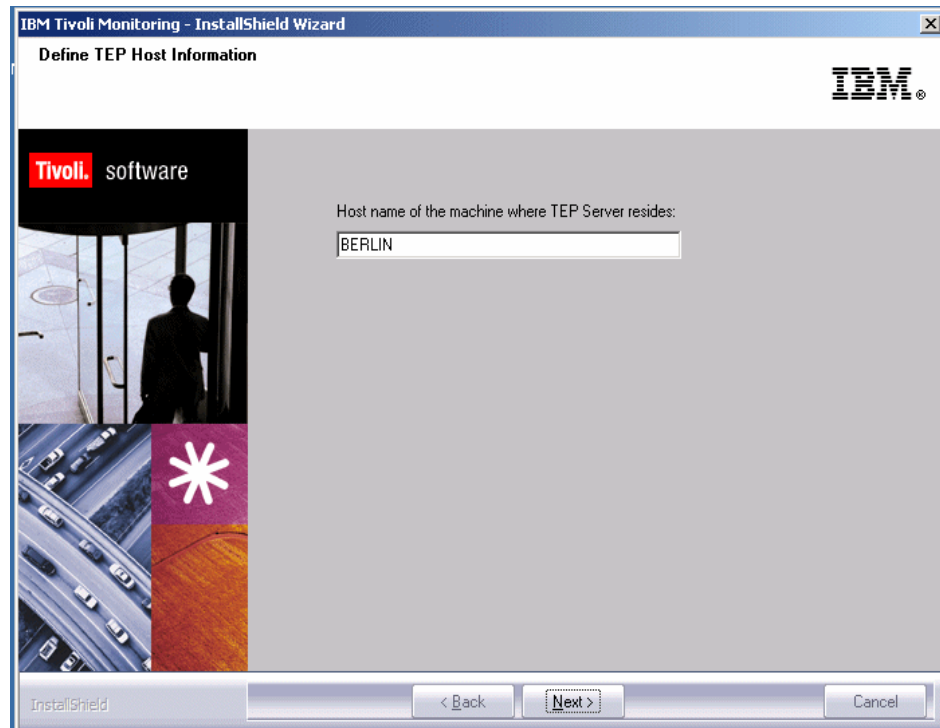


Figure 4-20 Hostname where TEPS will be installed

14. Configure the portal server's connection to the data source (such as your DB2 database). Type the password for the database administrator in the Admin Password field.
15. Then type a database userid and password for your db2 Administrator account.

**Note:** DB2 Administrator account was created during the DB2 installation.

16. Click **OK**. Refer to Figure 4-21 on page 140.

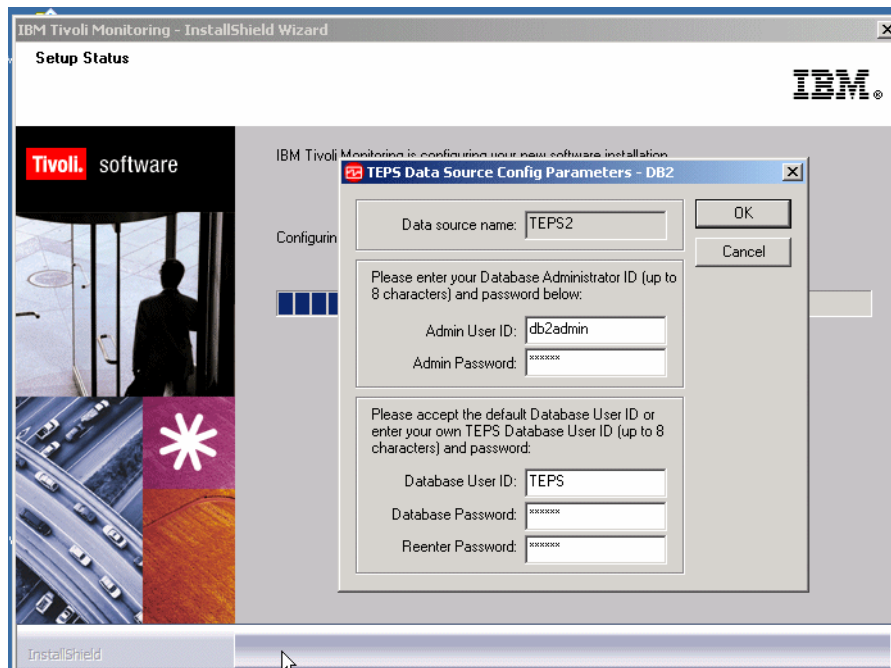


Figure 4-21 TEPS database configuration

17. Click **OK** on the message that tells you that the portal server configuration was successful (Figure 4-22 on page 141).

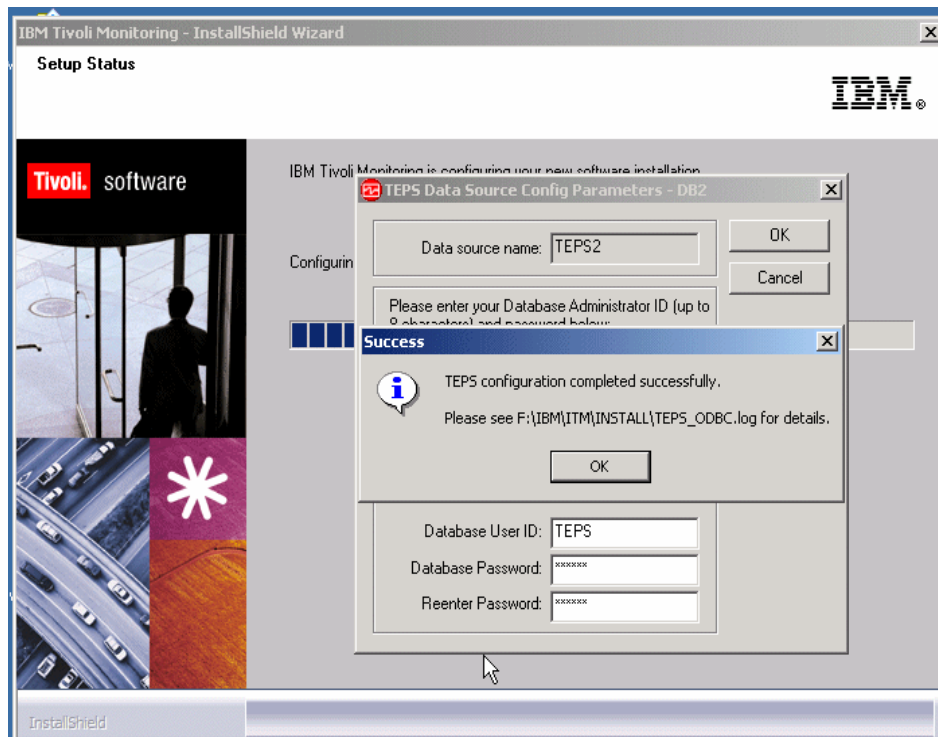


Figure 4-22 TEPS configuration completion window

18. Next it will ask about the user credentials to access the Data Warehouse database. Type a userid (such as candle, this user must be previously created.) in the User ID field and type a password for the user in the Password field. Click **Next** (Figure 4-23 on page 142).

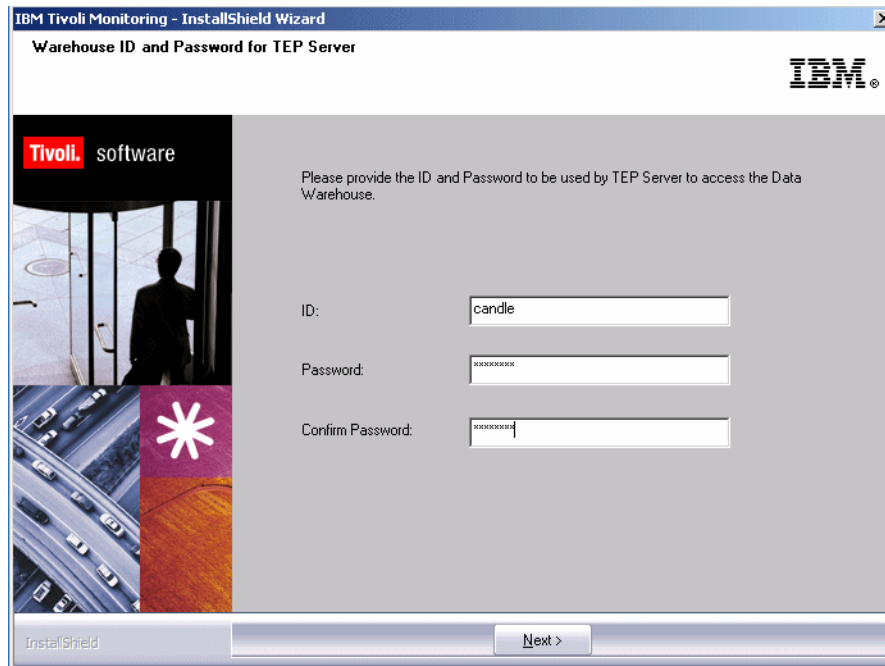


Figure 4-23 TEPS user configuration

19. Select the communication protocols as shown in Figure 4-24 and click **OK** (Figure 4-24). This will define the values for the connection between the portal server and the hub monitoring server.

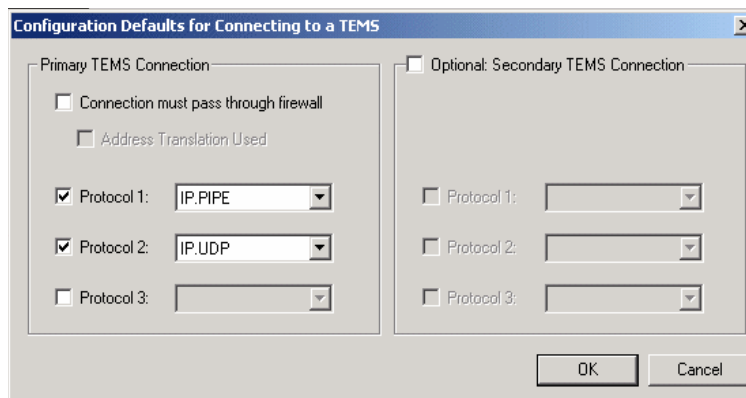


Figure 4-24 Communication protocol window configuration

20. Type the host name or IP address and the port number for the hub monitoring server as shown in Figure 4-25 on page 143. Click **OK** when finished.

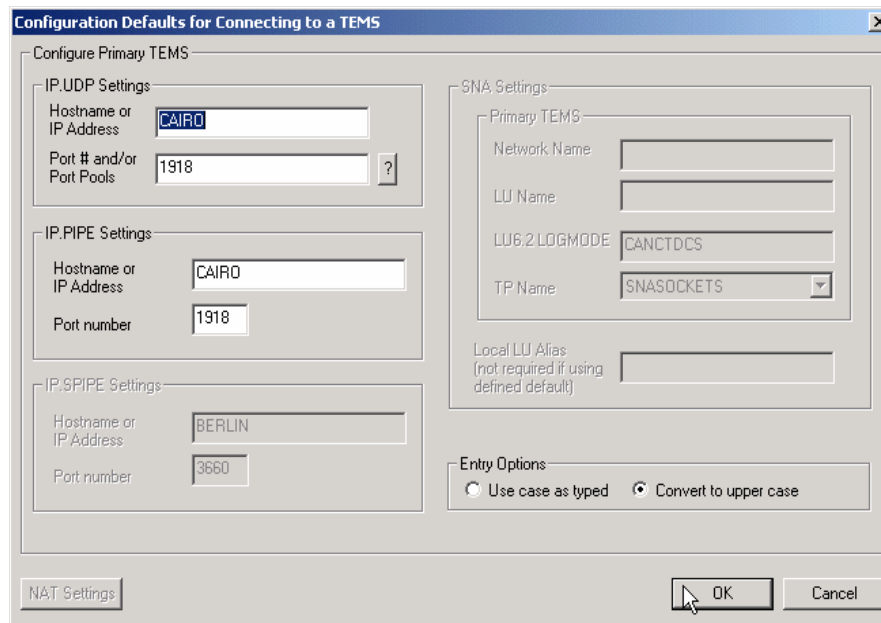


Figure 4-25 Configuration for connection to the TEMS

21. Click Finish to close the installation wizard. After the installation completes, a README about Tivoli Enterprise Portal configuration is displayed, read it and close the window.

Now the Hub TEMS, Remote TEMS and the TEPS are installed and configured. We will proceed with the installation of the TEMAs and the TEP, WPA, and Event Synchronization.

## 4.2.8 Tivoli Enterprise Monitoring Agent - TEMA

In this section we will cover the installation of Tivoli Enterprise Monitoring Agents.

### Deploying TEMA on a Linux server (using local images)

The following section will show step by step how we deploy a TEMA on a Linux server using local downloaded IBM Tivoli Monitoring, V6.1 images. Our server name is oslo and the user is itmuser.

**Note:** Whenever we did not enter with or select an option Enter key was hit to accept the default.

1. From the directory where the images are uncompressed, execute the following procedure:

```
itmuser@oslo:/home/itmuser> ./install.sh
```

The output of the command is shown in the following. You will see our selections in bold.

---

*Example 4-1 Output of ./install.sh*

---

```
Enter the name of the IBM Tivoli Monitoring directory
[ default = /opt/IBM/ITM ]:
CANDLEHOME directory "/opt/IBM/ITM" already exists.
OK to use it [ y or n; "y" is default ]? y
```

Before installing IBM Tivoli Monitoring agents, you must install at least one IBM Tivoli Enterprise Monitoring Server. You will need the host name or IP address and port number for the monitoring server to configure any agents.

---

**Notes:**

- ▶ If /opt/IBM/ITM does not exist, you will receive the following message:  
“/opt/IBM/ITM” does not exist  
try to create it [y or n; “y” is default]?
- ▶ You will notice small differences on the message between the following menu with the one you will be running because of the version differences. But the functions remains the same.

---

*Example 4-2 Output of ./install.sh*

---

```
install.sh      : searching for product families; please wait.
Select one of the following:
1) Install products via command line.
2) Install products to depot via command line.
3) Exit install.
Please enter a valid number: 1
install.sh      : OK to install.
install.sh      : removing old JRE.
install.sh      : old JRE has been removed.
install.sh      : unloading JRE package(s).
install.sh      : calculating available disk space.
install.sh      : "33631276" kilobytes available.
install.sh      : running li6243 jre.
Software Licensing Agreement
1. Czech
2. English
3. French
4. German
```



5. Italian
6. Polish
7. Portuguese
8. Spanish
9. Turkish

Please enter the number that corresponds to the language you prefer.

2

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.

---

2. Hit Enter key.

#### *Example 4-3 Output of ./install.sh*

---

International License Agreement for Early Release of Programs

Part 1 - General Terms

BY DOWNLOADING, INSTALLING, COPYING, ACCESSING, OR USING THE PROGRAM YOU AGREE TO THE TERMS OF THIS AGREEMENT. IF YOU ARE ACCEPTING THESE TERMS ON BEHALF OF ANOTHER PERSON OR A COMPANY OR OTHER LEGAL ENTITY, YOU REPRESENT AND WARRANT THAT YOU HAVE FULL AUTHORITY TO BIND THAT PERSON, COMPANY, OR LEGAL ENTITY TO THESE TERMS. IF YOU DO NOT AGREE TO THESE TERMS,

- DO NOT DOWNLOAD, INSTALL, COPY, ACCESS, OR USE THE PROGRAM; AND

1

```
runGSkit      : Preparing to install the Global Security Kit.
runGSkit warning: the 'root' ID or password is required for this phase,
continuing ..
```

Will enable automatic agent initiation after reboot.

Please enter root password or press Enter twice to skip.

Password:

Enter the root password

Preparing packages for installation...

gsk7bas-7.0-3.9

```
runGSkit      : creating security files.
runGSkit      : create keyfile.
runGSkit      : create certificate.
runGSkit      : setting encryption key.
```

Enter a 32-character encryption key, or just press Enter to use the default  
Default = **IBMTivoliMonitoringEncryptionKey**

....+....1....+....2....+....3..

Press Enter to continue viewing the license agreement, or,  
Enter "1" to accept the agreement, "2" to decline it or  
"99" to go back to the previous screen.

**1**

GSkit encryption key has been set.

Key File directory: /opt/IBM/ITM/keyfiles

Product packages are available in /home/itmuser/unix

Product packages are available for the following operating systems and  
component support categories:

- 1) Linux Intel R2.4 (32 bit)
- 2) Linux Intel R2.4 (64 bit)
- 3) Linux Intel R2.4 GCC 2.9.5 (32 bit)
- 4) Linux Intel R2.4 GCC 2.9.5 (64 bit)
- 5) Linux Intel R2.6 (32 bit)
- 6) Linux Intel R2.6 (64 bit)
- 7) Linux Intel R2.6 GCC 2.9.5 (32 bit)
- 8) Linux Intel R2.6 GCC 2.9.5 (64 bit)
- 9) Tivoli Enterprise Portal Browser Client support
- 10) Tivoli Enterprise Portal Desktop Client support
- 11) Tivoli Enterprise Portal Server support

Type the number for the OS or component support category you want, or type  
"q" to quit selection

[ number "5" or "Linux Intel R2.6 (32 bit)" is default ]:

**5**

Is the operating system or component support correct [ y or n; "y" is  
default ]? **y**

The following products are available for installation:

- 1) IBM Eclipse Help Server V610R104
- 2) Monitoring Agent for Linux OS V610R115
- 3) Monitoring Agent for Unix Logs V610R121
- 4) Summarization and Pruning agent V610R141
- 5) Tivoli Enterprise Monitoring Server V610R215
- 6) Tivoli Enterprise Portal Desktop Client V610R172
- 7) Tivoli Enterprise Portal Server V610R172
- 8) Tivoli Enterprise Services User Interface V610R194
- 9) Universal Agent V610R229
- 10) all of the above

Type the numbers for the products you want to install, or type "q" to quit selection.

If you enter more than one number, separate the numbers by a comma or a space.

Type your selections here: **2**

The following products will be installed:

**Monitoring Agent for Linux OS V610R115**

Are your selections correct [ y or n; "y" is default ]? **y**

... installing "Monitoring Agent for Linux OS V610R115 for Linux Intel R2.6 (32 bit)"; please wait.

=> installed "Monitoring Agent for Linux OS V610R115 for Linux Intel R2.6 (32 bit)."

... Initializing database for Monitoring Agent for Linux OS V610R115 for Linux Intel R2.6 (32 bit).

... Monitoring Agent for Linux OS V610R115 for Linux Intel R2.6 (32 bit) initialized.

Do you want to install additional products or product support packages [ y or n; "n" is default ]? **n**

... postprocessing; please wait.

... finished postprocessing.

Installation step complete.

You must install TEMS support for the agent products. This is done by starting and seeding the TEMS for the supported agents.

You may now reconfigure any installed IBM Tivoli Monitoring product via the "/opt/IBM/ITM/bin/itmcmd config" command.

---

## Post TEMA installation procedure

1. From the \$CANDLEHOME/bin (/opt/Tivoli/IBM is the default \$CANDLEHOME directory) execute the following line:

```
itmuser@oslo:/opt/IBM/ITM/bin> ./itmcmd config -A lz
```

The output of the command is shown in the following:

*Example 4-4 Post TEMA installation procedure*

---

```
lz for linux, ux for unix
CandleConfig      : installer level 400 / 100.
CandleConfig      : running li6243 jre.
Agent configuration started...

Will this agent connect to a TEMS? [YES or NO] (Default is: YES):YES
TEMS Host Name (Default is: oslo): edinburg
```

---

**Note:** edinburg is the Remote TEMS where the agent will connect to.

*Example 4-5 Post TEMA installation procedure*

---

```
Will the agent connect through a firewall? [YES or NO] (Default is: NO):NO

Network Protocol [ip, sna, ip.pipe or ip.spipe] (Default is: ip.pipe):ip.pipe
```

Now choose the next protocol from one of these:

- ip
- sna
- ip.pipe
- none

```
Network Protocol 2 (Default is: none): ip
```

Now choose the next protocol from one of these:

- ip
- sna
- none

```
Network Protocol 3 (Default is: none):none
IP Port Number (Default is: 1918):1918
IP.PIPE Port Number (Default is: 1918):1918
Enter name of KDC_PARTITION (Default is: null):null
IP.SPIPE Port Number (Default is: 3660)
```

```
Configure connection for a secondary TEMS? [YES or NO] (Default is: NO): YES
Secondary TEMS HostName (Default is: none): copenhagen
```

```
Will the agent connect through a firewall? [YES or NO] (Default is: NO):NO
```

```
Secondary TEMS protocol [ip, sna, or ip.pipe] (Default is: ip): ip.pipe
```

Now choose the next protocol from one of these:

- ip
- sna
- ip.pipe
- none

```
Secondary TEMS Protocol 2 (Default is: none): ip
```

```

Now choose the next protocol from one of these:
- ip
- sna
- none
Secondary TEMS Protocol 3 (Default is: none):none
Secondary TEMS IP Port Number (Default is: 1918):1918
Secondary TEMS IP.PIPE Port Number (Default is: 1918):1918
Enter Optional Primary Network Name or "none" (Default is: none):none
Agent configuration completed...

```

---

**Note:** When installing on AIX, it will ask the following:

Are you installing this product into a clustered environment (Default is: NO)

1. Once done, you can start the agent using the following command line:  
`./itmcmd agent start lz`
2. If you don't know the agent code, execute the `./cinfo` command line from `$CANGDELHOME/bin` directory. You should have something like the following:

*Example 4-6 Output ./cinfo command*

---

```

[root@ankara bin]# ./cinfo

***** Fri Sep 23 15:31:15 EDT 2005 *****
User       : root           Group: root bin daemon sys adm disk wheel
Host name  : ankara.itsc.austin.ibm.com  Installer Lvl: 400 / 100
CandleHome: /opt/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

```

---

3. Select option 1 to have the following type of result:

*Example 4-7 Post TEMA installation procedure*

---

```

***** Fri Sep 23 15:33:37 EDT 2005 *****
User       : root           Group: root bin daemon sys adm disk wheel
Host name  : ankara.itsc.austin.ibm.com  Installer Lvl: 400 / 100
CandleHome: /opt/IBM/ITM
*****
...Product inventory

```

```
ax      IBM Tivoli Monitoring Shared Libraries
        li6243  Version: 610 Rel: 221
jr      Tivoli Enterprise-supplied JRE
        li6243  Version: 400 Rel: 100
lz      Monitoring Agent for Linux OS
        li6263  Version: 610 Rel: 115
uf      Universal Agent Framework
        li6243  Version: 610 Rel: 100
ui      Tivoli Enterprise Services User Interface
        li6243  Version: 610 Rel: 194
um      Universal Agent
        li6243  Version: 610 Rel: 229
-- 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
```

---

**Note:** You can also have the same result executing the following command:  
**./cinfo -i**

4. If you have installed the Universal Agent as well, you can start executing the following command line:

```
./itmcmd config -A um
```

## Installing TEMA on a Window Server

Use the following steps to install a monitoring agent:

1. Launch the installation wizard by double-clicking the setup.exe file on the installation media.
2. Click **Next** on the welcome window (Figure 4-26 on page 151).

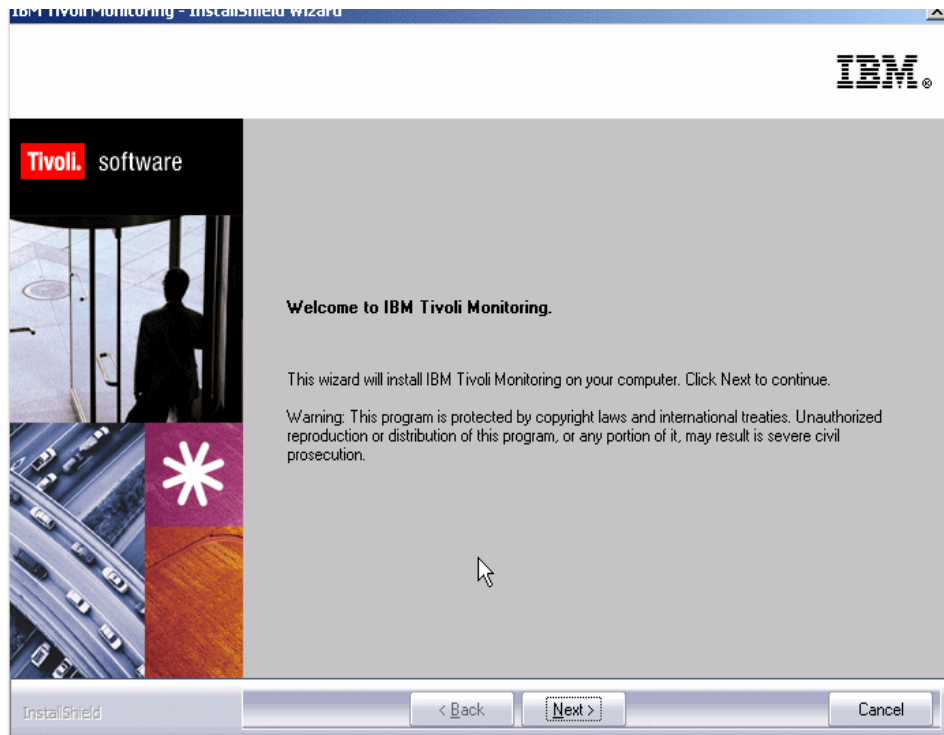


Figure 4-26 IBM Tivoli Monitoring, V6.1 welcome installation window

3. Click **Accept** to accept the license agreement (Figure 4-27 on page 152).

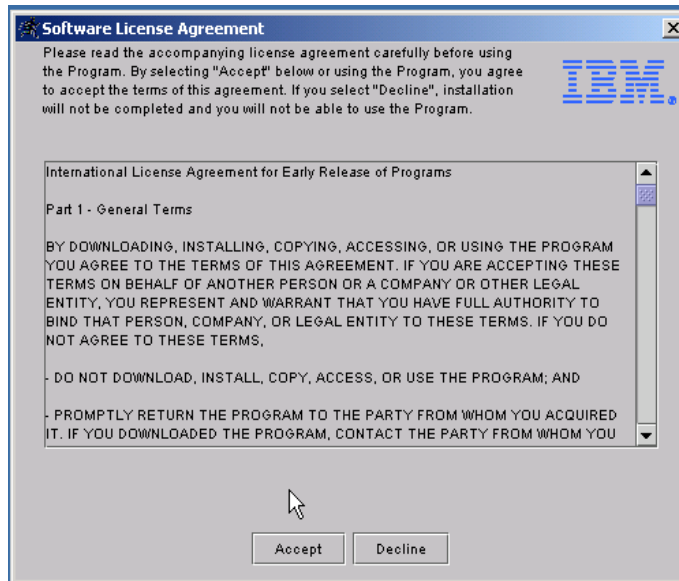


Figure 4-27 IBM Tivoli Monitoring, V6.1 license agreements

4. If you do not have a database (DB2 or MS SQL) installed on this computer, a message regarding potentially missing software is displayed as shown in Figure 4-28 on page 153. You do not need a database to install a management agent on this computer, so you can click **Next** and ignore this message.



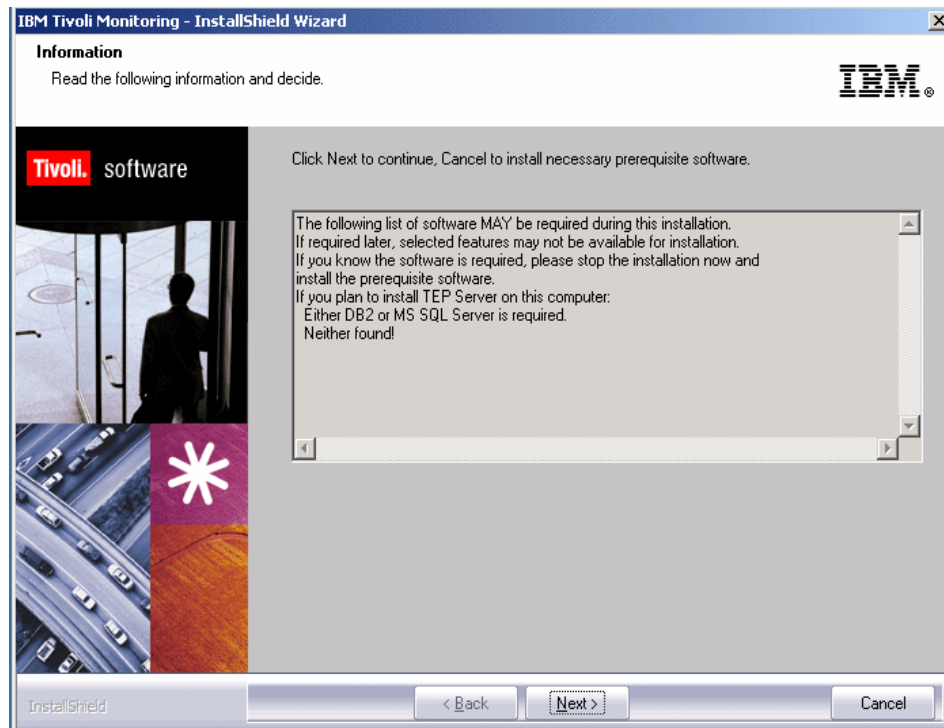


Figure 4-28 IBM Tivoli Monitoring, V6.1 requisites information screen

5. Choose the directory where you want to install the product, default is c:\IBM\ITM as shown in Figure 4-29 on page 154. Click **Next**.



Figure 4-29 IBM Tivoli Monitoring, V6.1 default destination installation directory

6. Type a 32-bit encryption key. This key should be the same as the key that has been used during the installation of the monitoring server, to which this monitoring agent connects. Click **Next** and then click **OK** to confirm the encryption key. See Figure 4-30 on page 155.

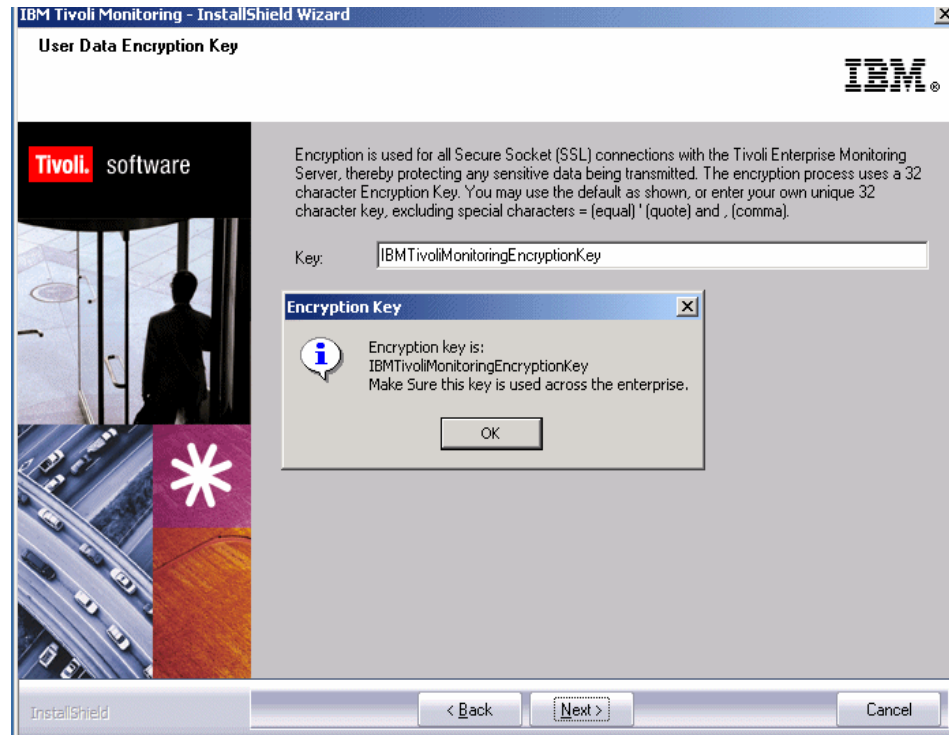


Figure 4-30 IBM Tivoli Monitoring, V6.1 encryption key confirmation

7. Expand **Tivoli Enterprise Monitoring Agents**.
8. Select the name of the agent that you want to install and click **Next** (Figure 4-31 on page 156).

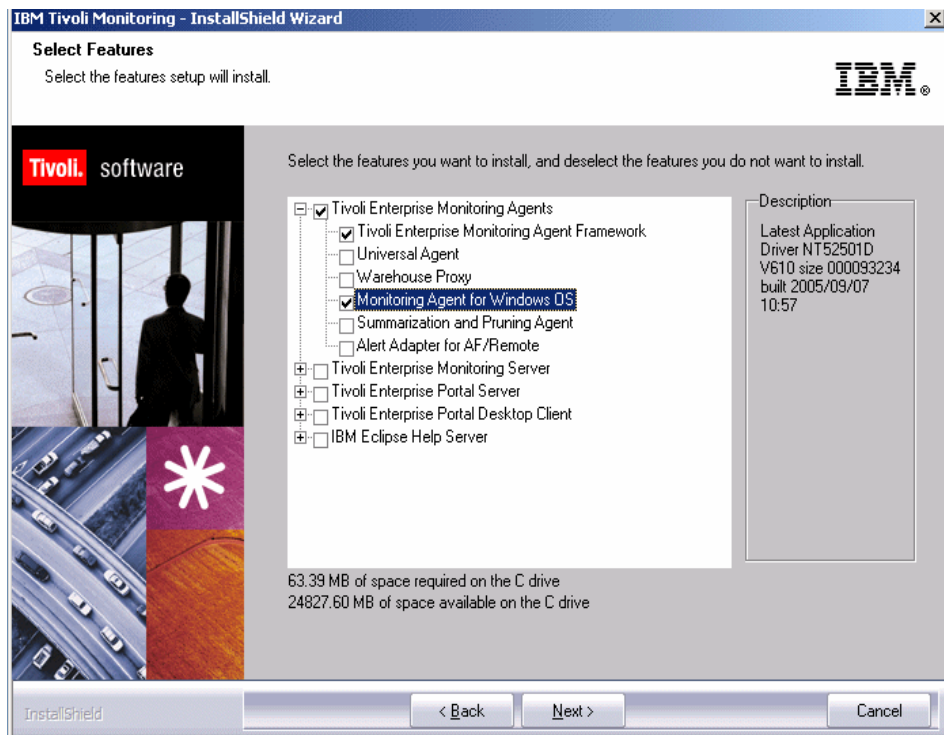


Figure 4-31 Monitoring agents to be installed

- Click **Next** on the Agent Deploy window. Do not select any agents.
- Type a program folder to use in your Start menu and click **Next**. The default folder is IBM Tivoli Monitoring, as shown in Figure 4-32 on page 157.

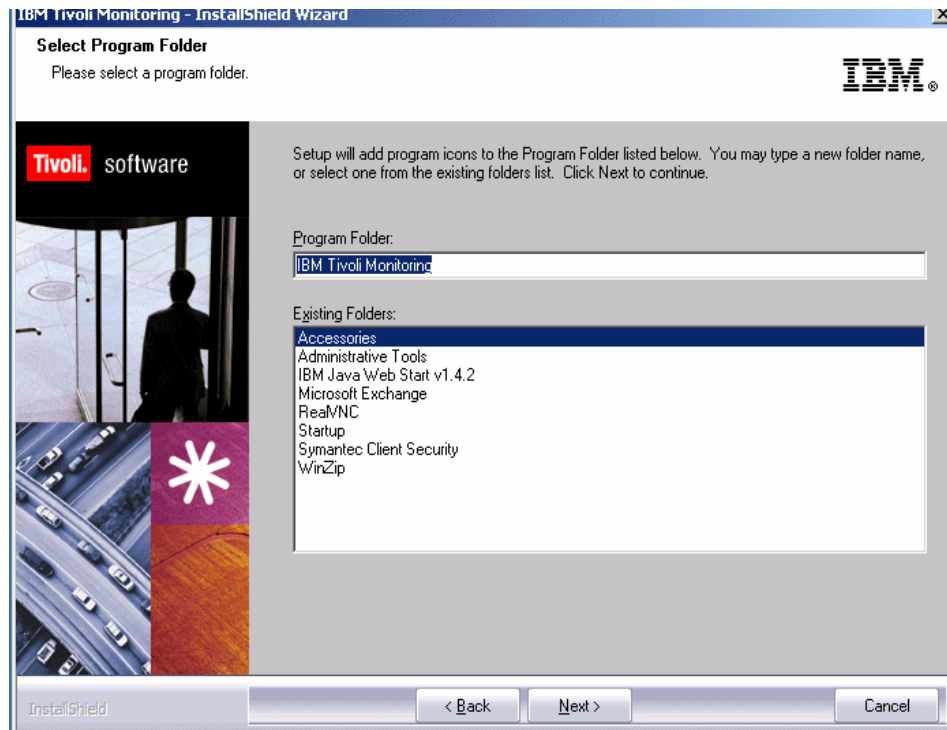


Figure 4-32 IBM Tivoli Monitoring, V6.1 program folder

11. Review the installation summary details. This summary identifies what you are installing and where you have chosen to install (Figure 4-33 on page 158). Click **Next** to begin the installation of components. After the components are installed and the configuration environment is initialized (indicated by a pop-up window), a configuration window is displayed.

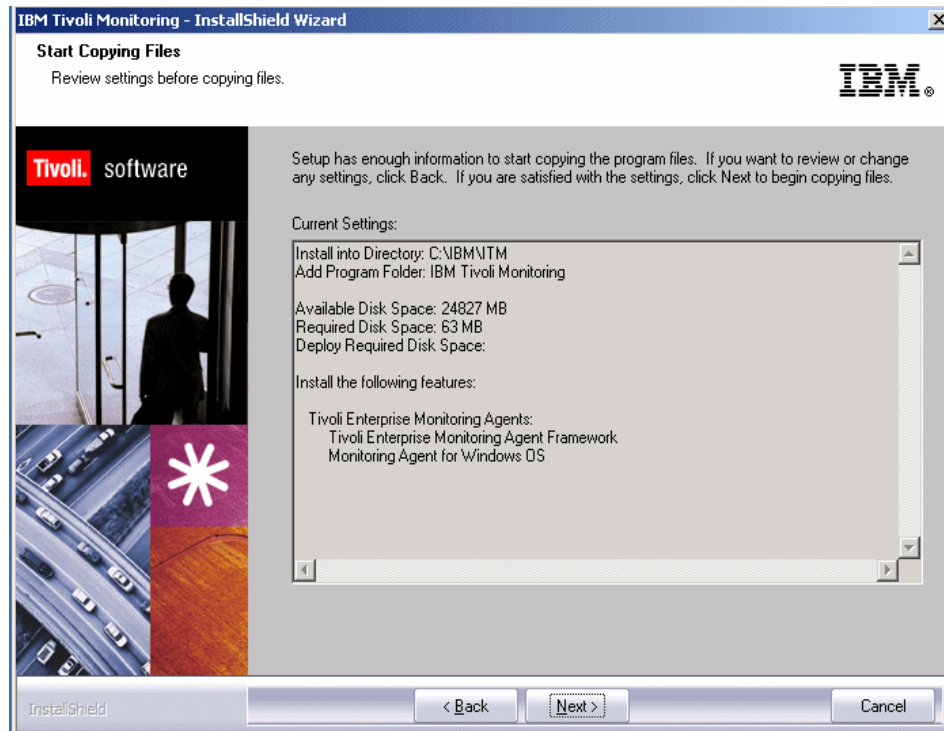


Figure 4-33 Installation summary details

12. Click **Next** to begin configuring the default values for your agent (Figure 4-34 on page 159).

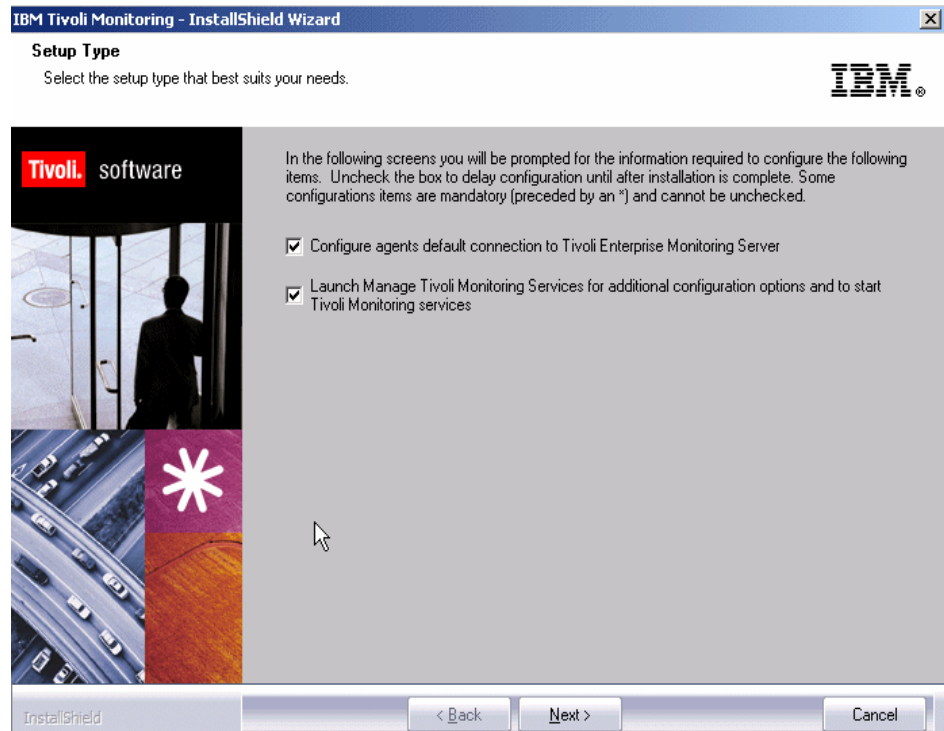


Figure 4-34 Configuration option choice

13. Specify the default values for any IBM Tivoli Monitoring agent to use when they communicate with the monitoring server.
  - a. If the agent must cross a firewall to access the monitoring server, select Connection must pass through firewall.
  - b. Identify the type of protocol that the agent uses to communicate with the monitoring server. You have four choices: IP.UDP, IP.PIPE, IP.SPIPE, or SNA. You can specify three methods for communication - this enables you to set up backup communication methods. If the method you have identified as Protocol 1 fails, Protocol 2 will be used. Click **OK**.

Figure 4-34 shown an example of the protocol communication to be used to communicate with TEMS.

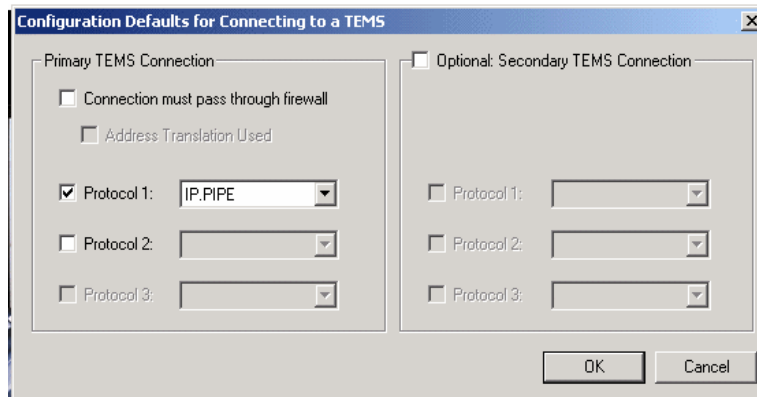


Figure 4-35 Agent communication protocols

14. Complete the following fields to define the communications between agents and the monitoring server. Figure 4-36 shows the primary TEMS the agent will be connected to.

If you have defined more than one TEMS a second window will be opened requesting the configuration of the secondary TEMS hostname.

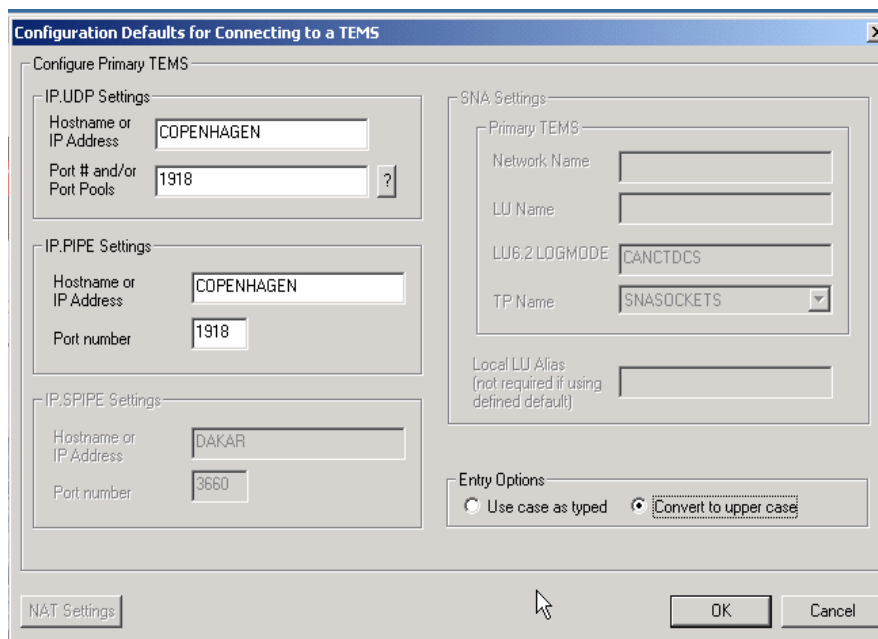
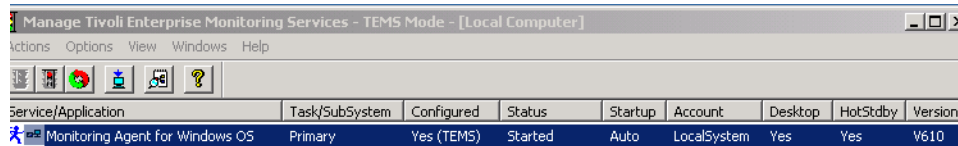


Figure 4-36 Agent's TEMS configuration



15. **Click Finish** to complete the installation.
16. Open the **Manage Tivoli Monitoring Services** utility to see if the monitoring agent has been configured and started as shown on Figure 4-37. If you see “Yes” in the Configured column, the agent has been configured and started during the installation process.



Service/Application	Task/SubSystem	Configured	Status	Startup	Account	Desktop	HotStdy	Version
Monitoring Agent for Windows OS	Primary	Yes (TEMS)	Started	Auto	LocalSystem	Yes	Yes	V610

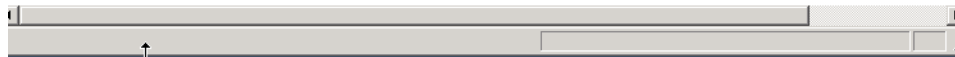


Figure 4-37 Tivoli monitoring services console.

17. If the value in the Configured column is blank and “Template” is in the **Task/Subsystem** column, right-click the **Template** agent and do the following:
  - a. Click **Configure Using Defaults**.
  - b. Complete any windows requiring information by using the agent-specific configuration settings in the User’s Guide for your agent.
  - c. Repeat this step as necessary to create monitoring agent instances for each application instance you want to monitor.

The above procedure will be used by default to configure any agent from a Windows server.

## Installing TEMA on an OS/400 server

Before installing the Monitoring Agent for i5/OS™, complete the following procedures if applicable:

- ▶ During installation, you are required to know whether or not the primary language of your iSeries™ system is the English language. To determine this, complete the procedure described in Section , “Determining the primary language of your iSeries system” on page 162.
- ▶ If you are using TCP/IP for network communications, verify that your TCP/IP network services are configured to return the fully qualified host name of the computer where you will install the monitoring agent as described in “Verifying the TCP/IP configuration” on page 6.
- ▶ If you have a previous version of a Candle Monitoring Agent installed, delete it as described in “Deleting previous versions of the monitoring agent” on page 7.

### *Determining the primary language of your iSeries system*

Use the following procedure to determine the primary language of your iSeries system:

1. Login onto you system using QSECOFR user.
2. From an i5/OS command line, enter the following command:

GO LICPGM

See Figure 4-38.

```

LICPGM                                Work with Licensed Programs
                                     System:  AS20

Select one of the following:

Manual Install
  1. Install all

Preparation
  5. Prepare for install

Licensed Programs
  10. Display installed licensed programs
  11. Install licensed programs
  12. Delete licensed programs
  13. Save licensed programs

More...

Selection or command
===>

F3=Exit  F4=Prompt  F9=Retrieve  F12=Cancel  F13=Information Assistant
F16=AS/400 Main menu
(C) COPYRIGHT IBM CORP. 1980, 2002.
MA a MW A 20/007

```

Figure 4-38 Main OS/400 Menu window

3. Enter 20 (Display installed secondary languages).
4. Note the primary language and description that is displayed in the upper left corner of the window. For an English language system, the primary language is 2924, and the description is English. See example on Figure 4-39.

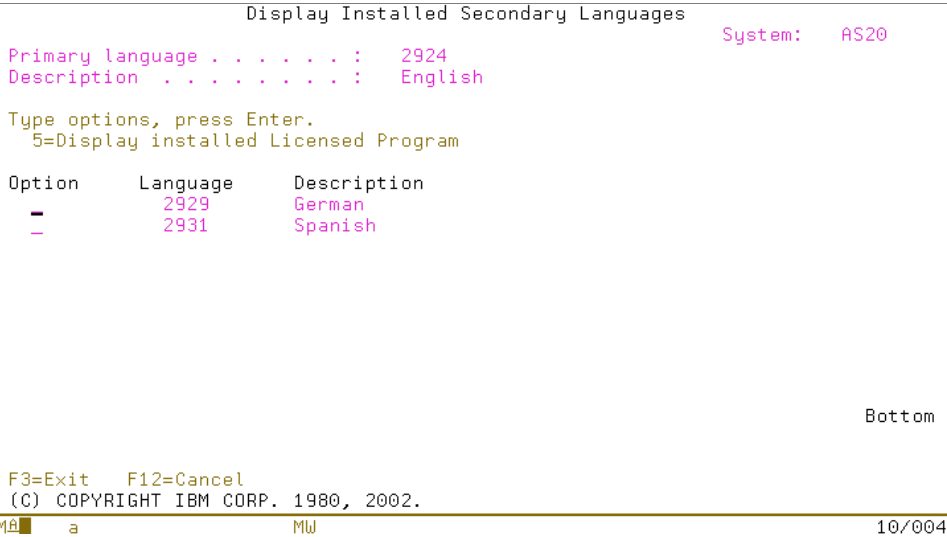


Figure 4-39 Primary language OS/400 definition window

Verifying the TCP/IP configuration

Ensure that your TCP/IP network services are configured to return the fully qualified host name (for example, myhost.ibm.com). The following procedure will show you how to check that TCP/IP on your system is properly configured. This procedure is not necessary if you are using SNA for network communications.

Required authorization role is \*IOSYSCFG.

1. From an i5/OS command line, enter the following command: **CFGTCP**.
2. Select **Work with TCP/IP host tables entries: option 10**.
3. Confirm that the first entry in the Host Name column is the fully qualified host name that is associated with the IP address of the iSeries computer where you plan to install the monitoring agent. If it is not, change the entry to the fully qualified host name. see example below on Figure 4-40 on page 164.

```

Work with TCP/IP Host Table Entries
System: AS20

Type options, press Enter.
  1=Add  2=Change  4=Remove  5=Display  7=Rename

Opt  Internet      Host
     Address      Name
-----
  -   9.3.5.107    AS20
  -                   as20.itsc.austin.ibm.com
  -   127.0.0.1    LOOPBACK
                        LOCALHOST

F3=Exit  F5=Refresh  F6=Print list  F12=Cancel  F17=Position to
Bottom
MA a MW 08/00

```

Figure 4-40 OS/400 TCP/IP configuration panel

4. Return to the Configure TCP/IP menu and select **Change TCP/IP domain information**; option 12.
5. Confirm that a host name and domain name are provided and that they match the entry you just confirmed in the TCP/IP Host Table.
6. Confirm that the first entry for Host name search priority is \*LOCAL.

### ***Installing the monitoring agent***

You can install the Monitoring Agent for i5/OS from a PC or from an iSeries computer, whichever method is more convenient at your site. This procedure includes instructions for both methods.

Required authorization role "Sign on as QSECOFR or with a profile with an equivalent special authority (SPCAUT)":

- \*ALLOBJ
- \*AUDIT
- \*IOSYSCFG
- \*JOBCTL
- \*SAVSYS
- \*SECADM
- \*SERVICE
- \*SPLCTL

**Note:** Before beginning this procedure, install IBM Tivoli Monitoring and the Tivoli Enterprise Portal.

When you finish Configure the Monitoring Agent for i5/OS as described in the previous sections, run the following procedure:

1. From an i5/OS command line, ensure that the QALWOBJRST system value is set to \*ALL. To do this, follow these steps:
  - a. Enter the following command: **WRKSYSVAL QALWOBJRST**.
  - b. Select **5** (Display) and verify that the value is set to \*ALL.
  - c. Press Enter to continue.
  - d. If the value of QALWOBJRST is set to \*ALL, go to step 3. If the value of QALWOBJRST is not set to \*ALL, make note of the values and go to step 2.
2. If the value of QALWOBJRST is not set to \*ALL, follow these steps:
  - a. On the Work with System Values window, enter 2 to change the values.
  - b. On the Change System Value window, change the existing values to \*ALL and press Enter.
  - c. Press F3.
3. From an i5/OS command line, enter the following command to create an i5/OS CCCINST library for the Monitoring Agent for i5/OS installation if this library does not already exist: **CRTLIB LIB(CCCINST)**.
4. Enter the following command to create a save file in the CCCINST library for the Monitoring Agent for i5/OS: **CRTSAVF CCCINST/A4520CMA TEXT('ITM 61 i5/OS')**.

**Note:** When pasting this command to an iSeries session, the single quote (') characters that enclose the text string might be missing. If this happens, manually add the single quote (') characters for the command to work.

5. Transfer the software for the Monitoring Agent for i5/OS to the target iSeries computer. Do one of the following:
  - From a PC, follow these steps:
    - a. Insert the IBM Tivoli Monitoring, V6.1 product CD into the PC CD-ROM drive.
    - b. Enter the following command to create a work folder:  
**WRKFLR**

- c. Select **1 (Create Folder)** and specify the following name for the folder:  
A4FLR.

- d. Enter the following command:

```
WRKLNK QOPT
```

The Work with Object Links window displays the qopt object link.

- e. Select **5 (Next Level)** at the qopt object link to select the next object link; the volume ID of the CD-ROM. Make note of this volume ID for use in the remainder of this procedure.

- f. Continue to select 5 for each link level until the  
/QOPT/volume\_id/OS400/TMAITM6 path is displayed, where volume\_id is  
the volume ID of the CD-ROM drive from step 5e.

- g. Look for the A4520CMA.SAV file and enter the following command to copy  
this save file to the QDLS directory:

```
CPY OBJ('/QOPT/volume_id/OS400/TMAITM6/A4520CMA.SAV')
TODIR('/QDLS/A4FLR')
```

where volume\_id is the volume ID of the CD-ROM drive from step 5e.

- h. Enter the following command to start an FTP session: ftp computer\_name  
where computer\_name is the name of the target i5/OS computer.

- i. Enter the following command to change to the file type to binary: binary

- j. j. Enter the following command:

```
NAMEFMT 1
```

- k. Enter the following command to transfer the software for the monitoring  
agent:

```
put /QDLS/A4FLR/A4520CMA.SAV /QSYS.LIB/CCCINST.LIB/A4520CMA.SAVF
```

- l. Enter F3 and select **1** to end the FTP session.

- 6. From an i5/OS command line, install the software for the Monitoring Agent for  
i5/OS. Do one of the following:

- If you are installing the monitoring agent on a system that is set to the  
English language (language ID 2924), enter the following command:

```
RSTLICPGM LICPGM(OKA4610) DEV(*SAVF) SAVF(CCCINST/A4520CMA)
```

- If you are installing the monitoring agent on a system that is not set to  
language ID 2924, enter the following two commands:

```
RSTLICPGM LICPGM(OKA4610) DEV(*SAVF) RSTOBJ(*PGM)
SAVF(CCCINST/A4520CMA)
RSTLICPGM LICPGM(OKA4610) DEV(*SAVF) RSTOBJ(*LNG) LNG(2924)
SAVF(CCCINST/A4520CMA) LNGLIB(QKA4LNG)
```

7. If you plan to install other monitoring agents, leave the value of QALWOBJRST set to \*ALL until you are finished. If you do not plan to install other monitoring agents, change the value of QALWOBJRST to the values you recorded in 1d on page 8.
8. Optional: Enter the following command to delete the installation library, which is no longer needed: **DLTLIB CCCINST**
9. Optional for an iSeries computer: Delete the A4520CMA.SAV file from your folder. Follow these steps:
  - a. Enter the following command: **WRKDOC FLR(A4FLR)**
  - b. Enter 4 for the A4520CMA.SAV file.
  - c. Press Enter to return to the command line.
  - d. Enter the following command to delete the installation folder: **WRKFLR**
  - e. Enter 4 for the A4FLR folder.
  - f. Press F3 to return to the command line.

### ***Configuring the Monitoring Agent for i5/OS***

Use the following procedure to configure or reconfigure the network connections between the Monitoring Agent for i5/OS and the Tivoli Enterprise Monitoring Server (monitoring server).

1. From an i5/OS command line, enter the following command:  
`GO OMA`
2. Enter **4 (Configure Tivoli Monitoring: i5/OS Agent)**. The Config i5/OS Monitoring Agent (CFGOMA) window is displayed.
3. Enter your site's values for the configuration parameters as shown in Figure 4-41 on page 168.

```

Config i5/OS Monitoring Agent (CFGOMA)

Type choices, press Enter.

TEMS SNA location . . . . . *NONE
TEMS TCP/IP address . . . . . '9.3.5.50'
TEMS IP.PIPE address . . . . . '9.3.5.50'
Secondary TEMS SNA location . . *NONE
Secondary TEMS IP address . . . '9.3.5.48'
Secondary TEMS IP.PIPE address . '9.3.5.48'
Partition name . . . . . *SAME
Firewall in use . . . . . *NO *YES, *NO
TEMS TCP/IP port address . . . . 1918 Address, *SAME
TEMS SNA port address . . . . . *NONE Address, *SAME
TEMS IP Pipe port address . . . . 1918 Address, *SAME
Action user profile . . . . . QAUTOMON QAUTOMON, NAME ,*SAME

F3=Exit F4=Prompt F5=Refresh F10=Additional parameters F12=Cancel
F13=How to use this display F24=More keys

[A] a MW

```

*Figure 4-41 Configuring the monitoring agent*

4. Optional: Customize the data collection intervals by changing the values of the following configuration variables in the KMSPARM(KBBEV) file, which are listed with their default values:

- KA4\_JOB\_DATA\_INTERVAL=15
- KA4\_IOP\_DATA\_INTERVAL=30
- KA4\_DISK\_DATA\_INTERVAL=30
- KA4\_POOL\_DATA\_INTERVAL=15
- KA4\_COMM\_DATA\_INTERVAL=60

Valid values for these configuration variables are 15, 30, 60, 120, and 240. These configuration variables follow the rules of the collection interval parameter of the i5/OS QPMWCOL API. Keep the following items in mind:

- Disk and IOP-related data require a minimum of 30 seconds between collection intervals.
- Communication-related data requires a minimum of 60 seconds between collection intervals.
- Collect job-related data as infrequently as possible to minimize the impact on system performance.
- The i5/OS collection services performance data collector supports data collection at one-minute intervals, not at two or four-minute intervals.



Therefore, when using the API and requesting data at two or four-minute intervals, the data is collected at one-minute intervals, but reported back every two or four minutes.

5. Optional: Customize the time interval for custom situations by changing the value of the following configuration variable in the KMSPARM(KBBEV) file, which is listed with its default value:

KA4\_COMM\_SIT\_INTERVAL=3600

**Note:** Custom situations created using APPN Topology or communication attributes use the time interval specified by the KA4\_COMM\_SIT\_INTERVAL configuration variable. Change the value of this configuration variable if you communication-related alerts to be raised at a different interval. The default interval is set to 3600 to prevent overloading the monitoring agent, because these custom situations are also created as a workaround for a known problem of agent failure when running consecutive APPN reports or running a situation after running an APPN report. These situations might be continuously running and based on events and can overload the monitoring agent when alerting for these conditions.

## Starting the monitoring agent

The following steps will show how to star the Monitoring Agent for i5/OS.

### Background information

When the Monitoring Agent for i5/OS is started, you can use the associated CLI commands. The table shows the group profiles that are authorized to these commands by default when the Monitoring Agent for i5/OS is first installed. A check mark in a column indicates that users associated with that group profile can use the command.

Table 4-7 Commands owned by QSYS with \*PUBLIC \*CHANGE

Command	QSRV	QSRVBAS	QSYSOPR	QPGMR
CFGOMA	√			
DSPOMALOG	√	√	√	√
ENDOMA	√		√	
STROMA	√		√	

To determine which group profile a user is associated with, use the **Display User Profile (DSPUSRPRF)** command. The group profile to which the user is associated is listed in the group profile field.

**Required authorization role**

\*USER or, in some cases, \*JOBCTL special authority if authorities for QAUTOMON were changed after installation

**Starting the agent**

1. From an i5/OS, enter the following command:

```
GO OMA
```

You will be presented the following window (Figure 4-42).

```

OMA                                Tivoli Monitoring: i5/OS Agent
                                     System:  AS20
Select one of the following:

1. Display  Tivoli Monitoring: i5/OS Agent Log
2. Start    Tivoli Monitoring: i5/OS Agent
3. End      Tivoli Monitoring: i5/OS Agent
4. Configure Tivoli Monitoring: i5/OS Agent

Selection or command
==> _

F3=Exit   F4=Prompt   F9=Retrieve   F12=Cancel   F13=Information Assistant
F14=Roll Off      F16=AS/400 Main menu
(C) Copyright IBM Corp. 2005.
MA a MW 20/007

```

Figure 4-42 Monitoring agent configuration window

2. Enter **2** (Start Tivoli Monitoring: i5/OS Agent). The greater than character (>) preceding option 2 indicates that the monitoring agent is not started. When the monitoring agent is started the greater than character (>) is not displayed.

**Important:** If you did not seed the hub and Remote TEMS during their installation with this type of application (i5/OS), you will have to do it before the agent be up and running properly. By default i5/OS is selected for seeding during TEMS installation. You can verify the supported application by using the command line *cinfo* on the Hub and Remote TEMS.

**Note:** Use the same procedure to stop the monitoring agent selecting the option 3.

## Deploying TEMA from TEPs

In order to deploy a monitoring agent through the portal, you have to deploy first the O.S monitoring agent on the system and then you will be able from the TEP deploy any other agent.

**Note:** You will need also to install the bundles on the server where the monitoring agent is being deployed.

Use the following steps to deploy an agent through the portal GUI:

1. Open the Tivoli Enterprise Portal.
2. In the Navigation tree and navigate to the computer where you want to deploy the agent.
3. Right-click the computer and click **Add Managed System**.
4. Select the agent that you want to deploy and click **OK**.
5. Select the configuration fields required for the agent. For information about these fields, see the configuration documentation for the agent that you are deploying.
6. Click Finish.
7. If the computer where you are deploying the agent already has a version of that agent installed, you can either stop the deployment or, if the existing version is older than the version you are deploying, specify to replace the existing agent with this new agent. To replace the existing agent, click **Yes**.
8. Click **Finish** on the message that tells you that deployment was successful.

### 4.2.9 Deploying TEMA from command line interface

In many cases you will need to create a node (i.e. install an O.S agent) from the command line. Before beginning the procedure you have to be sure the packages are already in the depot server from where you will execute the commands.

#### Deploying a Windows O.S Agent from a Remote TEMS using command line

1. Check if the target platform bundles are already installed in the server. Execute the following command:

```
tacmd login -s tems_hostname -u tems_user -p tems_password
```

where:

- **tems\_hostname** is the hostname from where you want to initiate the installation
  - **tems\_user** is the userid on the tems\_hostname
  - **tems\_password** tems\_hostname password
2. Execute the following:
 

```
tacmd listBundles
```
  3. If the bundles are not present, execute the following commands to add them on the server:
 

```
cd image_dir
```

where image\_dir is the directory, where you untar the IBM Tivoli Monitoring, V6.1 codes.

```
tacmd addBundles -i bundles_path
```
  4. Deploy the agent on the targeted server executing the following command:
 

```
tacmd createNode -h server -u user -w password -d target_directory
```

The example below installs the Window agent on london from copenhagen using the *-p* option to set the agent properties:

---

*Example 4-8 Deploying the agent on the targeted server*

---

```
C:\>tacmd createNode -h london -u Administrator -w **** -d c:/IBM/ITM -p
KEY=IBMTivoliMonitoringEncryptionKey PROTOCOL1=IP.PIPE PROTOCOL2=IP.UDP
PORT=1918 SERVER=COPENHAGEN BSERVER=EDINBURG BPROTOCOL1=IP.UDP
PROTOCOL2=IP.PIPE PORT=1918
KUICCN001I Initializing required services...
KUICCN039I Attempting to connect to host london ...
KUICCN050I Distributing file 203 of 203 (85.9 MB / 85.9 MB)...
KUICCN002I Beginning the installation and configuration process...

KUICCN057I The node creation on host london was successful.

KUICCN065I The node creation operation was a success.
```

---

## Deploying an application agent from a Remote TEMS using command line

The same procedure can be used to installed a monitored agent using *addSystem* option instead of *createNode*. The following command line will perform this operation:

```
tacmd addSystem -t type -n node_name -p SECTION.NAME=value ....
```

The following example shows how to deploy a Microsoft SQL Server agent on nice server to monitor the wproxy database instance:

*Example 4-9 Deploying an application agent*

---

```
tacmd addSystem -t OQ -n Primary:nice:NT -p DBSETTINGS.db_sid=MyServer
DBSETTINGS.db_login=sa DBSETTINGS.db_password=sapwd
"DBSETTINGS.db_home=c:\Program Files\Microsoft SQL Server\MSSQL"
"DBSETTINGS.db_errorlog=C:\Program Files\Microsoft SQL
Server\MSSQL\LOG\ERRORLOG" INSTANCE=wproxy
```

---

## Starting the TEMA from the Remote TEMS

Once the agent installed you have to start it executing the following procedure:

1. Login to the agent Remote TEMS executing the following command line  

```
tacmd login -s remote_tems -u user -p password
```
2. Now you are logged in you can execute the command line to start the agent.

```
tacmd startAgent -n hostname -t pc
where pc is the product code (lz for Linux, nt for windows, um for
universal agent and so on).
```

## 4.2.10 Installing a new managed systems - Microsoft Exchange example

We will use the Microsoft Exchange Server deployment as an example of deploying a new managed system on TEMS environment.

### Installing the OS Agent

First of all install the OS Agent on the Microsoft Exchange Server. To perform this task refer to “Tivoli Enterprise Monitoring Agent - TEMA” on page 143. You can either install the OS Agent locally or remotely using **tacmd createNode** command line.

### Installing the Application Agent

Once you’ve installed the OS Agent, proceed with the Microsoft Exchange Server Agent installation. You can refer to the procedure in “Installing TEMA on a Window Server” on page 150 if you want to install the agent locally, or “Deploying TEMA from TEPS” on page 171 if you want to deploy the agent from the TEPS. If you want to deploy the agent from a TEMS command line interface, you can refer to “Deploying an application agent from a Remote TEMS using command line” on page 172.

## Install the support for the agent being deployed

Install the support on the Hub TEMS, the Remote TEMS and the TEPs.

**Note:** If you fail to install the support (seed) for the agent, you will be able to see the agent on the TEP, but when you click on the attribute group, you will not see any data. Instead, you will see a message saying that the request has failed.

### 4.2.11 Tivoli Enterprise Portal -TEP

There are two ways to access the Tivoli Enterprise Portal: Browser and Desktop client. The browser based client has two main advantages. Firstly there is no need to install an updated client if there is a newer version available; the browser client will always be at the latest level available from the server. Secondly you can store links to some of your favorite workspaces as you would store any other link in a browser. The only downside to the browser based client is the fact that you lose desktop real state due to the headers of the web browser itself. From a functional point of view, there are no differences between the two.

**Tip:** IBM Tivoli Monitoring, V6.1 requires IBM Java V 1.4.2 installed on all the systems where the TEP browser client will be initiated. One likely error which signifies this: KFWITM215E - unable to process login request.

#### Installing Tivoli desktop client on a Window machine

Use the following steps to install the desktop client for Tivoli Enterprise Portal:

1. On the computer where you want to install the desktop client, start the installation wizard by launching the **setup.exe** file from the installation media.
2. Click **Next** on the welcome window.
3. Accept the software license by clicking **Accept**.
4. Read the information regarding potentially missing prerequisites and click **Next**.
5. Specify the directory where you want to install the portal software and accompanying files. The default location is C:\IBM\ITM. Click **Next**.
6. Type an encryption key to use. This key should be the same as the one used during the installation of the portal server to which the client will connect. Click **Next** and then **OK** to confirm the encryption key.
7. Select **Tivoli Enterprise Portal client**.

8. If you want to view IBM Tivoli Enterprise Console events through the Tivoli Enterprise Portal, expand **Tivoli Enterprise Portal client** and ensure that **Tivoli Enterprise Console GUI Integration** is selected.
9. Click **Next**.
10. Click **Next** without selecting any agents to deploy.
11. Specify the program folder name and click **Next**.
12. Confirm the installation details and click **Next** to start the installation. After the installation is complete, a configuration window is displayed.
13. Click **Next** to configure the connection to the portal server, the connection to the monitoring server, and to launch Manage Tivoli Monitoring Services.
14. Type the host name of the portal server and click **OK**.
15. Configure the default connection to the monitoring server:
16. If the agent must cross a firewall to access the monitoring server, select **Connection must pass through firewall**.
17. Identify the type of protocol that the agent uses to communicate with the hub monitoring server. Click **OK**.
18. Complete the following fields (refer to Table 4-5 on page 125) for the monitoring server.
19. Click **Finish** to complete your installation.

## Installing the desktop client on a Linux machine

Use the following steps to install and configure the portal desktop client on a Linux computer:

### *Installing the desktop client*

Use the following steps to install the portal server and desktop client:

1. In the directory where you extracted the 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 change the directory as per your needs.
3. Type y to create this directory when prompted. If the directory already exist, you will receive the following type of message:

```
CANDLEHOME directory "/opt/IBM/ITM" already exists.  
OK to use it [ y or n; "y" is default ]?  y
```

Select option 1 when the following message is displayed:

*Example 4-10 Selecting install options*

---

Select one of the following:

- 1) Install products via command line.
- 2) Install products to depot via command line.
- 3) Exit install.

Please enter a valid number:

---

4. Type 1.
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 an encryption key to use and press Enter. This key should be the same key as that used during the installation of the portal server to which the client will connect. A numbered list of available operating systems is displayed. If you have already installed other IBM Tivoli Monitoring, V6.1 components on that machine, the key should already be defined and you will receive the following message  

```
runGSkit      : Keyfile.kdb already exists, skipping keyfile and
certificate creation.
```
9. Press Enter to accept the O.S type; the default value is your current operating system. If not, type the number for the operating system that you are installing on.
10. Type y to confirm the operating system and press Enter. A numbered list of available components is displayed.
11. A list of products will be presented to you as shown below. Type the number corresponding to the TEP Desktop client: 6.

*Example 4-11 List of products*

---

The following products are available for installation:

- 1) IBM Eclipse Help Server V610R104
  - 2) Monitoring Agent for Linux OS V610R115
  - 3) Monitoring Agent for UNIX Logs V610R121
  - 4) Summarization and Pruning agent V610R141
  - 5) Tivoli Enterprise Monitoring Server V610R215
  - 6) Tivoli Enterprise Portal Desktop Client V610R172
  - 7) Tivoli Enterprise Portal Server V610R172
  - 8) Tivoli Enterprise Services User Interface V610R194
  - 9) Universal Agent V610R229
  - 10) all of the above
-



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. Installation is complete. The next step is to configure the desktop client.

Once the installation finished you will receive the following message:

---

*Example 4-12 Installation complete message*

---

Installation step complete.

You must install TEMS support for the agent products.  
This is done by starting and seeding the TEMS for the supported agents.

You may now reconfigure any installed IBM Tivoli Monitoring product via the "/opt/IBM/ITM/bin/itmcmd config" command.

---

14. Next is to configure the TEP desktop client on the server.

### ***Configuring the portal desktop client on Linux***

Use the following steps to configure the desktop client on Linux:

1. At the command line change to the opt/IBM/ITM/bin directory.
2. Run the following command:  
`./CandleConfig -A cj`
3. Type your TEP instance and press Enter or just press Enter to use the default instance name. We use tep\_ankara, ankara being the server name where we are installing TEP.
4. Type the host name for the portal server and press Enter.
5. Then type your browser path directory and type Enter.
6. Press Enter when you are asked if you want to use HTTP Proxy support. The default value is no. The desktop client is now configured. The next step is to start the portal server and portal desktop client.

The example below shows the TEP desktop configuration on server ankara.

---

*Example 4-13 TEP desktop configuration*

---

```
[root@ankara bin]# ./CandleConfig -A cj
CandleConfig      : installer level 400 / 100.
CandleConfig      : running li6243 jre.
Agent configuration started...
Enter TEP Instance Name(Default is: none): tep_ankara
TEP Server Hostname(Default is: none): berlin
Browser Path(Default is: /usr/bin/mozilla):
HTTP Proxy Support? [YES or NO] (Default is: no):
```

Agent configuration completed...

---

7. Seed the TEMS executing the following command line:

```
./CandleSeed -t tems_name pc
```

where pc = cj

8. Start the agent executing the following command:

```
./itmcmd agent start cj
```

## 4.2.12 Warehouse Proxy installation and configuration

This section will describe the different steps on installing and configuring a Warehouse Proxy agent. The Tivoli Data Warehouse needs a relational database to store the historical data. DB2 UDB is the preferred database, but MS SQL and Oracle are also supported. The product ships with a copy of DB2 UDB.

### Pre-installation configuration

Before initiating the Warehouse Proxy agent (WPA) installation and configuration, you need to create a Windows user.

**Note:** ITMUser is default user used in the WPA.

#### *Creating a Windows user*

Use the following steps to create Windows user called ITMUser; remember that the database used for this Redbook is DB2 so depending on the one you are using the configuration can be different:

1. Open the Computer Management window.
2. In the navigation pane of the Computer Management window, expand **Local Users** and **Groups** by clicking on the plus sign (+).
3. Right-click the **Users** folder and click **New User**.
4. Type ITMUser in the User Name field.
5. Type marath0n in the Password field. Type the password again in the Confirm password field to confirm it.

**Note:** If you have security concern you can set a different user and password.

6. Clear **User must change password at next logon** checkbox.
7. Click **Create** to create the user.
8. Click **Close** to close the window.

9. Click the **Groups** folder.
10. Double-click **DB2ADMNS** in the right pane of the window.

**Note:** DB2ADMNS group is created with the DB2 database installation.

11. Do the following step if you are using Windows 2003:
  - a. Click **Add**.
  - b. Type ITMUser in the Enter the names to select field and click **Check Names**.
  - c. Click **OK** and then click **OK** again.
12. Do the following step if you are using Windows 2000:
  - a. Click **Add** in the Administrator Properties window.
  - b. Locate ITMUser, the new user you created, and select it.
  - c. Click **Add**.
13. Click **OK** successively twice to close the Administrator Properties window.
14. Close the Computer Management window.

**Important:**

1. You will need to create a database for the IBM Tivoli Monitoring Warehouse proxy if you are using a non DB2 database or you are using DB2 database on a unix server, you will also need to create in to create an ODBC that point to the database you created to store the data in the datawarehouse proxy.

Execute the following command to create the wproxy database in your DB2 RDBMS:

```
db2 create database wproxy using codeset utf-8 territory US
```

2. When creating an Oracle or DB2 database the codeset must also be utf-8.

## Installing the Warehouse Proxy Agent

The Warehouse Proxy is used to upload historical data from agents into the Tivoli Enterprise Data Warehouse for historical reporting. As any other IBM Tivoli Monitoring, V6.1 agent, the Warehouse Proxy agent installation follows the same procedure as the one described in “Installing TEMA on a Window Server” on page 150. Because WPA only runs on Windows platform, you do not need to worry on how to install it on UNIX environment, at least for now.

***Database configuration and installation pre-requisites***

Use the following recommendation when installing you RDBMS on DB2 or Oracle:

**DB2**

You need to have at least DB2 v8.2 FP10. You need also to set the environment variable DB2CODEPAGE=1208 as a system environment on the Windows box where the Warehouse Proxy is installed.

You can find the DB2 Fix Packs at the following address:

<http://www-306.ibm.com/software/data/db2/udb/support/downloadv8.html>

**ORACLE**

If you have Oracle 9.2, you need to upgrade the ODBC Driver to the version 9.2.0.4. You need also to set the environment variable NLS\_LANG=AMERICAN\_AMERICA.AL32UTF8 as a system environment on the windows box where the Warehouse Proxy is installed.

Site for Oracle ODBC drivers:

<http://www.oracle.com/technology/software/tech/windows/odbc/htdocs/utilsoft.html>

**Note:** IBM plans to provide Warehouse Proxy Agent on UNIX/Linux platform as well, but at the GA time only Windows will be supported.

**Configuring the Warehouse Proxy agent**

The next step after having installed the Warehouse Proxy is to configure it to connect to the database in order to insert and retrieve data from the database. The following steps show you how to perform the WPA configuration.

1. From the Manage Tivoli Enterprise Monitoring Services console right click on the Warehouse Proxy and select **Reconfigure**.
2. Click on **OK** when you receive a window message shown in Figure 4-43 on page 181. is displayed.

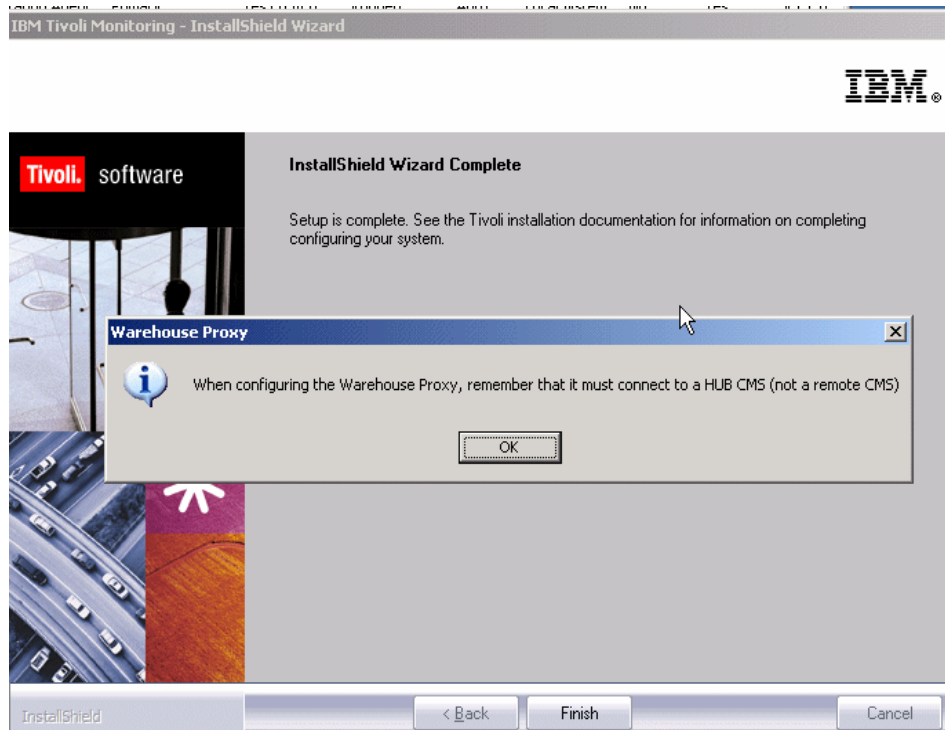


Figure 4-43 Informational window display

3. Configure the protocol communication between the TEMS and the Warehouse Proxy as shown in Figure 4-44 on page 182 and click **OK**.

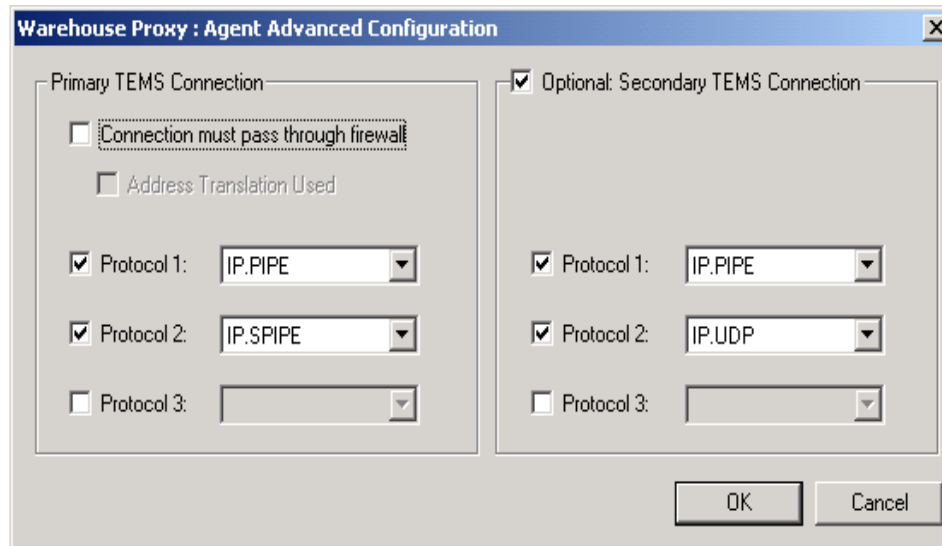


Figure 4-44 Warehouse Proxy agent communication protocol configuration

4. Configure the Hub TEMS hostname and the ports where the Warehouse Proxy will connected to and click **OK**.

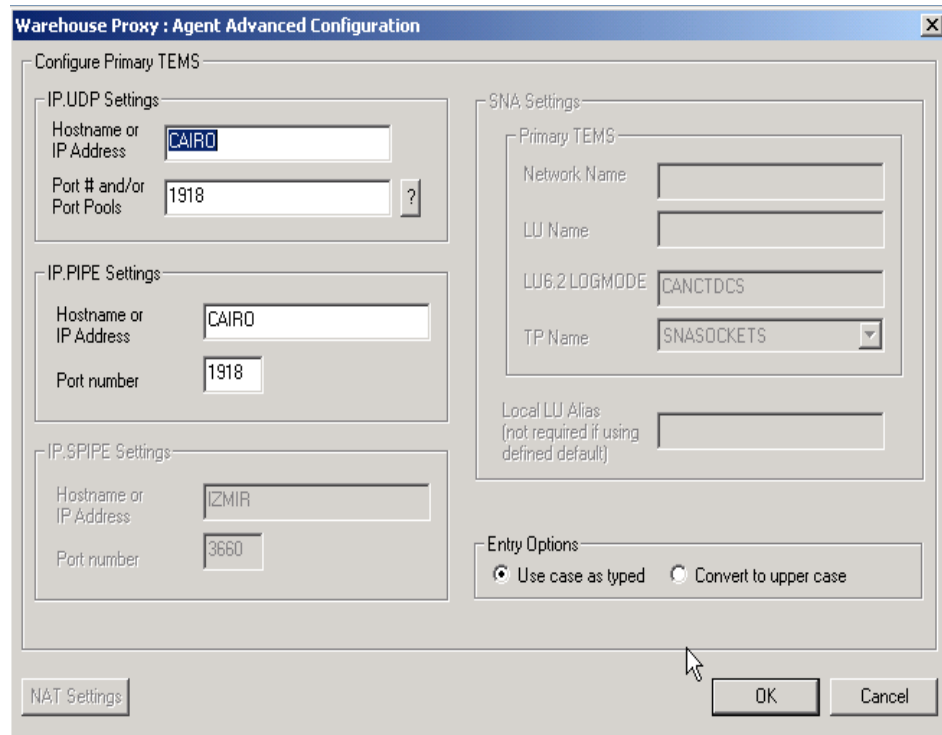


Figure 4-45 Warehouse Proxy agent Hub TEMS and port configuration

5. Click on **OK** when you receive the following pop window (Figure 4-46).

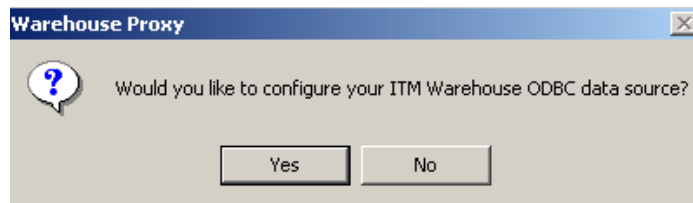


Figure 4-46 ITM Warehouse ODBC configuration confirmation window

6. Select the database the Warehouse Proxy agent you will be using. See Figure 4-47 on page 184.

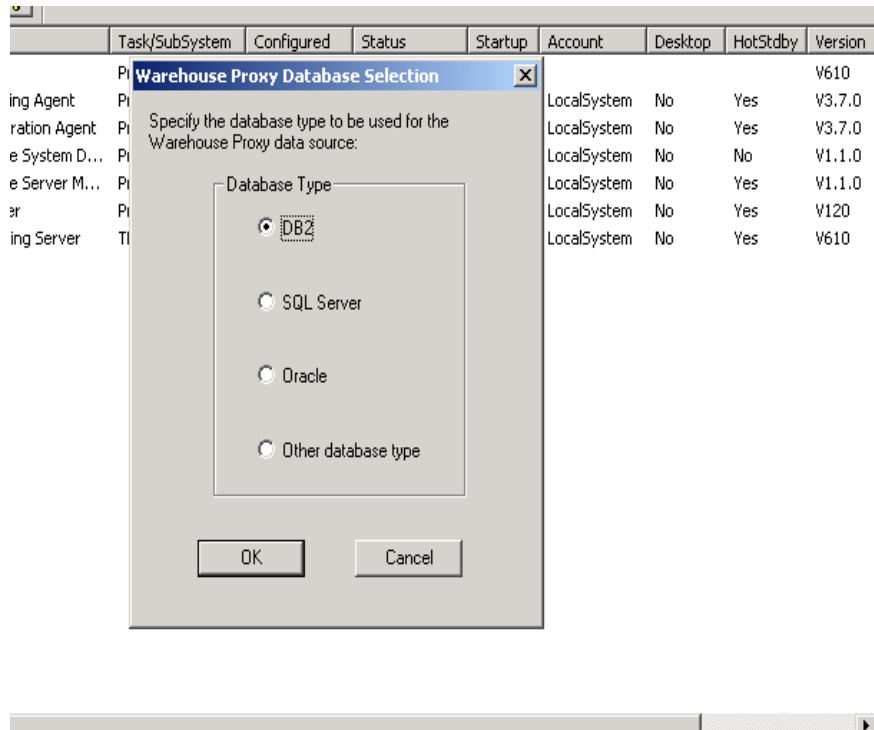
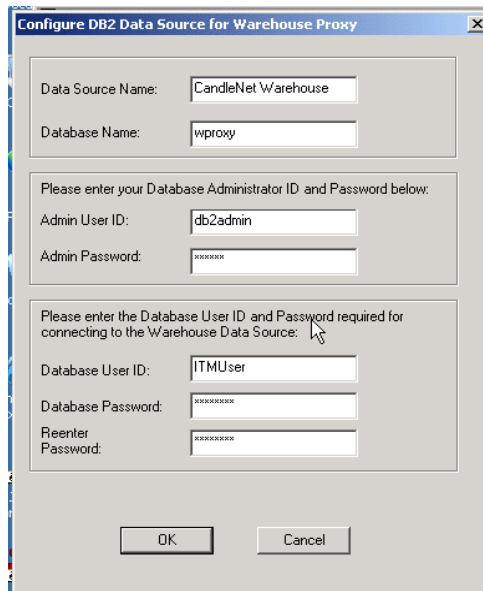


Figure 4-47 Database selection for Warehouse Proxy configuration

7. Fill in the following fields:
  - a. **Data Source Name:** Leave it as ITM Warehouse.
  - b. **Database Name:** Type the name of the database the Warehouse Proxy agent will be using to store the data
  - c. **Admin User ID:** Type the database user administrator, the one created during database installation (default is db2admin for DB2).
  - d. **Admin Password:** The user database administrator password.
  - e. **Database User ID:** Enter with the userid that will own the table created to store warehouse data. This user must be created on the OS first; please refer to “Creating a Windows user” on page 178. the default user is ITMUser.
  - f. **Database Password:** Enter the password of the Database User ID.
  - g. **Reenter Password:** Re-type the password and click **OK**. Refer to Figure 4-50 on page 186.



**Note:** Once this step completed the database and the associated tables will be created on your database.



The dialog box is titled "Configure DB2 Data Source for Warehouse Proxy". It contains three main sections for input:

- Data Source Name:** A text box containing "CandleNet Warehouse".
- Database Name:** A text box containing "wproxy".
- Please enter your Database Administrator ID and Password below:**
  - Admin User ID:** A text box containing "db2admin".
  - Admin Password:** A password box with masked characters.
- Please enter the Database User ID and Password required for connecting to the Warehouse Data Source:**
  - Database User ID:** A text box containing "ITMUser".
  - Database Password:** A password box with masked characters.
  - Reenter Password:** A second password box with masked characters.

At the bottom are "OK" and "Cancel" buttons.

Figure 4-48 Data source configuration window for the Warehouse Proxy

8. Click **OK** on the next popup window stating that the data warehouse was successfully completed as shown on Figure 4-49.
9. Click **OK** on the next popup window stating that the Data Warehouse was successfully completed as shown on Figure 4-49.

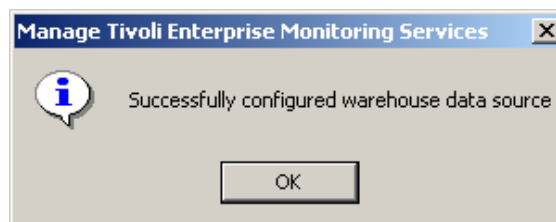


Figure 4-49 Warehouse configuration status message

10. Click **Yes** on the next window (Figure 4-50 on page 186) to complete the configuration.

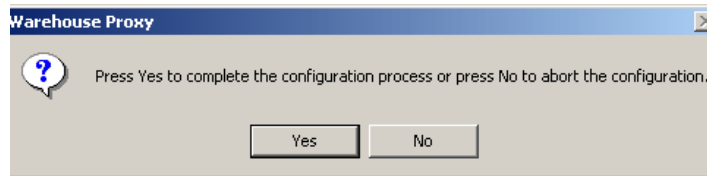


Figure 4-50 Warehouse Proxy database configuration completion

11. Restart the Warehouse Proxy agent double clicking on it.

#### **Important:**

You can change the default ODBC data source name using the following procedure:

- ▶ Edit the windows registry: **regedit**.

Under the registry key:

HKEY\_LOCAL\_MACHINE\SOFTWARE\CANDLE\KHD\Ver610\Primary\Environment

- ▶ Double click the string ODBCdatasource and enter with the ODBC data source name of your choice.

### **4.2.13 Summarization and Pruning agent (SPA) installation and configuration**

The Summarization and Pruning agent is responsible for aggregating the historical data and for pruning to the size of the database according to the desired guidelines. The SPA installation is identical to the other agent installation. We will be focused on this section on how to configure your SPA.

#### **Installing the Summarization and Pruning agent**

SPA is an agent like any other common agent. To install it, follow the procedure described in "Installing TEMA on a Window Server" on page 150 and use "Configuring the Summarization and Pruning agent" on page 186 to make the appropriate configurations.

#### **Configuring the Summarization and Pruning agent**

Once the SPA installed, the next step is to configure when and how data will be collected aggregated and pruned. The following steps describes the procedure to perform those tasks.

1. From your Windows desktop, click **Start->Programs-> IBM Tivoli Monitoring->Manage Tivoli Enterprise Monitoring Services**. On a Linux or UNIX system, cd to install\_dir/bin. Type:

```
./itmcmd manage
```

**Note:** For more details about this command, execute the following: **itmcmd manage ?** or see the *IBM Tivoli Monitoring, V6.1.0 Installation and Setup Guide*, GC32-9407.

2. Right-click Summarization and Pruning agent.
3. Click on **Reconfigure** as shown in Figure 4-51.

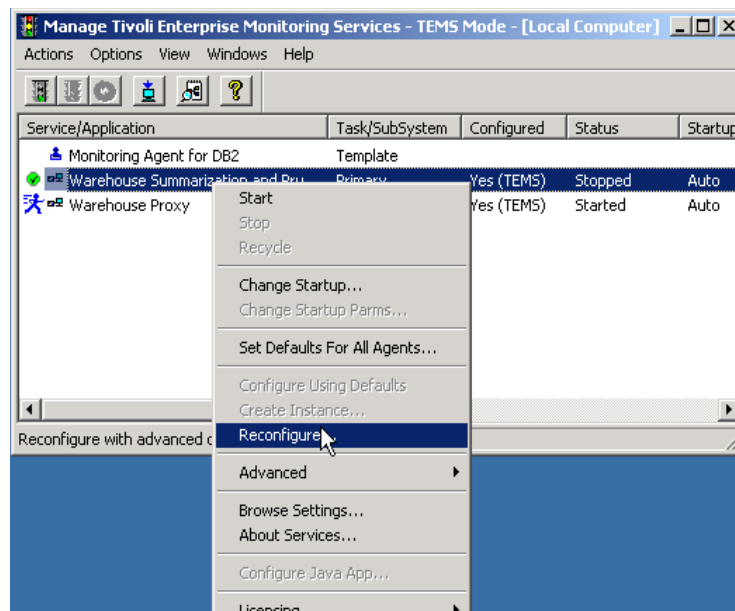


Figure 4-51 Configuring the SPA through the monitoring console

4. Click **OK** in the WarehouseSummarization and Pruning agent: Advanced Configuration window (Figure 4-52 on page 188).

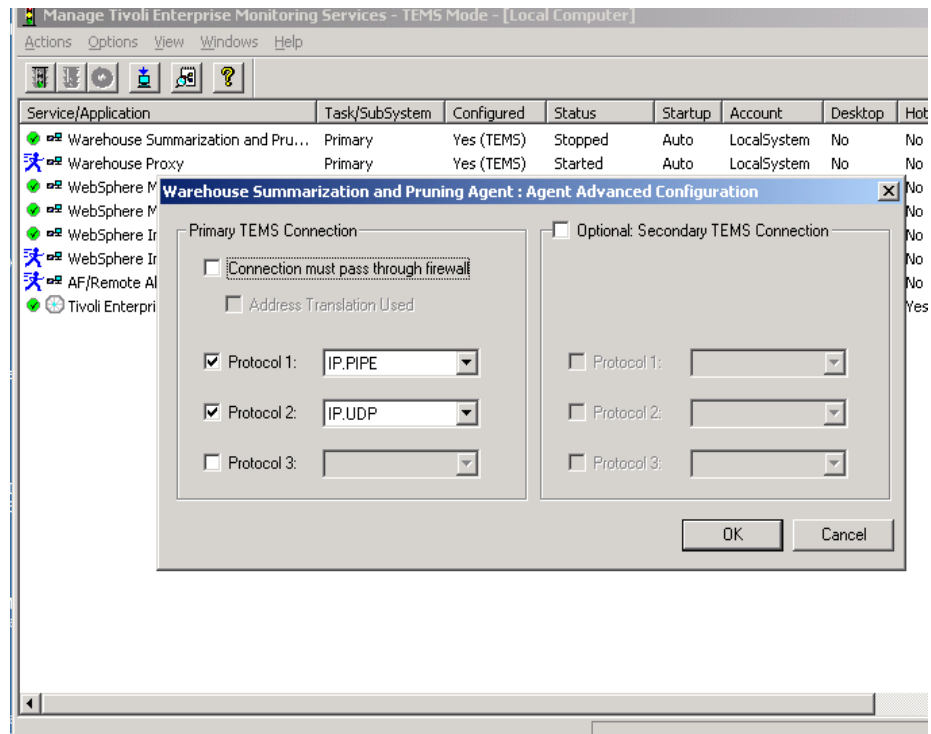


Figure 4-52 Configuring the SPA connection protocol

5. Click **OK** in the next window.
6. Click **Yes** in the WarehouseSummarization and Pruning agent window to configure the Summarization and Pruning agent.
7. Enter the Tivoli data warehouse database and Tivoli Enterprise Portal server information in the Sources tab. Before performing any update check if the default configuration is accurate; if not use the following procedure to update the information:
  - ▶ In the JDBC™ drivers field:
    - Click **Add** to invoke the file browser window to select your JDBC driver, the default is:  
**DB2:** C:\Program Files\IBM\SQLLIB\java\db2java.zip
    - Click **OK** to close the browser and add the JDBC drivers to the list.
    - Highlight an entry in the JDBC drivers list and Click **Delete** to delete a driver.

This gives you the ability to collect JDBC drivers to communicate with your Tivoli data warehouse database. JDBC drivers are installed separately and each database provides a set of these JDBC drivers.

**Notes:**

- ▶ If your Tivoli Data Warehouse database is on UNIX, find the directory where your database is installed and in the jdbc drivers directory, select only the db2jcc.jar and db2java.zip files. For example:  
<db2installdir>/java/db2jcc.jar and db2java.zip.
- ▶ If your Tivoli Data Warehouse database is on MS SQL Server, you install the JDBC drivers from the Microsoft SQL Server website. These are the three files that you need:
  - c:\Program Files\Microsoft SQL Server 2000 Driver for JDBC\lib\msbase.jar
  - c:\Program Files\Microsoft SQL Server 2000 Driver for JDBC\lib\mssqlserver.jar
  - c:\Program Files\Microsoft SQL Server 2000 Driver for JDBC\lib\msutil.jarIn the drop down list, select the type of database for your Tivoli Data Warehouse.

- ▶ Enter the Warehouse URL, Driver, Schema, userid and password.

**Important:** During the configuration of the Warehouse Proxy, a database user (called ITMUser by default) is created. The userid that you enter here must match that database user.

- ▶ Click **Test database connection** to ensure you can communicate with your Tivoli Data Warehouse database.
- ▶ Enter with the Tivoli Enterprise Portal Server Host and Port, if you do not want to use the defaults.

The screenshot shows a Windows-style dialog box titled "Configure Summarization and Pruning Agent". It has five tabs: "Sources", "Defaults", "Scheduling", "Work Days", and "Additional Parameters". The "Defaults" tab is selected. The dialog contains several input fields and buttons:

- JDBC Drivers:** A text box containing "C:\Program Files\IBM\SQLLIB\java\db2java.zip". To its right are "Add" and "Delete" buttons.
- Database:** A dropdown menu showing "DB2".
- Warehouse URL:** A text box containing "jdbc:db2:wproxy".
- Warehouse Driver:** A text box containing "COM.ibm.db2.jdbc.app.DB2Driver".
- Warehouse User:** A text box containing "candle".
- Warehouse Password:** A text box containing "\*\*\*\*\*". Below it is a "Test database connection" button.
- TEP Server Host:** A text box containing "localhost".
- TEP Server Port:** A text box containing "1920".

At the bottom of the dialog are three buttons: "Save", "Reload", and "Close".

Figure 4-53 Configuring the SPA TEPS and database connection

8. Select the settings for your summarization and pruning information in the **Defaults** tab as shown in Figure 4-53.

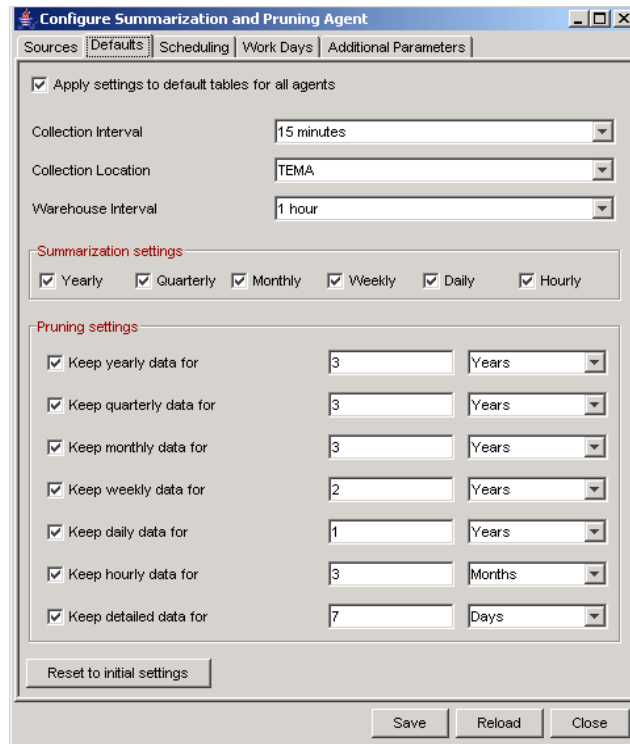


Figure 4-54 Configuring how data will be collected and pruned

- If you click on **Reset**, you change all settings in this window back to the default settings.
  - If you do not want to use the defaults, select the appropriate time periods you want in the Summarization section to change your summarization values.
  - To change your Pruning settings:
    - i. Select the time periods for the pruning of your data; **Keep yearly data** for, **Keep quarterly data** for, and so on.
    - ii. Enter the number of time periods you wish in the next field.
    - iii. Select the 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.
  - Select **Apply settings to default tables for all agents** to keep the changes you have made.
9. Select the scheduling information in the **Scheduling** tab (Figure 4-55).

- Schedule the agent to run every x days.
- Select the hour of the day that you want the summarization to run. The default is to run every day at 2 AM.

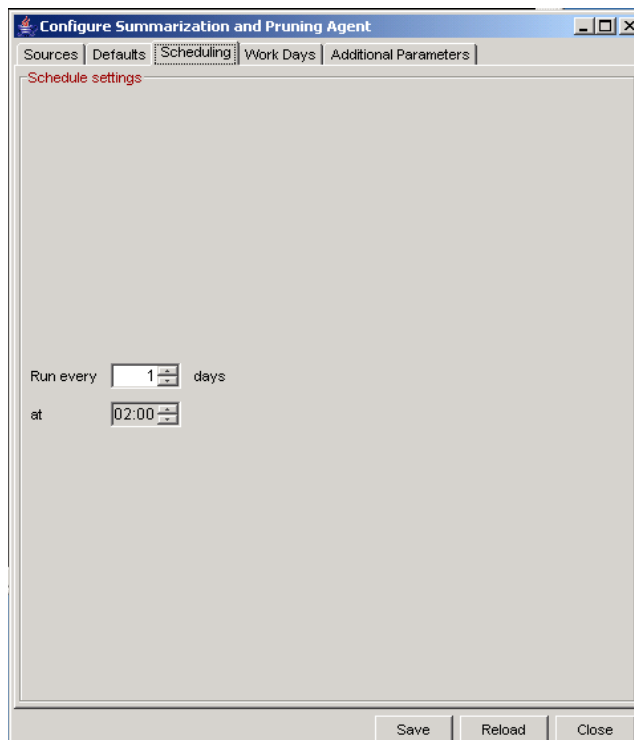


Figure 4-55 Scheduling the d collection and prunization

10. Specify the Shift Information and Vacation Settings in the **Work Days** tab:

- Select day in the **Week starts on**
- To change your shift information:
  - i. If you want to specify shifts, select **Specify shifts**.
  - ii. The default settings for this field are listed in the **Peak Shift Hours** box on the right side of the window.
  - iii. You can change these settings by selecting the hours you want in the Off Peak Shift Hours box and clicking the right arrow button to add them to the Peak Shift Hours box.



**Note:** Changing the shift information after data has been summarized can create an inconsistency in the data. Previous data collected and summarized can not be recalculated with the new shift values.

- To change your vacation settings: a. Select **Specify vacation days**. If you do not want to set your vacation days, do not select this check box.
  - i. Click **Yes** or **No** to specify weekends as vacation days.
  - ii. Select **Add** to add vacation days.
  - iii. Select the vacation days you want to add from the calendar.

**Note:** On UNIX or Linux, right-click, instead of left-click, to select the month and year.

- iv. The days selected display in the box below the Select vacation days field. If you want to delete any days you have previously chosen, select them and click **Delete** (Figure 4-56 on page 194).

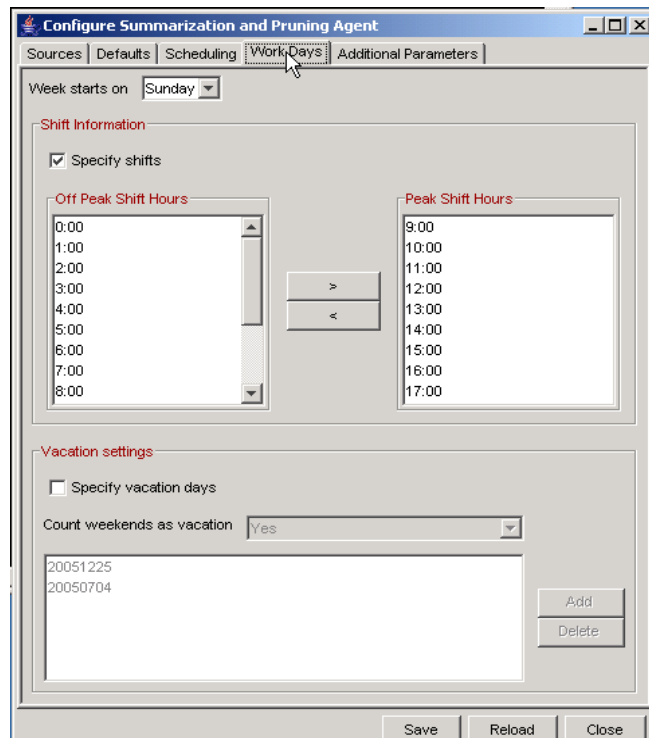


Figure 4-56 Defining shift periods and vacation settings

11. In the Additional Parameters tab, do the following (Figure 4-57 on page 195):
  - a. Specify the maximum rows that can be deleted in a single database transaction. The values are 1 through n. The default is 1000.
  - b. Specify the age of the data you want summarized in the Summarize hourly data older than and Summarize daily data older than fields. Values are 0 through n. The default is 1 for hourly data and 0 for daily data.
  - c. Choose the time zone you want to use from the “Use timezone offset” from the drop down list. If the Tivoli Data Warehouse and agents that are collecting data are all not in the same time zone, and all the data is stored in the same database, use this option to identify the time zone you want to use.

The screenshot shows a window titled "Configure Summarization and Pruning Agent" with a tabbed interface. The "Additional Parameters" tab is selected. The window contains the following fields and controls:

- Maximum rows per database transaction: 1000
- Use timezone offset from: Agent (dropdown menu)
- Summarize hourly data older than: 1 hours
- Summarize daily data older than: 0 days

At the bottom of the window are three buttons: Save, Reload, and Close.

Figure 4-57 Configuring additional parameter for SPA

12. Click **Yes** on the next window to save your configuration (Figure 4-58 on page 196).

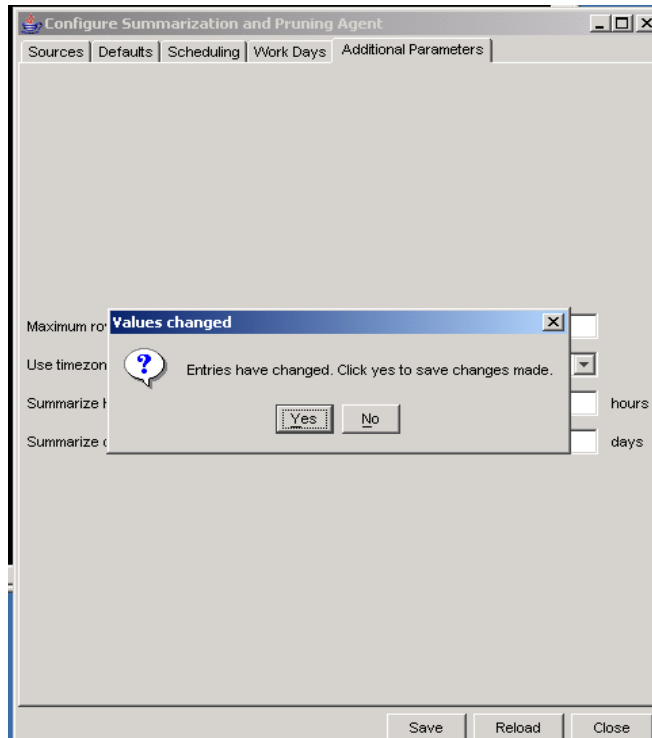


Figure 4-58 Saving the Pruning and Summarization agent configuration

12. The following buttons are visible only on a UNIX or Linux system:

- Click **Save** after you have all your settings correct.
- Click **Reload** to reload the original values.
- Click **Cancel**, at any time, to cancel out of the ConfigureSummarization and Pruning agent window. You are prompted to save any data you have changed.

#### 4.2.14 Event Synchronization installation

Once installed, Event Synchronization components enables IBM Tivoli Monitoring, V6.1 to send events to IBM Tivoli Enterprise Console server, as well as IBM Tivoli Monitoring, V6.1 user to view events from IBM Tivoli Enterprise Console in the Tivoli Enterprise Portal. You need to install the IBM Tivoli Enterprise Console on the event server and configure the TEMS to send events to the IBM Tivoli Enterprise Console server to have those features available. The following table provides an overview of the steps required to install and configure the IBM Tivoli Enterprise Console.

Table 4-8 TEC Event Synchronization installation and configuration steps

Step	Reference
Gather information required during the installation and configuration processes.	"Information to gather before you begin" on page 197
Install the IBM Tivoli Enterprise Console on your event server.	"Installing Event Synchronization on your event server" on page 198
Configure your monitoring server to forward events to IBM Tivoli Enterprise Console.	"Configuring the monitoring server to forward events" on page 209
Start and stop IBM Tivoli Enterprise Console on the monitoring server.	"Starting and stopping the process that sends updates to a monitoring server" on page 210

### Information to gather before you begin

You need the following information to successfully install and configure Event Synchronization between IBM Tivoli Monitoring and IBM Tivoli Enterprise Console:

- ▶ Host names (or IP addresses), userids, and passwords for the monitoring servers that you want to receive events from.
- ▶ Simple Object Access Protocol (SOAP) information to send events to a monitoring server (the URL, the rate to send requests to the server).
- ▶ Event rule base information (either the name of a new rule base to create or the name of an existing rule base to use).

#### Notes:

- ▶ If your IBM Tivoli Enterprise Console event server is running on Windows 2003 and you are planning to install the IBM Tivoli Enterprise Console remotely (using a program such as Terminal Services to connect to that Windows 2003 computer), you need to run the **change user /install** command before you run the installation. This puts the computer into the required "install" mode. After the installation, run the **change user /execute** command to return the computer to its previous mode.
- ▶ If you are running on a UNIX computer, you must configure your TCP/IP network services in the /etc/hosts file to return the fully qualified host name.

## Installing Event Synchronization on your event server

You can install the Event Synchronization either through an installation wizard or from the command line.

**Note:** The IBM Tivoli Enterprise Console event server needs to be recycled during this installation process.

## Configuring the Simple Object Access Protocol (SOAP) on the Hub TEMS

Simple Object Access Protocol (SOAP) is a communications XML-based protocol that lets applications exchange information through the Internet. SOAP is platform independent and language independent. SOAP uses XML to specify a request and reply structure. It uses HTTP as the transport mechanism to drive the request and to receive a reply.

By default, all monitoring servers are enabled for Web Services. Use the following sections to configure IBM Tivoli Monitoring Web Services (SOAP Server) on Windows XP Professional Edition or Windows 2000 computers.

The instructions in this section assume that you have a basic understanding of SOAP, XML and XML Namespaces, and the Web Services Description Language (WSDL).

For complete information about customizing the SOAP interface for your site, refer to *IBM Tivoli Monitoring Version 6.1.0, Administrator's Guide*, SC32-9408.

Table 4-9 on page 198 outlines the steps required to configure SOAP:

Table 4-9 SOAP configuration steps

Steps	References
Define the hubs with which your SOAP Server communicates.	"Defining the Hub TEMS which communicate with SOAP" on page 198
Create users and grant them access.	"Adding users" on page 199
Verify that you have successfully configured SOAP.	"Verifying the SOAP configuration" on page 200

### Defining the Hub TEMS which communicate with SOAP

In this step you use the Manage Tivoli Monitoring Services to activate the SOAP server and define hubs with which the SOAP server communicates.

Use the following steps to define SOAP hubs:

1. Open **Manage Tivoli Monitoring Services**.
2. Right click **Tivoli Enterprise Monitoring Server**.
3. Click **Advanced->Configure SOAP Server Hubs**.
4. Click **Add Hub**. The Hub Specification window is displayed:
5. Select the communications protocol from the Protocol menu.
6. Specify an alias name in the Alias field (For example: SOAP).
7. If you are using TCP/IP or TCP/IP Pipe communications, complete the following fields:
  - ▶ Hostname/ip address corresponds to the hostname/ip address of your Hub TEMS
  - ▶ Port, default is 1920 (as the one to connect to TEPS)

**Note:** If you are connecting to a remote monitoring server, the protocol information must be identical to that used for the hub monitoring server.

8. Click **OK**

### ***Adding users***

In this step you define users on each Hub and specify the access rights for each user (query or update).

Use the following steps:

1. Select the server (click anywhere within the server tree displayed), if necessary.
2. Under Add User Data, type the user name. userids must be identical to those specified for monitoring server logon validation. Access is restricted to only that monitoring server to which a user has access.

**Note:** If you do not supply a userid, all users are given permission to update data.

3. Click the type of user access: **Query** or **Update**.
4. Click **Add User**. The server tree is updated, showing the user and type of access. To delete a user: Select the user name from the tree and click **Delete** Item.
5. To delete a Hub: Click anywhere within the hub's tree and click **Clear Tree**.
6. Once all this steps done you will have a configuration that looks like the Figure 4-59.

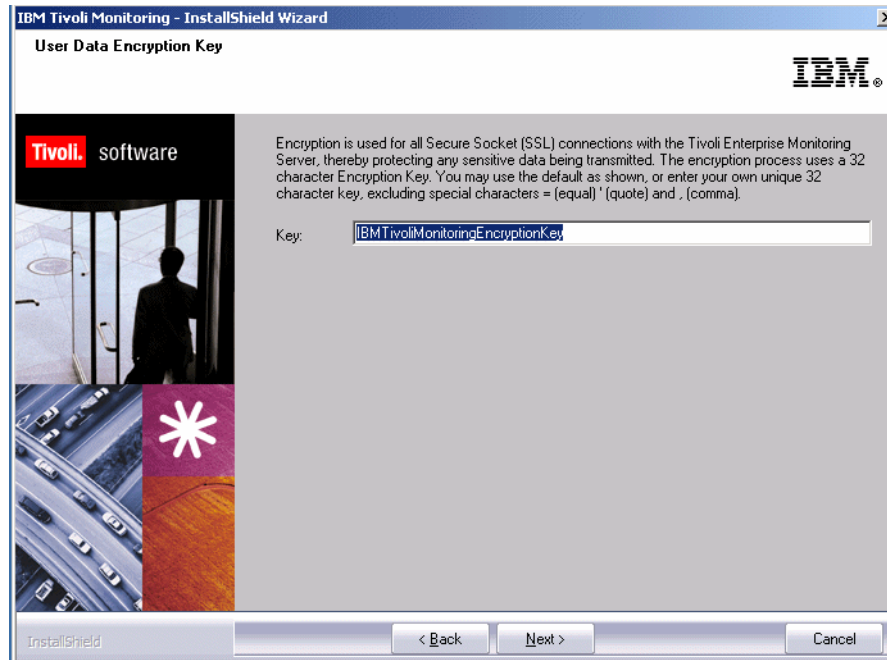


Figure 4-59 SOAP server hub configuration

### **Verifying the SOAP configuration**

In this step you verify that SOAP has been properly configured by starting the SOAP client and making a request using your Internet Explorer Web browser. Use the following steps:

1. From your Hub TEMS type the following address in you Internet browser and press Enter.  
<http://localhost:1920///cms/soap/kshhsoap.htm>
2. A window will be opened where you can enter the type of SOAP request and the endpoint from where you want to retrieve the data. See example on Figure 4-60.



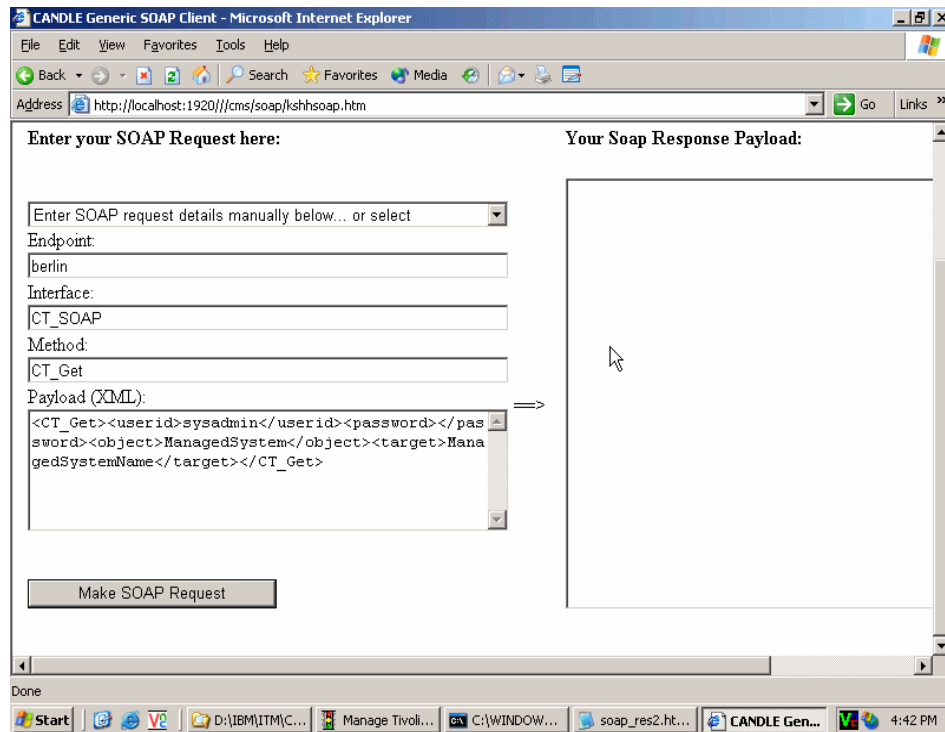


Figure 4-60 SOAP Web interface configuration test

3. Click **Make SOAP Request** button.
4. You will receive the following display in your browser as shown in Figure 4-61 on page 202:

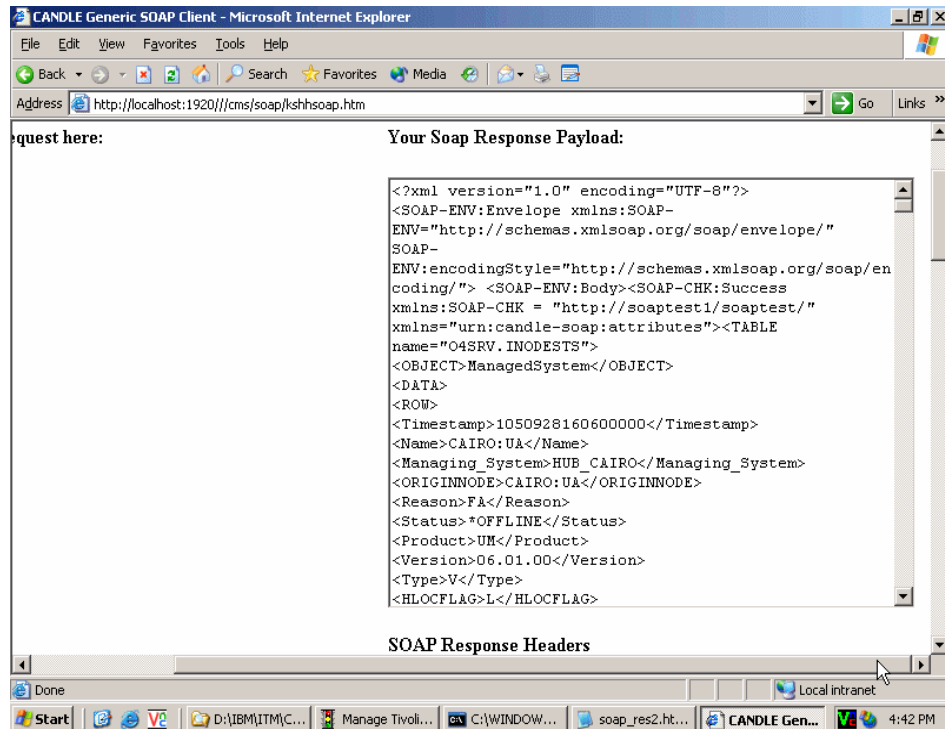


Figure 4-61 SOAP Response

### Installing Event Synchronization from a wizard

Use the following steps to install Event Synchronization from the installation wizard:

**Note:** If your IBM Tivoli Enterprise Console Server is a UNIX machine, you will need to execute the following procedure using a local GUI or an X-Terminal.

1. On the event server, launch the IBM Tivoli Enterprise Console installation by executing the following command:
 

```
cd $install_dir/unix/tec/
./setupAIX.bin
```
2. Click **Next** on the Welcome window
3. Select **Accept** and click **Next** when the license agreement window (Figure 4-62 on page 203) will pop up.

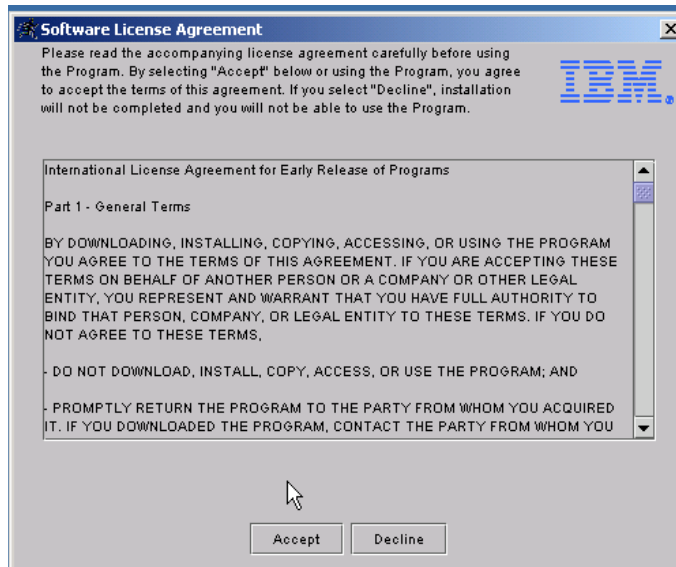


Figure 4-62 Event synchronization Software License Agreement window

4. Complete the following fields as shown in the example below and click **Next**:



Figure 4-63 Event synchronization configuration fields

The Table 4-10 shows each configuration field and its respective description.

Table 4-10 BM Tivoli Enterprise Console Event Synchronization configuration fields

Fields	Description
Name of the configuration file	The name of the file where Event Synchronization configuration information is stored. The default name is situpdate.conf.
Number of second to sleep when no situation updates	The polling interval, in seconds. The minimum (and default) value is 1. If there are no situation events, the process that forwards events to IBM Tivoli Enterprise Console will rest for 1 second.

Fields	Description
Number of bytes to use to save last events	Number of bytes that the long running process will use when it saves the location of the last event it processes. This value must be an integer. The minimum (and default) is 50.
URL of the monitoring server SOAP Server	The URL for the SOAP Server configured on the computer where the monitoring server is running. The default value is cms/soap. This value is used to create the URL to which IBM Tivoli Enterprise Console sends event information. For example, <a href="http://hostname:port///cms/soap">http://hostname:port///cms/soap</a> , where hostname is the host name of the monitoring server and port is the port used by that server.
Rate for sending events from IBM Tivoli Enterprise Console to TEMS via web services	The maximum number of events sent to the monitoring server at one time. The minimum (and default) value is 10 events.
Level of debug detail for log	The level of information for Event Synchronization that will be logged. You have the following choices: <ul style="list-style-type: none"><li>► Low (default)</li><li>► Medium</li><li>► Verbose</li></ul>

5. Complete the information about the files where events will be written upon as describe in Table 4-11 on page 206 when the following window (Figure 4-64 on page 206) pop up, and click **Next**.

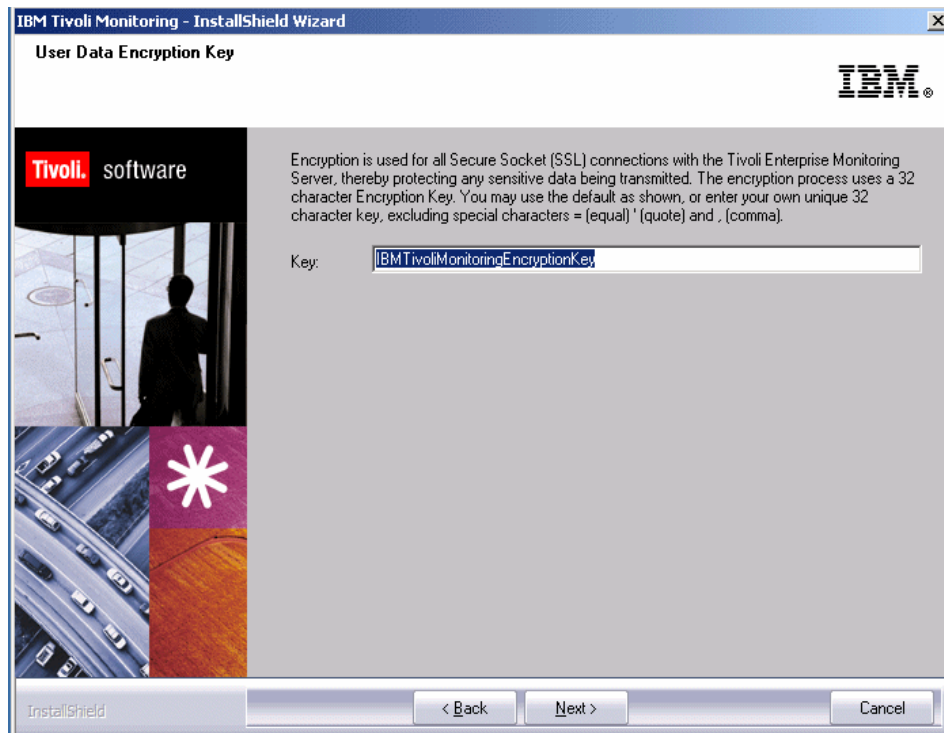


Figure 4-64 Event synchronization cache file configuration window

Table 4-11 IBM TEC Event Synchronization caches file configuration fields description

Fields	Description
Maximum size of any single cache file, in bytes	The maximum permitted size, in bytes, for any one event cache file. The minimum (and default) value is 50000. Do not use commas when specifying this value (50,000 instead of 50000).
Maximum number of cache files	The maximum number of event caches files at any given time. The minimum (and default) value is 10. When this value is reached, the oldest file is deleted to make room for a new file.

Fields	Description
Directory for cache files to reside	<p>The location where event cache files are located. The default locations are as follows:</p> <ul style="list-style-type: none"><li>▶ On Windows: C:\tmp\TME\TEC\OM_TEC\persis tence.</li><li>▶ On UNIX: /var/TME/TEC/OM_TEC/persisten ce</li></ul>

6. Provide hostname, userid and password for each monitoring server with which you want to synchronize events and click **Add**. You must specify information for at least one monitoring server. Figure 4-65 shows an example of TEMS information during the Event Synchronization configuration.

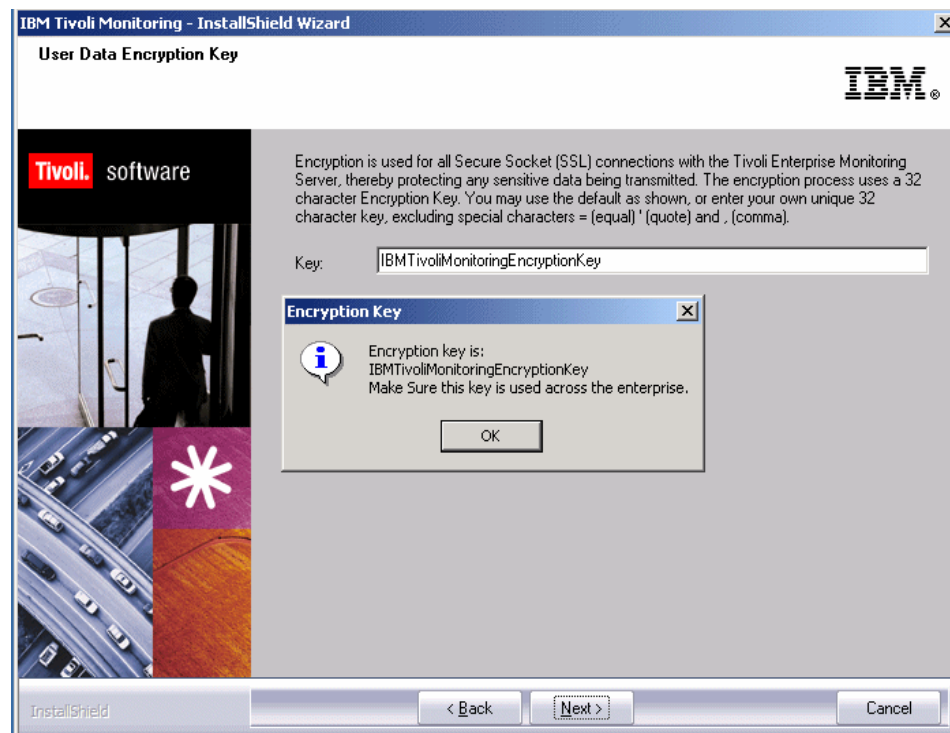


Figure 4-65 Event synchronization Tivoli Enterprise Monitoring Server information

Below is a description of each of the above fields:

- ▶ **Host name:** The fully qualified host name for the computer where the monitoring server is running. This should match the information that will be in events coming from this monitoring server.
  - ▶ **User ID:** The userid to access the computer where the monitoring server is running.
  - ▶ **Password:** The password to access the computer.
  - ▶ **Confirmation:** The password confirmation.
7. When you have provided information about all of the monitoring servers, click **Next**.
  8. Specify the rule base that you want to use to synchronize events. You have two choices:
    - a. Create a new rulebase.
    - b. Use existing rulebase If you select to use an existing rulebase, the IBM Tivoli Enterprise Console BAROC class files (omegamon.baroc and Sentry.baroc [if not present]) and the omegamon.rls ruleset file are imported into your existing rulebase.

We used the second option as we already have IBM Tivoli Enterprise Console set up and running properly. Refer to the Figure 4-66 on page 208.

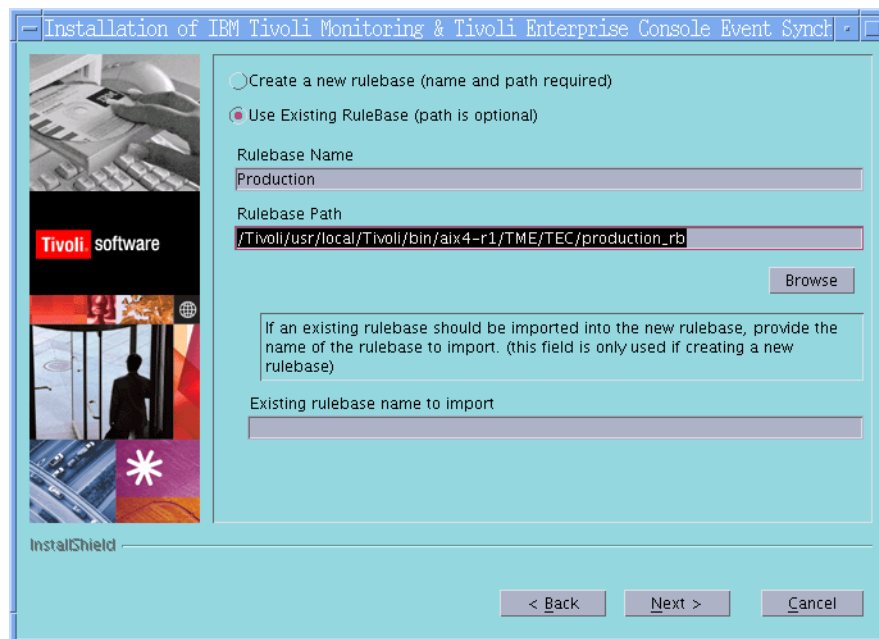


Figure 4-66 IBM Tivoli Enterprise Console rule base configuration



**Notes:**

- ▶ If you are creating a new rule base, type the name for the rule base you want to create and the path to where the new rule base will be located. There is no default location; you must specify a location.
- ▶ If you are using an existing rule base, type the name of the rule base.
- ▶ If you want to import an existing rule base into a new rule base, type the name of the existing rule base in the Existing rulebase to import field. This step is only available if you are creating a new rule base.

9. Click **Next**.

10. Click **Next** on the pre-installation summary panel. The installation begins.

11. When the installation and configuration steps are finished, 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.

If you did not configure the event forwarding during the Hub TEMS installation and configuration, refer to “Configuring the monitoring server to forward events” on page 209

## Configuring the monitoring server to forward events

Before the monitoring server forwards any situation events to IBM Tivoli Enterprise Console, you have to enable that forwarding and the filtering of events.

### *Enabling event forwarding*

Use the following steps to enable event forwarding on your monitoring server:

1. From your Hub TEMS, in Manage Tivoli Monitoring Services, right-click the monitoring server and click **Reconfigure** (Windows) or **Configure** (UNIX).
2. On the configuration options window, select **TEC Event Integration Facility**. For UNIX, click the **TEC** tab to view this configuration option.
3. Click **OK** and then **OK** again.
4. Complete the following fields on the IBM Tivoli Enterprise Console Server: Location and Port Number window and click **OK**:

#### **TEC Server Location**

Type the host name or IP address (using dotted format, such as 0.0.0.0) for the computer where the IBM Tivoli Enterprise Console event server is installed.

### **TEC Port Number**

Type the port number for the event server. Set this value to 0 (when your event server is a UNIX server) unless the portmapper is not available on the event server (as when the event server is running on a Windows server). When you specify 0, the port number is retrieved by the portmapper.

If you want to use the default port (5529), edit the `tec_installdir/TME/TEC/.tec_config` file on the event server and remove the semicolon (;) from the following line: `tec_recv_agent_port=5529`. Port 5529 is often used when the event server is a Window platform.

Once done any error during the installation can be found at the error log file is in `/tmp/tec_sync_install.log`.

5. Click on **Finish**.

### ***Enabling event filtering***

By default, all situation events are filtered out, meaning that they are never forwarded to IBM Tivoli Enterprise Console. Use the following steps to change the filtering on the TEMS servers that forward events to IBM Tivoli Enterprise Console:

1. Open the `om_tec.config` file (located in `<install_dir>\cms\TECLIB\` on Windows and `<install_dir>/tables/<tems_name>/TECLIB` on UNIX).
2. Comment out the following line by adding a pound sign (#) to the beginning of the following line: `Filter:Class=ITM_Generic;master_reset_flag="`;
3. Save and close the file.

### **Starting and stopping the process that sends updates to a monitoring server**

To send event updates to a monitoring server, you must start a long running process called Situation Update Forwarder. This process is started automatically when the event server starts. To stop the process manually, change to the `$BINDIR/TME/TEC/OM_TEC/bin` directory (where `$BINDIR` is the location of the IBM Tivoli Enterprise Console installation) and run the following command:

On Windows:

```
stopSUF.cmd
```

On UNIX:

```
stopSUF.sh
```

On Windows, you can also start and stop the Tivoli Situation Update Forwarder service to start or stop the forwarding of event updates. You can start and stop this service either from the Windows Service Manager utility or with the following commands:

```
net start situpdate
net stop situpdate
```

To start the process, run the following command:

On Windows:

```
startSUF.exe config_file
```

On UNIX:

```
startSUF.sh config_file
```

**Note:** config\_file is the name of the file where IBM Tivoli Enterprise Console configuration information is stored. The default name is /etc/TME/TEC/OM\_TEC/situpdate.conf. Please refer to Figure 4-63 on page 204 and Table 4-10 on page 204 for more details.

## 4.2.15 Configuring the Hot Standby

The optional Hot Standby function enables you to maintain continuous availability by defining a standby monitoring server to provide backup for your hub monitoring server. If the hub monitoring server fails, hub functions automatically switch to the standby monitoring server. IBM Tivoli Monitoring automatically connects all remote monitoring servers and agents to the standby monitoring server. There is no automatic switch that returns control to the hub monitoring server once it is available. If you want to switch back to the hub monitoring server, you must manually stop the standby monitoring server.

Configuring Hot Standby involves the following steps:

1. Install the monitoring server software on the systems you want to use as hub standby (refer to “Installing the backup hub monitoring server” on page 212). We assume that the primary Hub TEMS is already up and running.
2. Configure Hot Standby on the hub monitoring server, the backup monitoring server, and any remote monitoring servers associated with the hub monitoring server; refer to “Configuring Hot Standby” on page 212.

3. Configure Hot Standby on any agents that are associated with the hub monitoring server like the TEPS and the Warehouse Proxy agent; refer to “Configuring the Warehouse Proxy” on page 214.

### Installing the backup hub monitoring server

See “Installing and configuring a Hub TEMS on a Windows server” on page 14 or “Installing a Hub TEMS on a UNIX server” on page 116 for information about installing a hub monitoring server. When you are installing the backup hub monitoring server, use identical values to those you used when installing the primary hub monitoring server.

### Configuring Hot Standby

Configure the hub server, the standby hub server, and any remote servers associated with the hub server.

**Note:** The hub and standby monitoring servers should be configured as mirrors of each other.

### *Configuring Hot Standby on a Window TEMS*

Use the following procedure to configure Hot Standby on a Window TEMS:

1. In Manage Tivoli Monitoring Services, right-click the name of the hub monitoring server and click **Reconfigure** (or **Configure** on UNIX).
2. Select **Configure Standby CMS** and specify the protocols used by the standby server. These protocols should match those specified for the hub server.
3. Click **OK** and then **OK** again on the message that is displayed.
4. Click **OK** on the window that displays the communication settings for this server.
5. Type the host name or IP address for the standby monitoring server in the Hostname or IP Address field and click **OK**.
6. Configure the TEC server name and port in the next window. The default will be the one you configure on your Hub TEMS.
7. Restart the monitoring server.
8. Repeat these steps for the standby monitoring server and any remote monitoring servers.

### *Configuring Hot Standby on a UNIX TEMS*

Use the following procedure to configure Hot Standby on a UNIX TEMS:

1. From the \$CANDLEHOME/bin execute the following command:

```
./itmcmd config -S -t tems_name
```

where tems\_name is the name of the TEMS hosted by UNIX server. See example below where server MADRID is being configured; server cairo being its Hot Standby server:

*Example 4-14 ./itmcmd config -S -t HUB\_MADRID output*

---

```
[root@madrid][opt/IBM/ITM/bin]-> ./itmcmd config -S -t HUB_MADRID
CandleConfig      : installer level 400 / 100.
CandleConfig      : running aix516 jre.
Configuring CMS...
```

---

2. Next, press Enter if \*LOCAL is the default, if not type \*LOCAL.

```
Hub or Remote [*LOCAL or *REMOTE] (Default is: *LOCAL): *LOCAL
TEMS Host Name (Default is: madrid):
```

3. Select your primary communication protocol.

```
Network Protocol 1 [ip, sna, or ip.pipe] (Default is: ip.pipe):
```

4. Select your secondary communication protocol.

```
Now choose the next protocol from one of these:
```

- ip
- sna
- none

```
Network Protocol 2 (Default is: ip):
```

5. And the third communication protocol.

```
Now choose the next protocol from one of these:
```

- sna
- none

```
Network Protocol 3 (Default is: none):
```

6. Next choose the port used by the server being configured.

```
IP Port Number (Default is: 1918):
IP.PIPE Port Number (Default is: 1918):
```

7. Accept the default for the next option or enter with the correct file name.

```
Enter name of KDC_PARTITION (Default is: null):
Enter path and name of KDC_PARTITIONFILE (Default is:
/opt/IBM/ITM/tables/HUB_MADIRD/partition.txt):
```

8. Type Enter to accept the default.

```
Configuration Auditing? [YES or NO] (Default is: YES):
Now enter with the server host name used as hot standby (backup)
Hot Standby TEMS Host Name (Default is: milan):
```

9. Next enter with the communication protocol and the port as shown below.

*Example 4-15 Entering communication protocol and the port*

---

Hot Standby Protocol 1 [ip, sna,ip.pipe or ip.spipe] (Default is: ip.pipe):

Now choose the next protocol from one of these:

- ip
- sna
- ip.spipe
- none

Hot Standby Protocol 2 (Default is: ip):

Now choose the next protocol from one of these:

- sna
- ip.spipe
- none

Hot Standby Protocol 3 (Default is: none):

Hot Standby IP Port Number (Default is: 1918):

Hot Standby IP.PIPE Port Number (Default is: 1918):

---

10. The next steps are similar to the one in section “Configuring the UNIX monitoring server” on page 221.

***Configuring the Warehouse Proxy***

The Warehouse Proxy also need to be configured to point also to a Secondary TEMS in case the primary Hub TEMS failed and the Hot Stanby took place. Use the following procedure to configure the Warehouse Proxy:

1. Open the Manage Tivoli Monitoring Services console from the Warehouse proxy server, right-click on the **Warehouse Proxy** server and click **Reconfigure**.
2. Click **OK** on the following window.

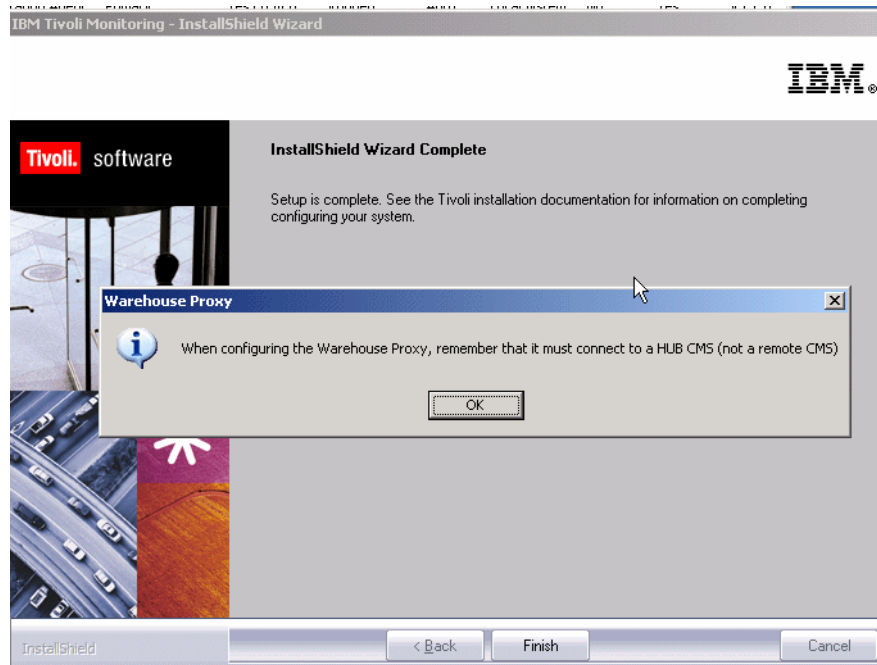


Figure 4-67 Warehouse Proxy confirmation window configuration

3. The primary TEMS communication protocol is already defined. Check the **Optional Secondary TEMS Connection** button and configure the communication protocol the secondary TEMS will be using as shown is the “Warehouse Proxy Secondary TEMS communication protocol configuration” on page 215.

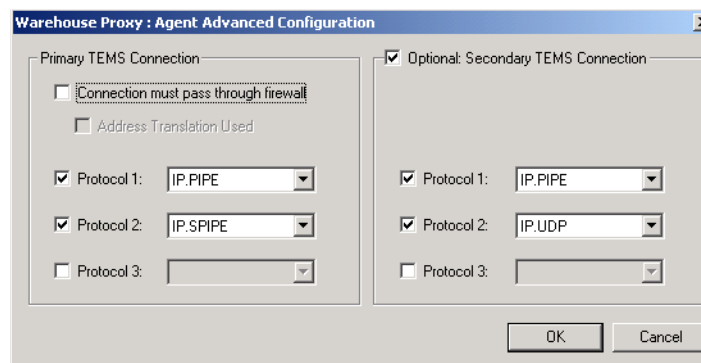


Figure 4-68 Warehouse Proxy Secondary TEMS communication protocol configuration

4. Select **OK** on the next window or update the primary TEMS if it has changed (Figure 4-69)

The image shows a Windows-style dialog box titled "Warehouse Proxy : Agent Advanced Configuration". It has a tab labeled "Configure Primary TEMS". The dialog is divided into several sections:

- IP.UDP Settings:** Contains fields for "Hostname or IP Address" (filled with "HELSINKI") and "Port # and/or Port Pools" (filled with "1918").
- IP.PIPE Settings:** Contains fields for "Hostname or IP Address" (filled with "HELSINKI") and "Port number" (filled with "1918").
- IP.SPIPE Settings:** Contains fields for "Hostname or IP Address" (filled with "HELSINKI") and "Port number" (filled with "3660").
- SNA Settings:** Contains a sub-section "Primary TEMS" with fields for "Network Name", "LU Name", "LU6.2 LOGMODE" (filled with "CANCTDCS"), and "TP Name" (filled with "SNASOCKETS" and a dropdown arrow). Below this is a field for "Local LU Alias (not required if using defined default)".
- Entry Options:** Contains two radio buttons: "Use case as typed" (unselected) and "Convert to upper case" (selected).
- NAT Settings:** A button located at the bottom left.
- Buttons:** "OK" and "Cancel" buttons at the bottom right.

Figure 4-69 Warehouse Proxy primary TEMS configuration

5. Next enter with the secondary TEMS hostname for each communication protocol chosen on "Warehouse Proxy Secondary TEMS communication protocol configuration" on page 215 and click **OK**.
6. The Warehouse Proxy is thus configured to connect to the secondary Hub TEMS case the primary one fails.

### Configuring the TEPS

The TEPS will need to be configured only when the primary Hub TEMS failed and the stanby Hub TEMS become the primary. Use the following steps to configure the TEPS:

1. Open the **Manage Tivoli Monitoring Services** console.
2. Right click on the **Tivoli Enterprise Portal Server service**.
3. Select **Reconfigure** (Window) or **Configure** (Linux).
4. Specify the new Hub TEMS and click **OK**.
5. You will then receive the following popup window(Figure 4-70 on page 217.) click **OK**.



**Note:** If you click **OK** on the last steps (Figure 4-70 on page 217) This will save the userids, queries, workspace, navigators, terminal scripts in the %CANDLEHOME%\CNPS\CMS\TEMS\_HOSTNAME\_PORT\saveexport.sql

where TEMS\_HOSTNAME is the new TEMS hostname and PORT the port number the TEPS will connect to the TEMS. as shown in the example below:

F:\IBM\ITM\CNPS\CMS\MADRID\_1918\saveexport.sql

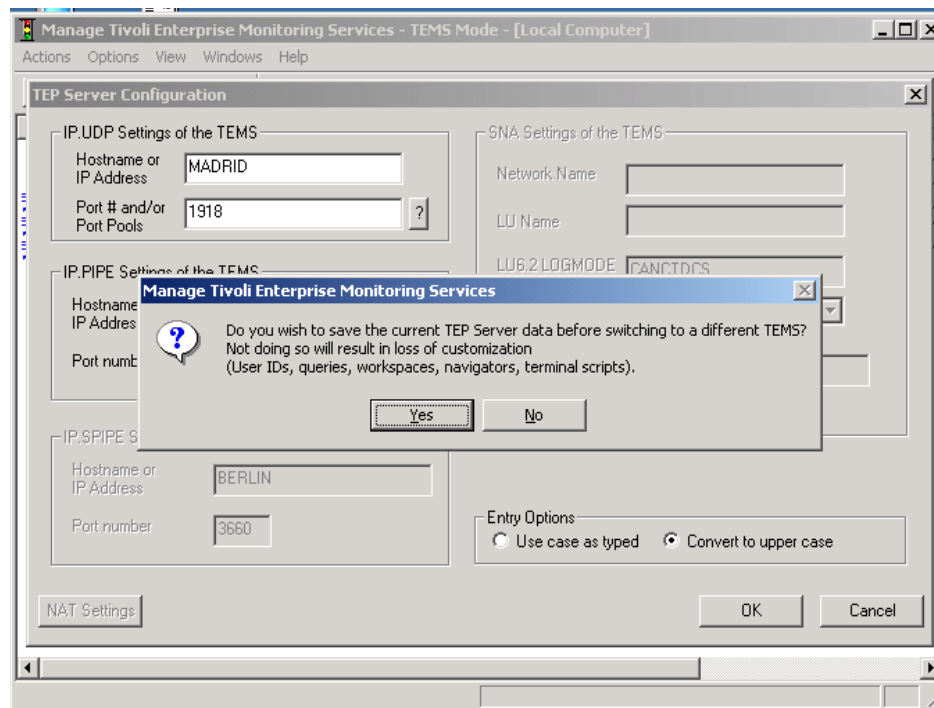


Figure 4-70 TEPS configuration window database backup confirmation

6. From the Enterprise Monitoring Server console restart the TEPS.

**Note:** You do not need to reconfigure the TEPS database.

## 4.2.16 Installing and configuring the scenario-2 environment

This section will describe the different IBM Tivoli Monitoring, V6.1 components installation and configuration on an UNIX Hub TEMS environment.

### Installing a Hub TEMS on a UNIX server

To install a Hub TEMS on a UNIX, you can use either root or a different user with the proper permissions on the IBM Tivoli Monitoring, V6.1 files and directories; refer to Section , “Creating an IBM Tivoli account on UNIX servers” on page 114.

Use the following steps to install the monitoring server on a UNIX computer:

#### Notes:

- ▶ We will not show the installation of the Hub TEMS individually; we will only focus on how to install a Hub TEMS on UNIX environment.
- ▶ This procedure is also valid for Linux servers, so we will not make any distinction between UNIX and Linux configurations in this section.

1. In the directory where you extracted the 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). If you want to use a different installation directory, type the full path to that directory and press Enter.

**Note:** If the directory you specified does not exist, you are asked whether to create it. Type y to create this directory.

3. The following prompt is displayed:

*Example 4-16 Select one of the following prompt*

---

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.
- 

Type **1** to start the installation process and press Enter. The following menu will be displayed to you (only the relevant information are shown to you):

*Example 4-17 Software Licensing Agreement*

---

Software Licensing Agreement  
1. Czech

2. English
3. French
4. German
5. Italian
6. Polish
7. Portuguese
8. Spanish
9. Turkish

Please enter the number that corresponds to the language you prefer.

---

4. Type the number that corresponds to the language that you want to display the software license agreement in and press Enter.
5. Press Enter to display the license agreement.
6. Type 1 to accept the agreement and press Enter. You will receive the following message:

*Example 4-18 Preparing to install the Global Security Kit message*

---

```
runGSKit      : Preparing to install the Global Security Kit.  
runGSKit warning: the 'root' ID or password is required for this phase,  
continuing ...  
Will enable automatic agent initiation after reboot.
```

Please enter root password or press Enter twice to skip.

---

**Notes:**

- ▶ If you are installing the IBM Tivoli Monitoring, V6.1 with root user you will not obviously be asked the root password for the GSKit installation
- ▶ GSKit is Global Security Kit, which is IBM toolkit that enables products to provide secure connections over TCP/IP between IBM Tivoli Monitoring, V6.1 components.

Two main functions to GSKit:

- a. –A toolkit that can be used for Secure Socket Layer (SSL) communications using public key encryption/decryption methodology
- b. –Key management functions using iKeyman (a Java-based application for managing keys and key requests)

7. Enter with the root password and press Enter if you want to use GSKit, otherwise press Enter twice.
8. Type a 32 character encryption key and press Enter. If you want to use the default key, press Enter without typing any characters.

**Important:** Save this key carefully because you will need it to install the other components

9. Type the number for the operating system for which you want to install products when the following menu is displayed and then Press Enter.

*Example 4-19 List of available OS for IBM Tivoli Monitoring, V6.1 installation*

---

Product packages are available in /opt/itm61s1/unix

Product packages are available for the following operating systems and component support categories:

- 1) AIX R5.1 (32 bit)
- 2) AIX R5.1 (64 bit)
- 3) AIX R5.2 (32 bit)
- 4) AIX R5.2 (64 bit)
- 5) AIX R5.3 (32 bit)
- 6) AIX R5.3 (64 bit)
- 7) Solaris R10 (32 bit)
- 8) Solaris R10 (64 bit)
- 9) Solaris R8 (32 bit)
- 10) Solaris R8 (64 bit)
- 11) Solaris R9 (32 bit)
- 12) Solaris R9 (64 bit)

Type the number for the OS or component support category you want, or type "q" to quit selection

[ number "5" or "AIX R5.3 (32 bit)" is default ]: 5

---

**Note:** The default value is your current operating system.

- 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 the Tivoli Enterprise Monitoring Server option and press Enter.
12. The list of available products to be installed will be listed. You can choose more than one product typing their corresponding numbers separated by a coma or a space. Below is the option list:

*Example 4-20 Option list*

---

The following products are available for installation:

- 1) Monitoring Agent for UNIX Logs V06.10.00.00

- 2) Monitoring Agent for UNIX OS V06.10.00.00
- 3) Summarization and Pruning agent V06.10.00.00
- 4) Tivoli Enterprise Monitoring Server V06.10.00.00
- 5) Tivoli Enterprise Services User Interface V06.10.00.00
- 6) Universal Agent V06.10.00.00
- 7) all of the above

Type the numbers for the products you want to install, or type "q" to quit selection.

If you enter more than one number, separate the numbers by a comma or a space.

Type your selections here: 4

---

13. Type y to confirm your selection or n otherwise to restart.

14. When prompted, type a name for your monitoring server see example below:

Please enter TEMS name: HUB\_MADRID

Do not use the fully qualified host name. Press Enter.

15. 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.

Installation is complete. The next step is to configure your monitoring server.

## Configuring the UNIX monitoring server

Use the following steps to configure the hub monitoring server:

**Note:** When we accept the default value on the various displayed options, we just hit Enter. Thus, for some cases in the following examples you will not see any entry, because we simply press Enter.

1. At the command line, change to the opt/IBM/ITM/bin directory (or the directory where you installed IBM Tivoli Monitoring, actually the \$CANDLEHOME/bin).

```
cd $CANDLEHOME/bin
```

2. Run the following command: `./itmcmd config -S -t tems_name.`

You will receive the following message:

*Example 4-21 itmcmd config output*

---

```
CandleConfig      : installer level 400 / 100.
CandleConfig      : running li6243 jre.
Configuring CMS...
```

```
Hub or Remote [*LOCAL or *REMOTE] (Default is: *LOCAL):*LOCAL
```

TEMS Host Name (Default is: madrid): (ENTER (hitted))

---

Choose **LOCAL** (the default) as you are installing a Hub TEMS.

3. Next you will be requested to configure the communication protocol. Several options are offered to you: IP, SNA, IP.PIPE, IP.SPIPE. Select your preferred protocol. You can refer to Section , “Communications protocol selection” on page 39 to have a detailed information on the protocols specifications.
4. If you want to use a secondary protocol in case the first one fails, enter it at the next option window. See example below:

---

*Example 4-22 Entering a secondary protocol*

---

Now choose the next protocol from one of these:

- ip
- sna
- ip.spice
- none

Network Protocol 2 (Default is: ip):

Now choose the next protocol from one of these:

- sna
- ip.spice
- none

Network Protocol 3 (Default is: none):

Network Protocol 1 [ip, sna, ip.pipe or ip.spice] (Default is: ip.pipe):

Now choose the next protocol from one of these:

- ip
- sna
- ip.spice
- none

Network Protocol 2 (Default is: ip):

Now choose the next protocol from one of these:

- sna
- ip.spice
- none

Network Protocol 3 (Default is: none):

---

We have chosen IP.PIPE as the primary protocol and IP.UDP as the secondary protocol.

5. Next you will have to set the ports for the communication protocols you have chosen; the default is 1918. You can choose another port if you want to, but you have to use those ones when setting up the Remote TEMS and the TEMA that will be connected to the Hub TEMS. Below is the two communication protocol ports we have chosen. We select the default configuration.

IP Port Number (Default is: 1918):  
IP.PIPE Port Number (Default is: 1918):

6. Next step you will be asked the KDC\_PARTITION as shown in Example 4-23. This is used in environment using NAT across firewall as described in the note below:

**Note:** When IBM Tivoli Monitoring components need to communicate across a firewall that performs NAT, those components must be able to retrieve an IP address of the other component that is valid on its side of the firewall. To support this capability, the location broker namespace is logically divided into partitions with unique partition IDs. Partition IDs are specified using the KDC\_PARTITION environment variable. The partition file is the means to insert appropriate IP addresses into the location broker namespaces.

*Example 4-23 KDC\_PARTITION question*

---

Enter name of KDC\_PARTITION (Default is: null):  
Enter path and name of KDC\_PARTITIONFILE (Default is:  
/opt/IBM/ITM/tables/REMOTE\_EDINBURG/partition.txt):

---

We've selected the default.

7. If you want to use Configuration Auditing, type y and press Enter. Otherwise, press Enter (During the installation, we chose to audit the configuration.)
8. Press Enter to accept the default setting for Hot Standby (NO).

**Tip:** It is a good idea to wait until after you have fully deployed your environment to configure Hot Standby for your monitoring server. See Section 4.2.15, "Configuring the Hot Standby" on page 211 for information about configuring Hot Standby.

9. Press Enter to accept the default for the Optional Primary Network Name (none).
- 10..Press Enter for the default security: Validate User setting (no). If you need to use security validation in your environment, you can enable it after initial configuration is complete. See "Configuring user security" on page 69 for more information.

**Note:** If you enable the security validation, you will need to create on the server the users that will need to access the IBM Tivoli Monitoring, V6.1 environment.

11. If you will be using Event Synchronization to view situation events, type **y** and press Enter to enable TEC Event Integration. Complete the following additional steps:
  - a. Type the name of the IBM Tivoli Enterprise Console event server and press Enter.
  - b. Type the port number for the event server and press Enter (if your event server is using port mapper: for example UNIX server, the port will be 0 otherwise if your event server is on a windows machine the default port is 5529).

**Note:** If your Tivoli Enterprise Console is not yet setup, you can skip the above section typing NO and perform the configuration later using the same procedure.

- c. Press Enter to not disable the Workflow Policy/Tivoli Emitter Agent.
12. Type **s** to save the SOAP (Simple Object Access Protocol) configuration and exit the configuration. We will perform the SOAP configuration later, when configuring the Event Synchronization.

## Installing agents support on (seeding) the hub monitoring server

Once you have finished configuring the TEMS, you will need to install the application support. Use the following steps to seed the hub monitoring server. Remember that seeding adds product-specific data to the monitoring server.

1. Start the monitoring server by running the following command from the `$CANDLEHOME\bin` directory:

```
./itmcmd server start <tems_name>
```

2. Run the following command to start the seeding process:

```
./itmcmd -t <tems_name> <pc pc pc>
```

where `tems_name` is the Hub TEMS name and `pc` is the product code for each agent whose data you want to send to the monitoring server (you can retrieve those information executing the command line: **cinfo -i**).

**Note:** Seed the server with all available pc codes in advance.

3. Stop the monitoring server by running the following command:

```
./itmcmd server stop <tems_name>
```
4. Restart the monitoring server by running the following command:



```
./itmcmd server start <tems_name>
```

Once you are done with the Hub TEMS, refer to Table 4-12 for installing the rest of the components.

*Table 4-12 How to install IBM Tivoli Monitoring, V6.1 components in scenario 2*

Components	References
Install and configure the second UNIX Hub TEMS	"Installing and configuring the scenario-2 environment" on page 218
install and configure the remote TEMS	"Installing a Remote TEMS on a Windows and UNIX server" on page 131
TEPS	"Tivoli Enterprise Portal Server - TEPS" on page 135
TEMAs	"Tivoli Enterprise Monitoring Agent - TEMA" on page 143 and "Deploying TEMA from command line interface" on page 171
TEP	"Tivoli Enterprise Portal -TEP" on page 174
Warehouse Proxy Agent	"Warehouse Proxy installation and configuration" on page 178
Summarization and Pruning agent	"Summarization and Pruning agent (SPA) installation and configuration" on page 186
Event Synchronization	"Event Synchronization installation" on page 196
Hot standby	"Configuring the Hot Standby" on page 211

## 4.2.17 Replacing a Hub TEMS server with a new one

For any reason (hardware upgrade, for example) if you want to replace your Hub TEMS server with a new one from the same platform or a different platform, IBM Tivoli Monitoring, V6.1 allows you to do so. The following describes the procedure we followed to replace our scenario-1 implementation (Windows TEMS servers) with scenario 2 (UNIX TEMS servers).

1. Install configure and seed the Hub TEMS on madrid and milan servers.  
Depending on the platform you are using, refer to "Installing and configuring a Hub TEMS on a Windows server" on page 117 or "Installing a Hub TEMS on a UNIX server" on page 218.
2. Stop all the Remote TEMS (copenhagen and edinburgh) using either the Manage Tivoli Enterprise Monitoring Services console or for UNIX servers use the following command:

```
itmcmd server stop tems_name
```

where `tems_name` is the of the TEMS host by the server your are stopping its TEMS service.

3. Stop the TEPS, Warehouse Proxy Agent and Summarization and Pruning agent from the Manage Tivoli Enterprise Monitoring Services console.
4. Stop the Hub TEMS (cairo and helsinki) using Manage Tivoli Enterprise Monitoring Services console or **itmcmd command for UNIX servers** as describe previously.
5. Configure the Remote TEMS (copenhagen and edinburgh) to point to your new Hub TEMS (madrid and milan primary and Hot Standby TEMS, respectively). Use the Reconfigure option on the Manage Tivoli Enterprise Monitoring Services console on UNIX servers or the following procedure on UNIX servers:  
  
**itmcmd config -S -t tems\_name**
6. Configure the WPA and SPA to point to the primary and Hot Standby TEMS (madrid and milan) respectively. This operation is performed using the Manage Tivoli Enterprise Monitoring Services console.
7. Using the Manage Tivoli Enterprise Monitoring Services console, configure the TEPS to point to madrid.

**Important:** Before pointing TEPS to the new TEMS, you must save TEPS data using the migrate-export.bat facility. The migrate-export.bat facility will detect the TEPS database and create the sql file script that will be used to restore you TEPS services. Use the following procedure to backup and import the data:

– Saving TEPS data

Use the following procedure to backup your TEPS database

- cd %CANDLEHOME%/CNPS
- run **migrate-export.bat**

The **migrate-export.bat** facility will stop the TEPS create a saveexport.sql and restart the TEPS

– Importing Backup Data

Use the following procedure to restore your TEPS initial state.

- In order to import the data back into TEPS, copy the presentation files back to the CNP directory.
- Copy saveexport.sql file to %CANDLEHOME%\cnps\sqllib directory and run **migrate\_import.bat**.

If you are using Linux as your TEPS read \$CANDLEHOME instead of %CANDLEHOME%.

8. Configure cairo to become a Remote TEMS. This is done using the Manage Tivoli Enterprise Monitoring Services console or itmcmd on UNIX server. This step can be skipped, if you don't want to re-configure any of your old Hub TEMS to a Remote TEMS.
9. Configure agents on oslo and dakar to point to cairo and copenhagen, primary and secondary Remote TEMS respectively. You do not need to reconfigure your agents to point to the new Hub. This operation was done to check if the remote TEMS cairo is working as expected.
10. Start the Remote TEMS (edinburg, copenhagen and cairo). Use Manage Tivoli Enterprise Monitoring Services console or itmcmd **command for UNIX servers**.
11. And finally from the Manage Tivoli Enterprise Monitoring Services console start the WPA, SPA and TEPS.

**Notes:**

- ▶ This procedure is only recommended if you want to change your platform's Hub TEMS. If you want to build a two Hub TEMS environment, you can install it from scratch.
- ▶ We were able to get all of the agents (from scenario-1) back up and running; we needed to restart a few agents to have them re-connected. Others re-connected automatically.
- ▶ We lost our situations, workspace and collections configuration because we did not save it to transfer it later on the new Hub TEMS.

**Tips:**

- ▶ If you want to change your Hub TEMS environment, backup all the environment and plan very carefully the transition.
- ▶ If you are replacing one Hub TEMS with another one with the same platform and configuration (hostname, tcp/ip configuration), you can backup the CANDLEHOME directory from the current Hub TEMS and restore it later onto the new Hub TEMS.
- ▶ If the new and old TEMS are installed on the same platform (such as both UNIX or Windows). you can backup your candle database from your current Hub TEMS and restore it later onto the new Hub TEMS. You need to copy the following files from your old HUB TEMS.

**Windows:**

%CANDLEHOME%/CMS/QA1\*.db and QA1\*.idx

**UNIX:**

\$CANDLEHOME/tables/TEMS\_NAME/QA1\*.db and QA1\*.idx

## 4.3 Uninstalling IBM Tivoli Monitoring, V6.1

In this section we will cover uninstalling IBM Tivoli Monitoring, V6.1, either uninstalling the whole environment or individual components.

### 4.3.1 Uninstalling the entire IBM Tivoli Monitoring environment

Use the following procedures to remove the entire IBM Tivoli Monitoring environment from your computer.

- ▶ “Uninstalling the environment on Windows” on page 229

- “Uninstalling the environment on UNIX” on page 229

### ***Uninstalling the environment on Windows***

Use the following steps to uninstall IBM Tivoli Monitoring from a Windows computer:

1. From the desktop, click **Start->Settings->Control Panel** (for Windows 2000) or **Start->Control Panel** (for Windows 2003).
2. Click **Add/Remove Programs**.
3. Select **IBM Tivoli Monitoring** and click **Change/Remove**.
4. Select **Remove** and click **Next**.
5. Click **OK**.

After Tivoli Enterprise services have stopped, you are asked if you want to remove the Tivoli Enterprise Portal database.

6. Click **Yes**.
7. Type the password for the DB2 administrator in the Admin Password field and click **OK**.

A pop-up window, indicating that GSKit is being uninstalled, is displayed.

8. Select **Yes** to restart your computer and click **Finish**.

### ***Uninstalling the environment on UNIX***

Before executing the uninstallation procedure, make sure that all IBM Tivoli Monitoring, V6.1 components are shut down.

1. Stop the agent executing the following command line from \$CANDLEHOME/bin:

```
./itmcmd agent stop pc
```

where pc is the product code (lz, ux, ul, um, ui, cj and so on).

2. Stop the TEMS executing the following command line from \$CANDLEHOME/bin.

```
./itmcmd server stop TEMS_NAME
```

3. Run the following command:

```
./uninstall.sh
```

A numbered list of product codes, architecture codes, version and release numbers, and product titles is displayed for all installed products.

4. Type the number for the installed product that you want to uninstall. Repeat this step for each additional installed product you want to uninstall; see example below.

*Example 4-24 Uninstalling the environment on UNIX*

```

***** Mon Oct 10 15:08:29 EDT 2005 *****
User       : itmuser      Group: itmuser
Host name  : edinburg.itsc.austin.ibm.com      Installer Lvl: 400 / 100
CandleHome: /opt/IBM/ITM
*****

...Products available to uninstall

Num      Product [ Code Platform Version:Release Description ]
1        cj li6243      v610:r172 Tivoli Enterprise Portal Desktop Client
2        lz li6263      v610:r115 Monitoring Agent for Linux OS
3        ms li6243      v610:r215 Tivoli Enterprise Monitoring Server
4        sh li6243      v610:r215 Tivoli Enterprise Monitoring SOAP
Server
5        uf li6243      v610:r100 Universal Agent Framework
6        ui li6243      v610:r194 Tivoli Enterprise Services User
Interface
7        um li6243      v610:r229 Universal Agent

Enter number for a product to uninstall or "EXIT" to exit: 1
Confirm: cj li6243 v610:r172 Tivoli Enterprise Portal Desktop Client ...
OK to delete? [y/n]: y

```

5. Once done, restart the computer to complete the uninstallation.

**Notes:**

- If for any reason, the UNIX uninstallation is not successful, run the following command to remove all IBM Tivoli Monitoring directories:
- If you are uninstalling the components using a userid different from root user you might have errors like the following:

```

rm -r $CANDLEHOME

rm: cannot remove `/etc/rc0.d/K10ITMAgents1': Permission denied
rm: cannot remove `/etc/rc1.d/K10ITMAgents1': Permission denied
rm: cannot remove `/etc/rc2.d/S99ITMAgents1': Permission denied
rm: cannot remove `/etc/rc3.d/S99ITMAgents1': Permission denied
rm: cannot remove `/etc/rc4.d/S99ITMAgents1': Permission denied
rm: cannot remove `/etc/rc5.d/S99ITMAgents1': Permission denied
rm: cannot remove `/etc/rc6.d/K10ITMAgents1': Permission denied
rm: cannot remove `/etc/init.d/ITMAgents1': Permission denied

```

Contact your system administrator to remove those files.

### 4.3.2 Uninstalling an individual IBM Tivoli Monitoring agent or component

Use the following procedures to remove an agent or other individual IBM Tivoli Monitoring component from your computer:

- ▶ “Uninstalling a component on Windows” on page 231
- ▶ “Uninstalling a component on UNIX” on page 232

#### Uninstalling a component on Windows

Use the following steps to remove a component on a Windows computer. You can uninstall a single agent or the entire agent bundle (such as IBM Tivoli Monitoring for Databases).

1. From the desktop, click **Start->Settings->Control Panel** (for Windows 2000) or **Start->Control Panel** (for Windows 2003).
2. Click **Add/Remove Programs**.
3. Do one of the following:
  - a. To uninstall a single IBM Tivoli Monitoring component, such as the portal server or portal client (but not all components), select **IBM Tivoli Monitoring**.
  - b. To uninstall an agent bundle or a specific agent, select the agent bundle.
4. Click **Change/Remove**.
5. Do one of the following:
  - a. To uninstall a specific agent or component, select **Modify**.
  - b. To uninstall the entire agent bundle, select **Remove**.
6. Click **Next**.
7. If you are uninstalling an agent bundle, click **OK** to confirm the uninstallation.
8. If you are uninstalling an agent or component, do the following:
  - a. For an agent, expand Tivoli Enterprise Monitoring Agents and select the agent you want to uninstall.
  - b. For a component, select the component (such as Tivoli Enterprise Portal Desktop Client).
  - c. Click **Next**.
  - d. Click **Next** on the confirmation screen.
  - e. Depending on the remaining components on your computer, there might be a series of configuration panels. Click **Next** on each of these panels.
9. Click **Finish** to complete the uninstallation.

10. Restart the computer to complete the uninstallation.

**Note:** When removing a specific component (Modify/Remove), do not unselect any other component except the one you are removing. Deselecting any other component will uninstall it from the machine.

## Uninstalling a component on UNIX

Use the following steps to remove a component from UNIX computer.

You can uninstall a single agent or the entire agent bundle (such as IBM Tivoli Monitoring for Databases).

1. From a command prompt, run the following command to change to the appropriate /bin directory:

```
cd $CANDLEHOME/bin
```

where \$CANDLEHOME is the path for the home directory for IBM Tivoli Monitoring.

2. Run the following command:

```
./uninstall.sh
```

A numbered list of product codes, architecture codes, version and release numbers, and product titles is displayed for all installed products.

3. Type the number for the agent or component that you want to uninstall. Repeat this step for each additional installed product you want to uninstall.
4. Restart the computer to complete the uninstallation.

### 4.3.3 Uninstalling the IBM Tivoli Enterprise Console Event Synchronization

Use the following steps to uninstall the Event Synchronization from your event server:

1. Stop the Event Synchronization on the event server by running the following command:

On Windows:

```
<tec_installdir>\TME\TEC\OM_TEC\bin\stop.cmd
```

On UNIX:

```
<tec_installdir>/TME/TEC/OM_TEC/bin/stop.sh
```

2. Run the following uninstallation program:

On Windows:



```
<tec_installdir>\TME\TEC\OM_TEC\_uninst\uninstaller.exe
```

On UNIX:

```
<tec_installdir>/TME/TEC/OM_TEC/_uninst/uninstaller.bin
```

where <tec\_installdir> is the location of the IBM Tivoli Enterprise Console installation.

3. Follow the prompts in the uninstallation program.

**Notes:**

- ▶ You can also run this uninstallation program in silent mode (by running the program from the command line with the -silent parameter) or in console mode (by using the -console parameter).
- ▶ You must stop and restart the event server for these changes to take effect.
- ▶ If your event server is running on an HP-UX computer, ensure that the \_uninst and \_jvm directories are successfully removed by the uninstallation program. If they are not, manually delete these directories.



## 5



## Working with IBM Tivoli Monitoring, V6.1

In this chapter, we will show you how to work with IBM Tivoli Monitoring, V6.1 using some examples. The examples in this chapter could be used as part of a quick proof of concept or demonstration of IBM Tivoli Monitoring, V6.1's capabilities.

First, we will describe the Tivoli Enterprise Portal client and walk you through some examples on how to monitor your environment using it. Finally, we will discuss IBM Tivoli Data Warehouse and cover some scenarios.

This chapter has the following sections:

- ▶ “Understanding Tivoli Enterprise Portal client” on page 236
- ▶ “Working with Tivoli Enterprise Portal” on page 238

## 5.1 Understanding Tivoli Enterprise Portal client

The Tivoli Enterprise Portal client provides a user interface for IBM Tivoli Monitoring, V6.1. In this topic, we will describe how to log on and work with Tivoli Enterprise Portal.

### 5.1.1 Launching the Tivoli Enterprise Portal

As we discussed in Section 5.1.1, “Launching the Tivoli Enterprise Portal” on page 236, we can access Tivoli Enterprise Portal either as a desktop or a web-based application. In the desktop version, we need to install the client on a workstation. This version gives you more area to configure the workspace and requires more maintenance than web-based. The web-based is available via Internet Explorer and can be accessed from any workstation that has access to the Tivoli Enterprise Portal Server.

You can use the following to launch Tivoli Enterprise Portal:

- ▶ Section , “Launching Tivoli Enterprise Portal from Internet Explorer” on page 93;
- ▶ Section , “Launching Tivoli Enterprise Portal Client desktop application” on page 95.

### 5.1.2 Tivoli Enterprise Portal components

As soon as we get logged on the Tivoli Enterprise Portal, we are presented with a window, as shown in Figure 5-1.

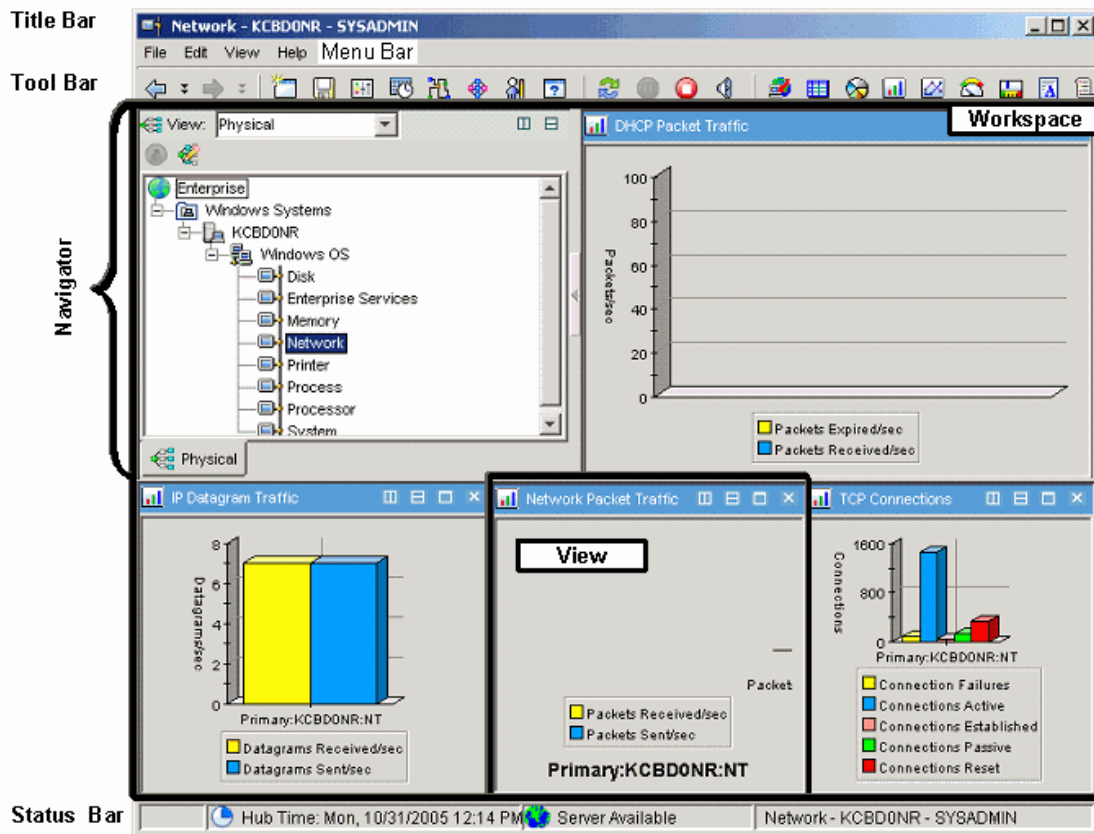


Figure 5-1 Tivoli Enterprise Portal desktop application

The three main components of the Tivoli Enterprise Portal are:

## Navigator

It is a tree like view of your monitored environment. You can navigate through the monitored environment by clicking in the *navigators items* in the Navigator. Every item opens a different workspace. In the Navigator we have:

### Physical view

It shows the network hierarchy from a system point of view. It is organized by operating platform, system name, monitoring agent, and attribute groups. You can change the Physical view.

***Logical view***

It allows you organize your view according your logical hierarchy, for instance you could have a Navigator view for your departments.

**Workspace**

The workspace is the working area of the Tivoli Enterprise Portal window. It is divided into panes to show different types of views. So we could say that every time we select one navigator item in the Navigator, we change the Workspace views.

**Views**

A View is a pane or frame in the workspace that could contain data from a monitoring agent as chart or table. There are non-data views such as the browser view and terminal view.

## **5.2 Working with Tivoli Enterprise Portal**

In this topic, we will walk you through some examples to demonstrate how to work with IBM Tivoli Monitoring, V6.1 using Tivoli Enterprise Portal desktop application.

### **5.2.1 Creating a new workspace and add custom views**

The first thing we will show you is to create a new workspace and add custom views.

**Navigating through workspaces**

Navigating means selecting or expanding the items under Navigator. When we select or expand an item in the Navigator, its default workspace opens. A Navigator item may have multiple workspaces and may have links to other workspaces.

***Expanding and collapsing the tree***

As shown in Figure 5-2 on page 239, we have the first view of navigator when we start the Tivoli Enterprise Portal.

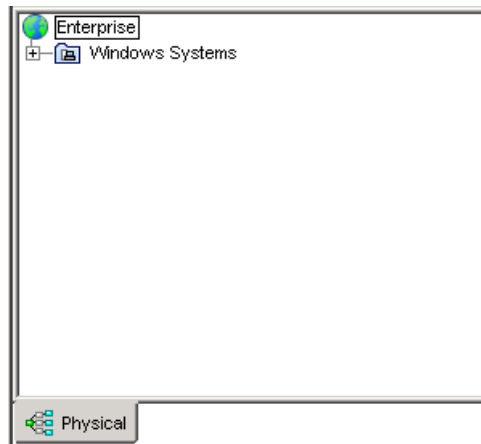




Figure 5-2 Navigator view

Expand  each level of the Navigator until you reach the lowest level (Figure 5-3). You can also collapse the Navigator tree selecting .

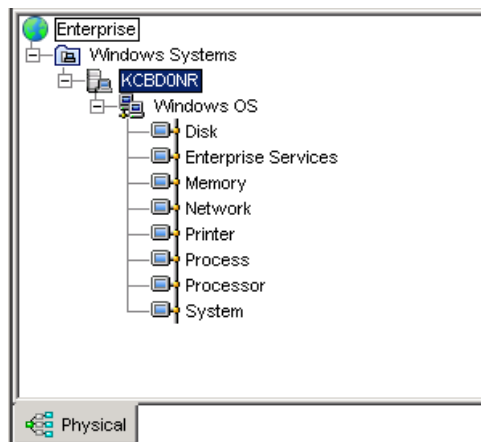



Figure 5-3 Navigator Lowest Level

### ***Navigating through the workspaces.***

When we select one item under the Navigator tree, a new workspace opens. You can navigate through the Navigator and note that views change every time you select one navigator item. Select  **Memory** item to open a workspace with views related with Memory attributes as shown in Figure 5-4.

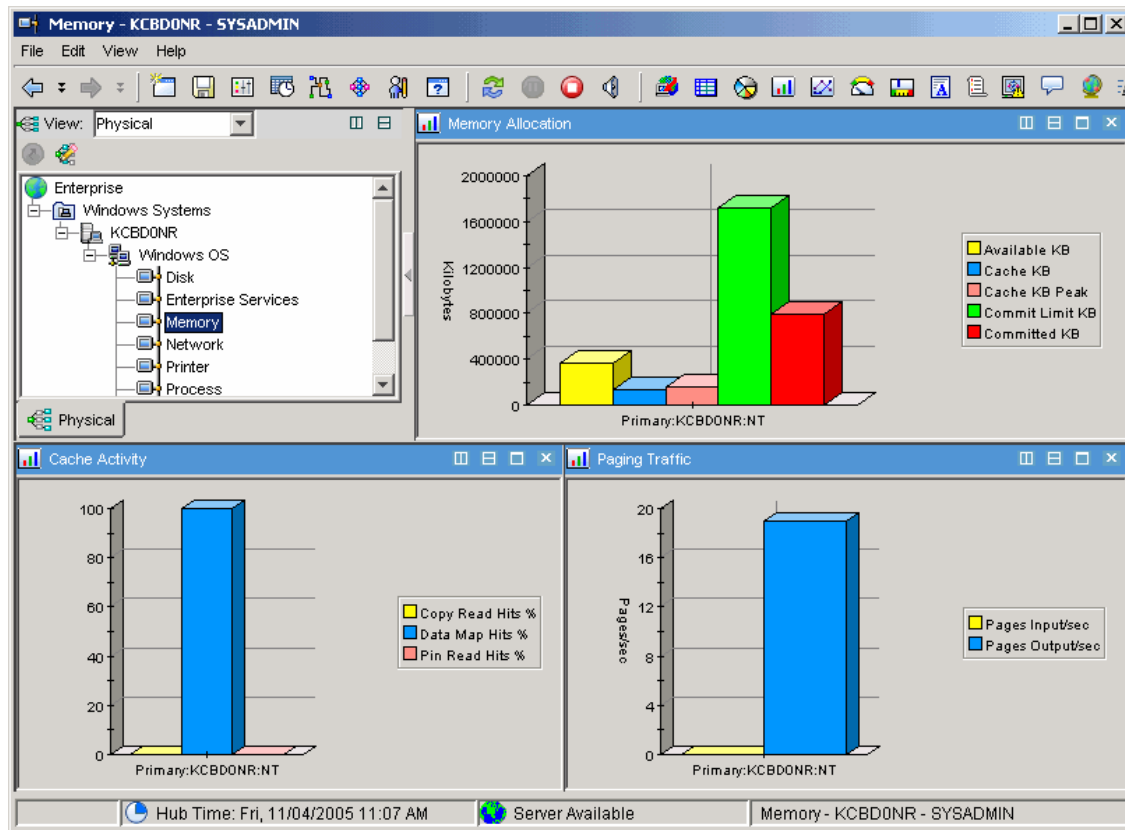


Figure 5-4 Selecting Memory attribute

### ***Saving the workspace***

When we navigate from one workspace to another, the system warns us about changing the workspace and ask if we want to save or not. Also, we can save the workspace manually selecting **File → Save Workspace** or we can create a new workspace following the instructions:

1. Launch the Tivoli Enterprise Portal desktop client.
2. In the Navigator select **Enterprise** Navigator item.
3. In the Menu bar select **File → Save Workspace As...**
4. Click **Yes** in Save Workspace message as show in Figure 5-5.



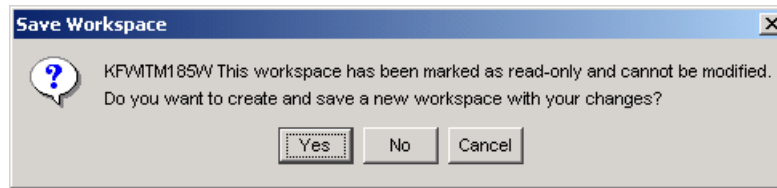


Figure 5-5 Save Workspace message

5. Type the name of this workspace as NewWorkspace, type description as Saving Workspace example and click **OK** as shown in Figure 5-6.

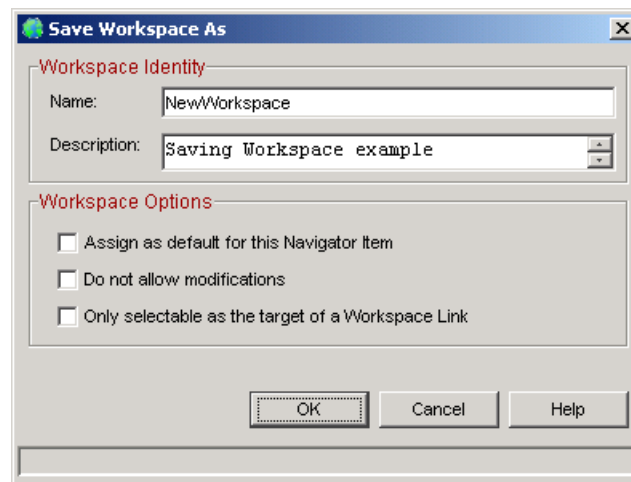



Figure 5-6 Save Workspace As

6. Close Tivoli Enterprise Portal, select **File** → **Exit** and click **Yes**.

**Note:** The Title Bar now has the name of the saved workspace called NewWorkspace.

## Selecting the workspace

We have, as default workspace, the System Enterprise Workspace. In order to select other workspaces, specially the saved ones, we can do the following:

1. Launch the Tivoli Enterprise Portal desktop client.
2. In the Navigator right-click the  **Enterprise Navigator**.
3. Select **Workspace** and **NewWorkspace** as shown in Figure 5-7.

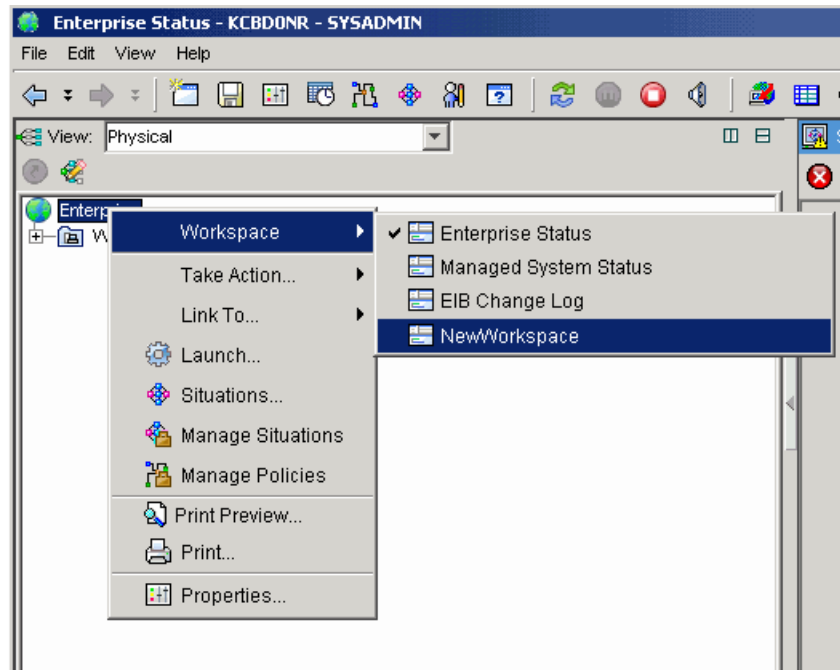


Figure 5-7 Selecting the workspace

**Note:** According to Navigator item we could have other workspaces.

## Working with Views

We have several kinds of view that can be added in the workspace, in the next steps we will show you how to add a view.

### Views Type

We have the following views



The Tivoli Enterprise Console view displays events from the Tivoli Enterprise Console Server and can integrate them with situation events from the Tivoli Enterprise Monitoring Server.



Table view and Chart view display data that the monitoring agents have gathered from the systems where they are running. They can also show data from any ODBC-compliant database you write a custom query for.



The Notepad view opens a simple text editor for writing text that can be saved with the workspace.



The Message log view shows the status of all situations distributed to the managed systems in your enterprise.



The Situation event console view shows the status of all situations associated with items on this branch of the Navigator view, and has tools for instant filtering and event handling.



The Universal message console view shows situation and policy activity, and messages received as the result of universal message generation.



The Graphic view places Navigator items as icons on a map or picture of your choosing.



The Take action view enables you to send a command to a managed system.



The Terminal view starts a 3270, 5250, or Telnet session, and enables you to write scripts for working with z/OS applications.







The Browser view opens the integrated browser for accessing Web pages.

We can add as many views to a workspace as you can easily see within the confines of the window.

### ***Adding a Non-data view***

Open the workspace where you want the view.

1. In the Navigator expand  **Windows System**.
2. Select **KCBD0NR**.
3. In the Toolbar, select the  **Situation event console** view, note that when you select a view, the  mouse pointer changes to .
4. Click **Inside the view** at the right side in top plane. This view becomes a Situation Event Console view, as shown in Figure 5-8.

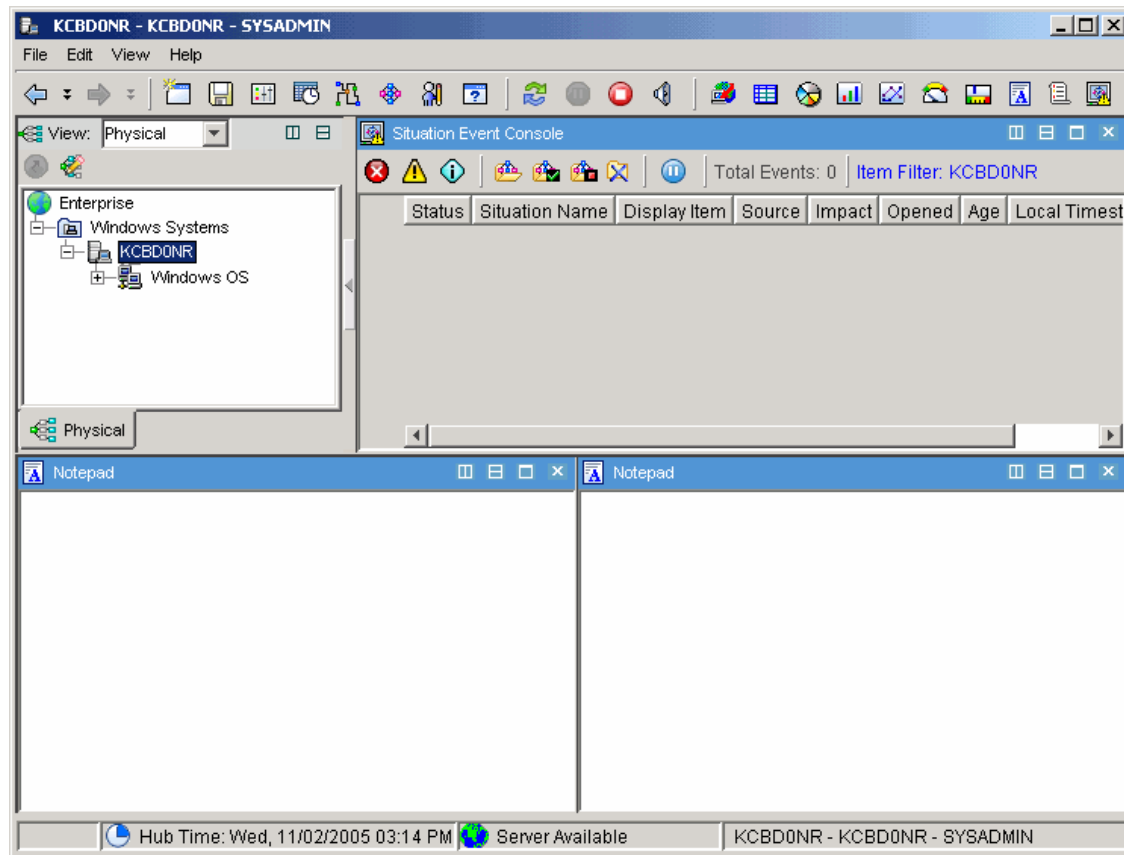


Figure 5-8 Adding a View

5. Click **File** → **Save Workspace**, to save that change.




## 5.2.2 Working with queries

The chart and tables views show the attributes values from Tivoli Monitoring Agents or ODBC data source. Your IBM Tivoli Monitoring products come with queries that are used to populate the table and chart views in workspaces. When we add a table or a chart view over a non-data view (as Message Log or Notepad view) we have to define the query. So before we show you how to add a data view, we are going to install IBM Tivoli Monitoring Agent for Databases.

### Working with data view

In this topic, we will demonstrate how to add a view that queries for Monitoring Agent data.

**Adding table view**

1. In the Navigator expand  **Windows System**.
2. Select  **KCBD0NR**.
3. In the Toolbar, click the  **Table view**.
4. Click inside the view at left side in bottom plane. This brings up the Selection option (Figure 5-9). Click on **Yes**.

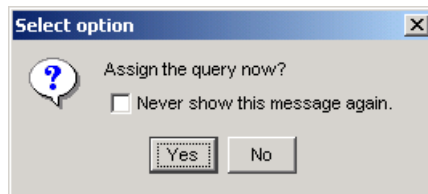


Figure 5-9 Assigning a query

5. In Properties - KCBD0NR (Figure 5-10), select **Click here to assign a query**.

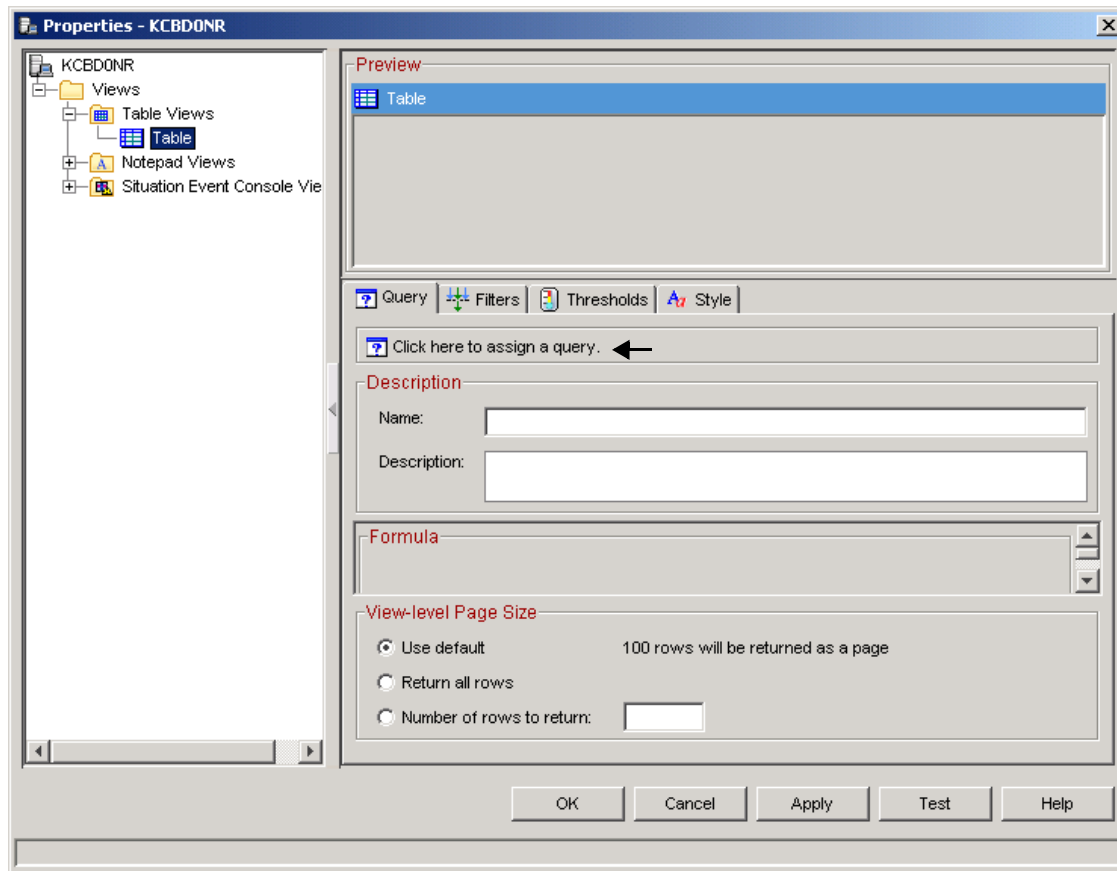


Figure 5-10 Click here to assign query

6. The Query editor opens as shown in Figure 5-11.

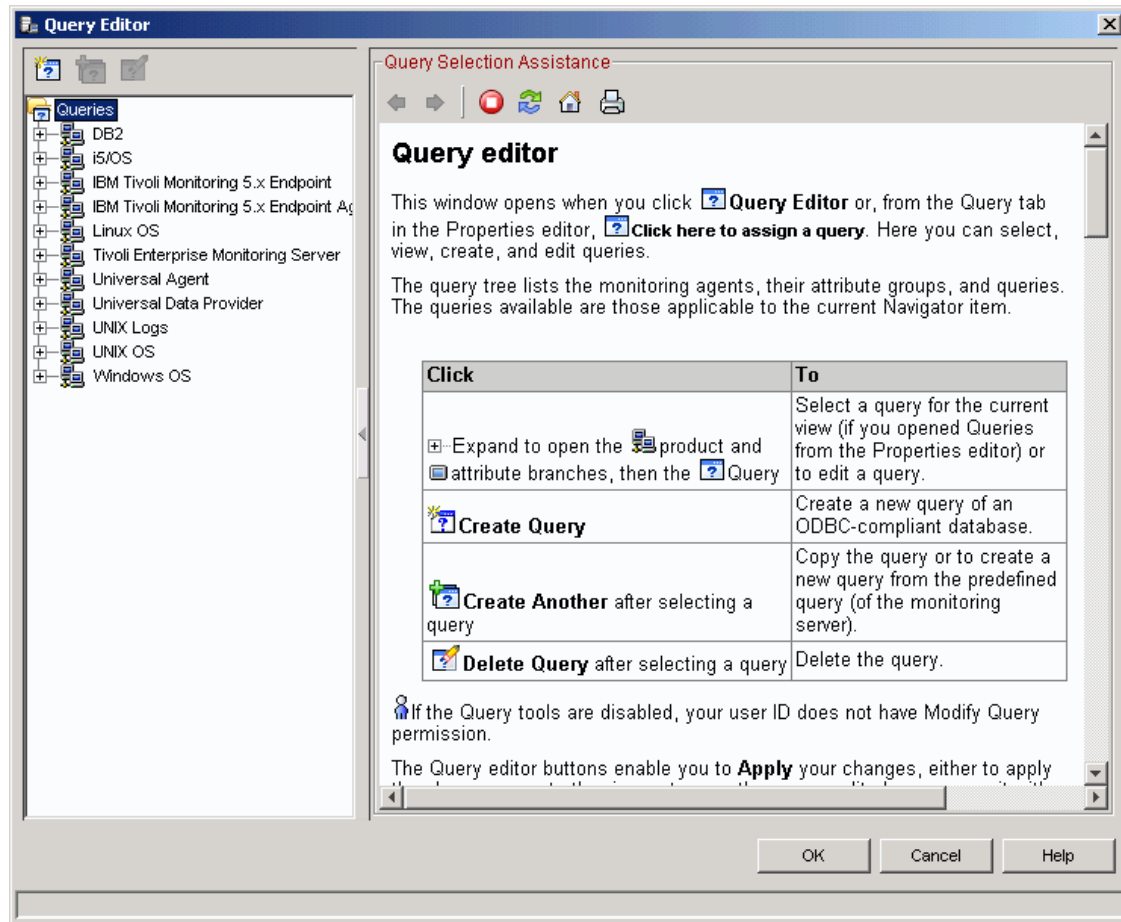
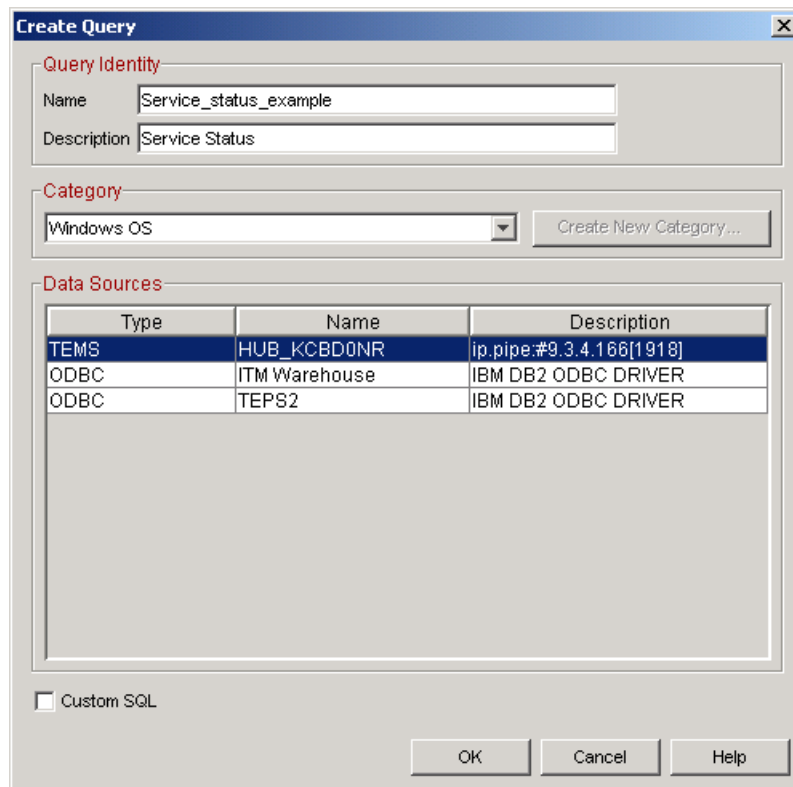


Figure 5-11 Query Editor

7. Select the **Create Query** icon.
8. This brings up the Create Query window. Name that query as Service\_status\_example and enter Service status as the description.

**Attention:** When you change a query, you affect every view where this query is being used. Be careful, because you might be changing other users' views.

9. In the Category select **Windows OS**.
10. For Data Sources, select **TEMS**, as shown in Figure 5-12.



The 'Create Query' dialog box is shown with the following fields and options:

- Query Identity:**
  - Name: Service\_status\_example
  - Description: Service Status
- Category:**
  - Dropdown menu: Windows OS
  - Button: Create New Category...
- Data Sources:**

Type	Name	Description
TEMS	HUB_KCBD0NR	ip.pipe.#9.3.4.166[1918]
ODBC	ITM Warehouse	IBM DB2 ODBC DRIVER
ODBC	TEPS2	IBM DB2 ODBC DRIVER
- ☐ Custom SQL
- Buttons: OK, Cancel, Help

Figure 5-12 Create Query

11. Click **OK**.
12. The Select attribute windows opens. Select Attribute Group **NT Services** and hold **CTRL** key to select **Current State**, **Display Name**, **Server Name** and **Service Name** in the Attribute item box, as shown in Figure 5-13.

**Note:** Monitoring agents are made up of attributes, that represent the properties of systems or networks, such as the amount of CPU usage or the message ID.

Attributes are organized into attribute groups. The attributes in a group can be displayed in a table view or chart view or used to specify a condition for testing in a situation. When you open the view or start the situation, data samples are taken of the selected attributes. IBM Tivoli Monitoring, V6.1 comes with a set of common attribute groups that can be applied to any managed system.



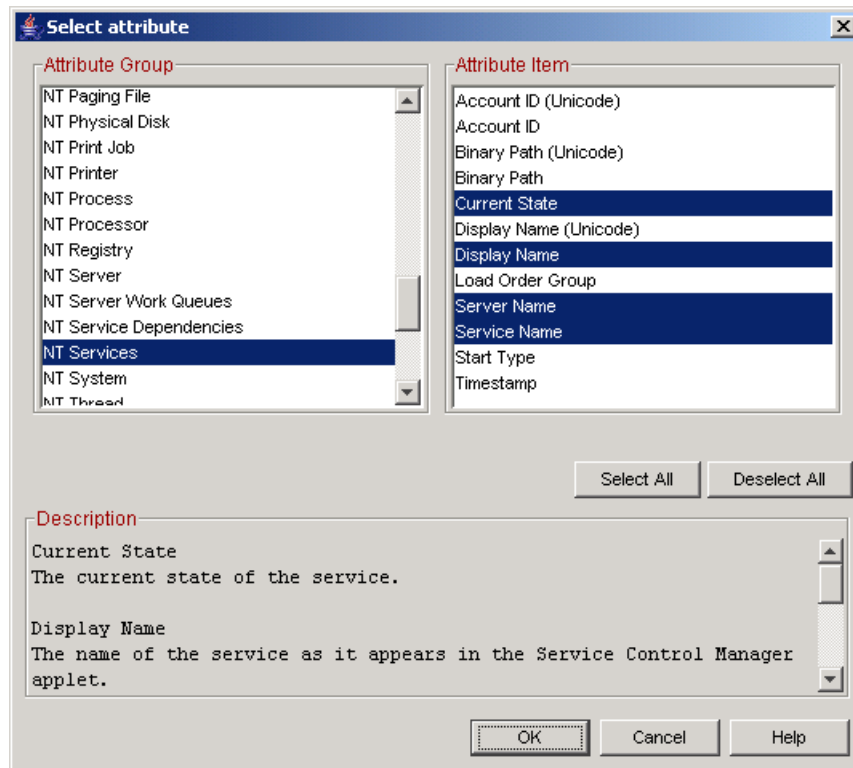


Figure 5-13 Selecting attributes

13. Click **OK** to finish the selecting attributes.
14. Now we have a new query under Query Editor (Figure 5-14). We need to configure this query.

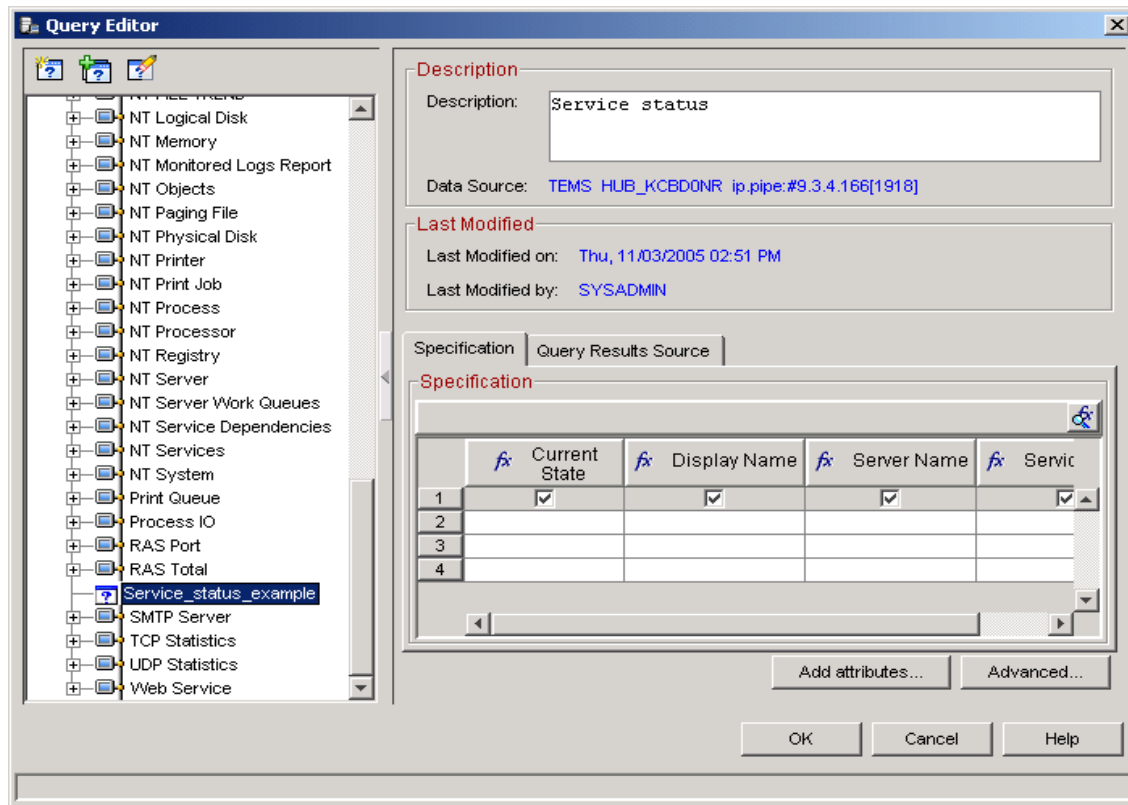


Figure 5-14 New query

15. In Specifications, click under **Current State** column and change the operator to **!= (Not equal)** and type Stopped.
16. Click under Server Name column and type \$NODE\$. Leave the operator as == (Equal), as shown Figure 5-15.

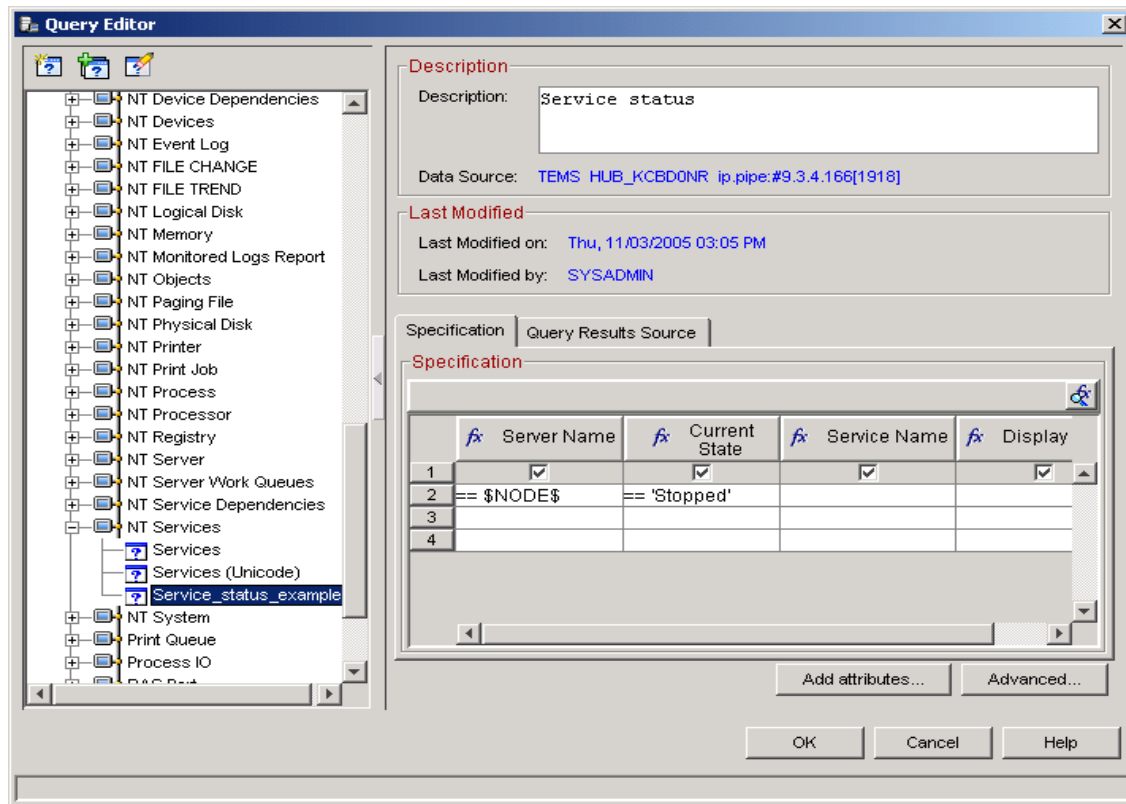


Figure 5-15 Query Editor Specification

17. Click the **Advanced** button, in Advanced Options, select **Ascending** for Sort By, select **Display\_Name** (Figure 5-16) and click **OK**.

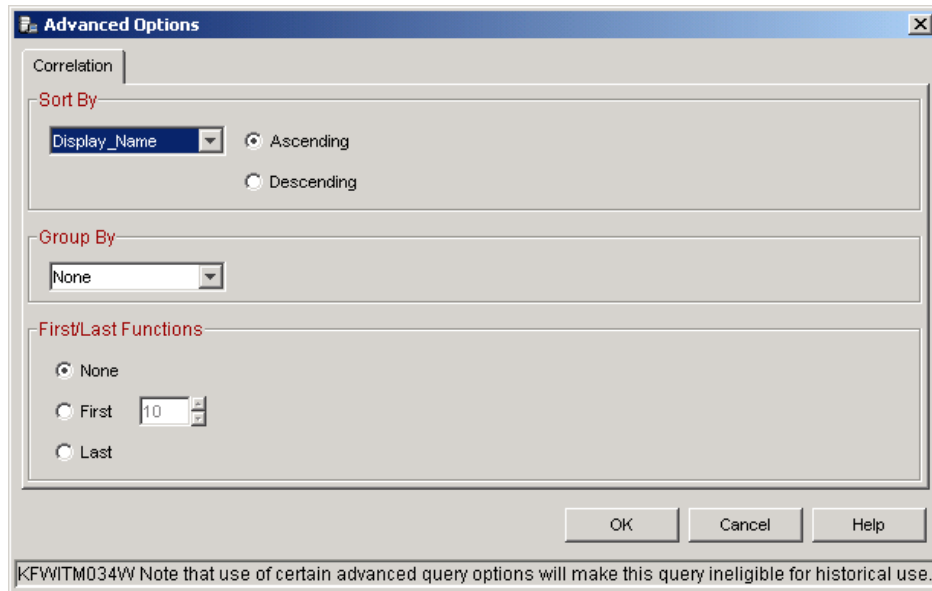


Figure 5-16 Advance Options

18. Click **OK** to close the query. The Preview shows any service with Service Status equals Stopped.
19. We can filter this to track certainly services status. Click **Filters**, under the Service Name, select **== Equal** and type Messenger in Service name as shown in Figure 5-17.

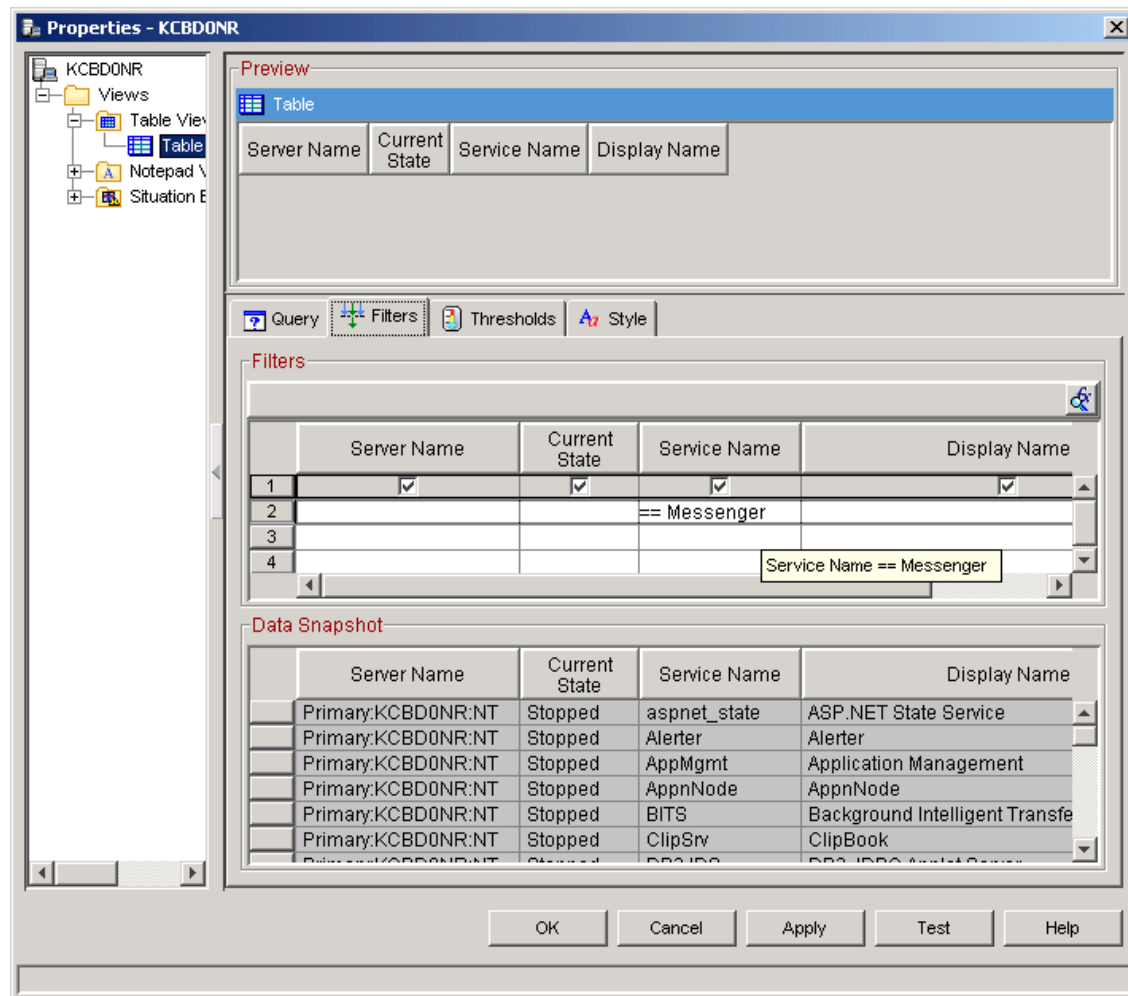


Figure 5-17 Filter Service Name

20. Click **Style** tab to change the table name. In the Options, select **Show** checkbox, in the Title types select **Service Status Stopped** and click **OK**.
21. Now we have the Services Status Stopped table view added. Select **File Save Workspace** to save this last configuration.

Since Messenger service is running, we can not see any row in table view, as shown Figure 5-18.

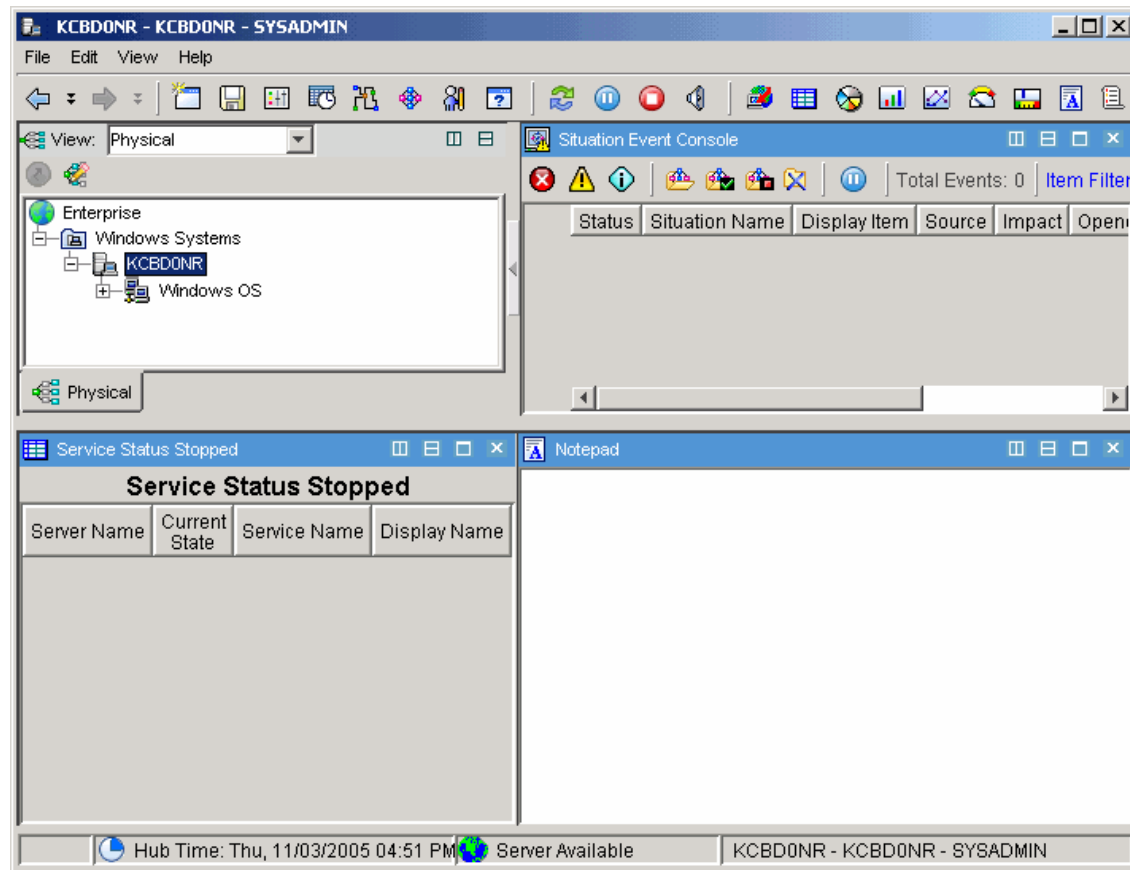


Figure 5-18 New view - Service Status Stopped

We can reproduce the service stopping to see the view behavior.

1. In Windows click **Start Run...** and type cmd in the Open window.
2. Click **OK**.
3. In command prompt, type **net stop messenger**. The following message appears.  
The Messenger service is stopping.  
The Messenger service was stopped successfully.
4. Open Tivoli Enterprise Portal Client and notice (Figure 5-19) that service is listed as stopped.

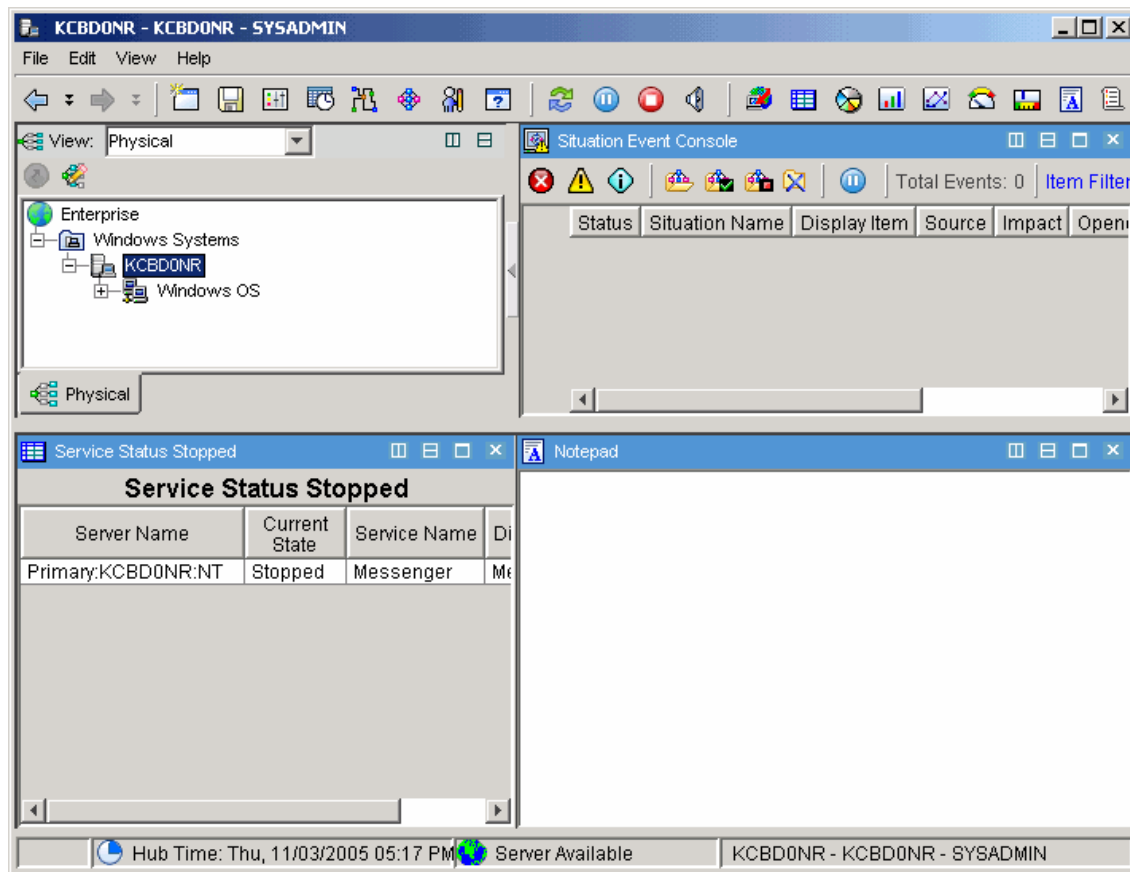


Figure 5-19 Service stopped

### Adding a chart view

Now that we have a table view, we can add a chart view in our workspace.

1. In Tivoli Enterprise Portal, select the Pie Chart view and click in the right view at the bottom side, answer **Yes** to “Assign query now” question.
2. In Properties window click **Click here to assign a query**.
3. In the Query Editor expand **Windows OS** → **NT Logical Disk** → **Logical Disk** and click **OK**.
4. Select **Filters** tab, we need filter what we want to show in our Pie Chart.

**Note:** Different than Queries when we use Filters we do not affect other views.

5. Select **%Used** and **%Free**. Under the Disk Name, select **== Equal** and type **C:..**.
6. Select the **Style** tab in order to name the view. In Options, select **Show** checkbox and in the Text box type Drive Space.
7. Click **OK** to add this view to our workspace, as shown in Figure 5-20.

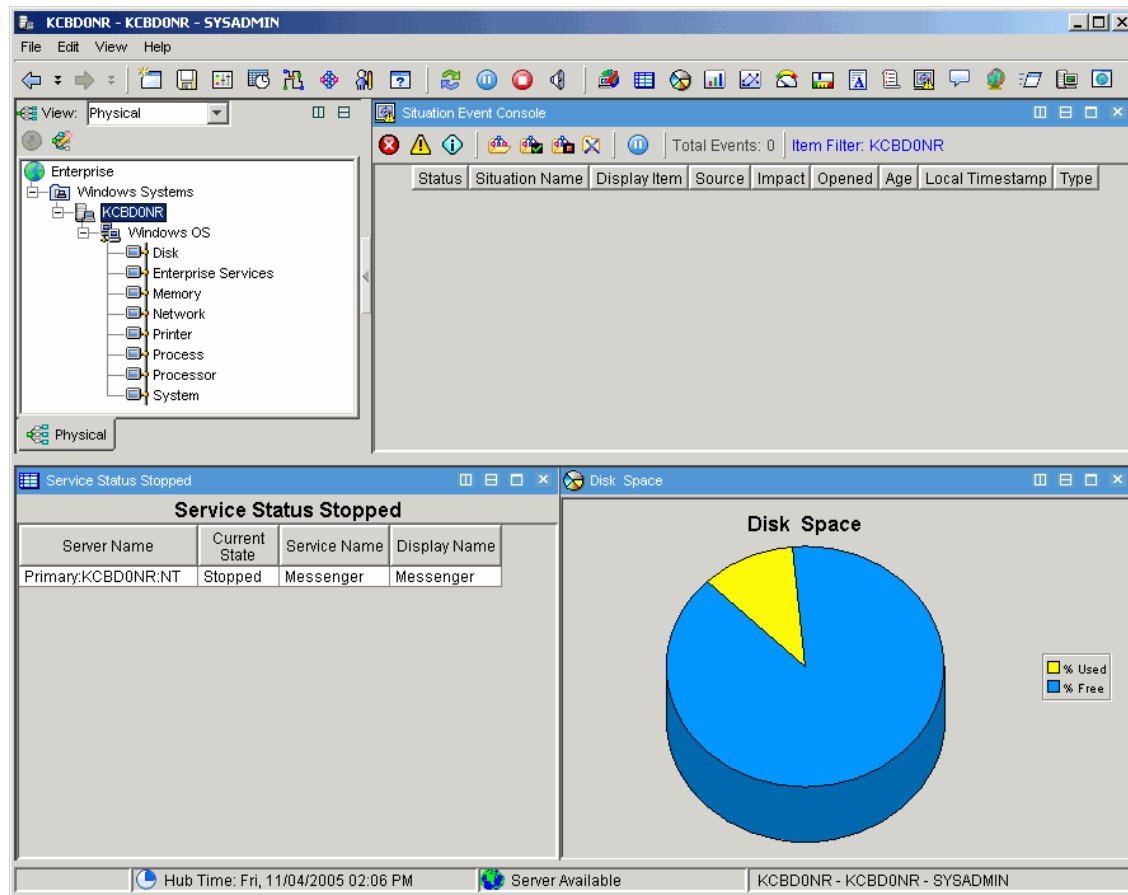


Figure 5-20 Disk Space Chart Pie view

## Installing IBM Tivoli Monitoring Agent for Databases

Since we only have one Monitor Agent running this next step we install Monitoring Agent for Databases DB2.

Following the next steps to install IBM Tivoli Monitoring, V6.1 for Databases:

1. Log on to the system with the Administrator account.



2. Access IBM Tivoli Monitoring, V6.1 installation image. In our case, it was under C:\ITM61\_image\db\_agent.

**Note:** You can also install IBM Tivoli Monitoring, V6.1 Databases from the CD image.

3. Open Windows folder and launch **setup.exe**. This launch IBM Tivoli Monitoring for Databases - InstallShield Wizard.
4. In Welcome to IBM Tivoli Monitoring for Database click **Next**.
5. In Software License Agreement window, click **Accept** to accept the License Information.
6. Expand each of the four sections and check the box that corresponds to the DB2 Agent as shown in Figure 5-21.

**Attention:** Do not unselect Tivoli Enterprise Monitoring Agent for Framework.

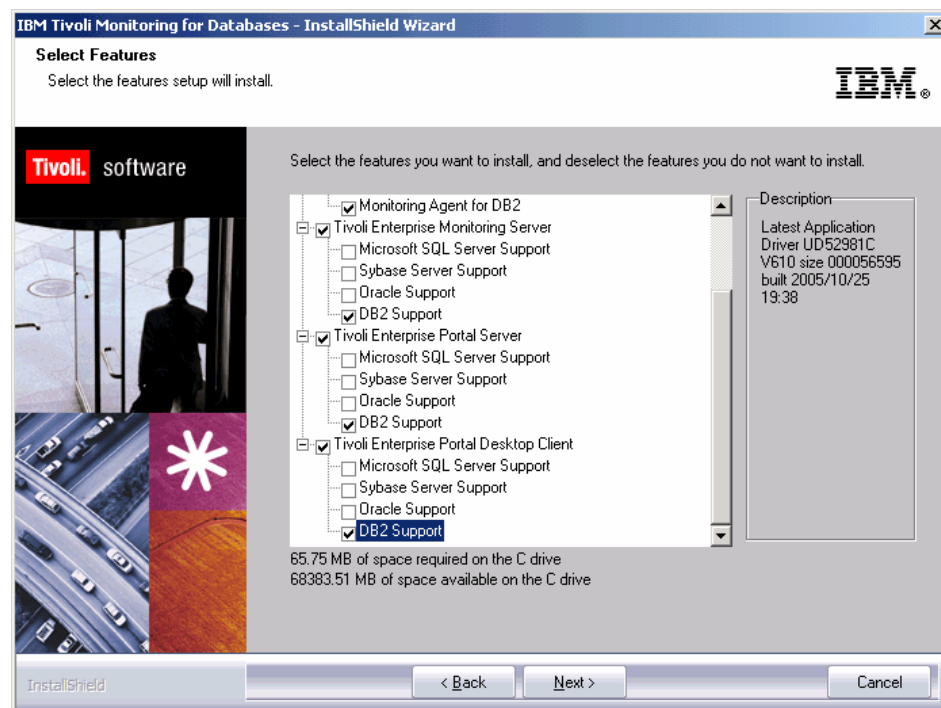


Figure 5-21 Select Features

7. Click **Next**.

8. Select **Monitoring Agent DB2** in Agent Deployment and click **Next**.
9. Click **Next** in Start Copying Files.
10. After finished the files copy, we need to configure the components. Click **Next** in Setup Type window, as shown in Figure 5-22.

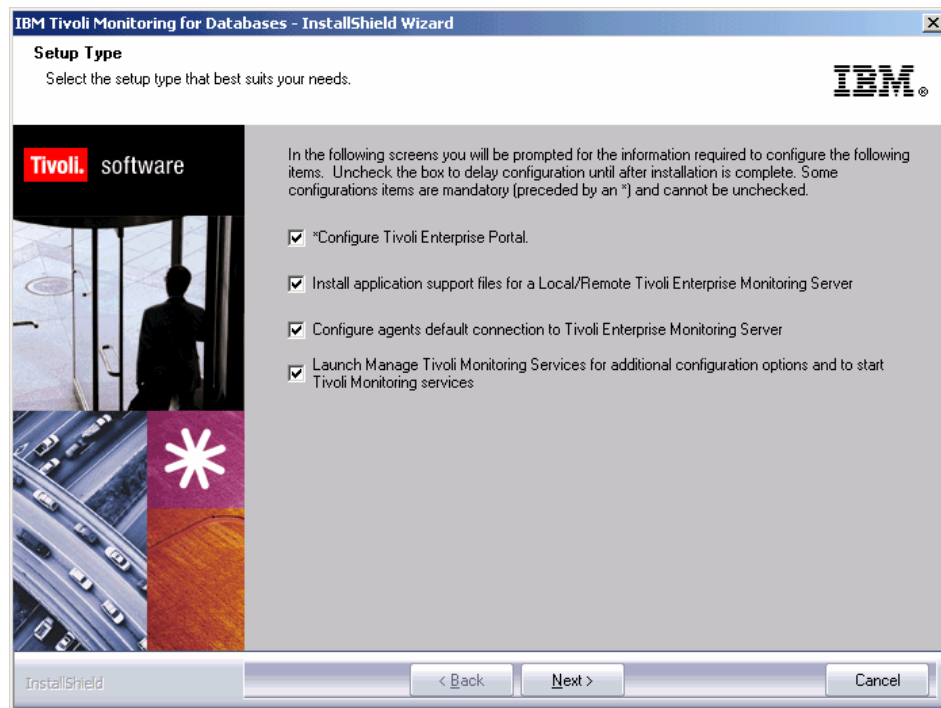


Figure 5-22 Setup Type

11. Click **Next** in Define TEP Host Information.
12. After a while the Tivoli Enterprise Monitoring Server Configuration windows pop up, click **OK** to accept TEMS configuration, and **OK** again in Hub TEMS Configuration window.
13. Click **OK** in Add application support to the TEMS window and **OK** again in Manage Tivoli Enterprise Monitoring Services.
14. Click **OK** in Select the application support to add to the TEMS (Figure 5-23), this will add DB2 Support to TEMS.

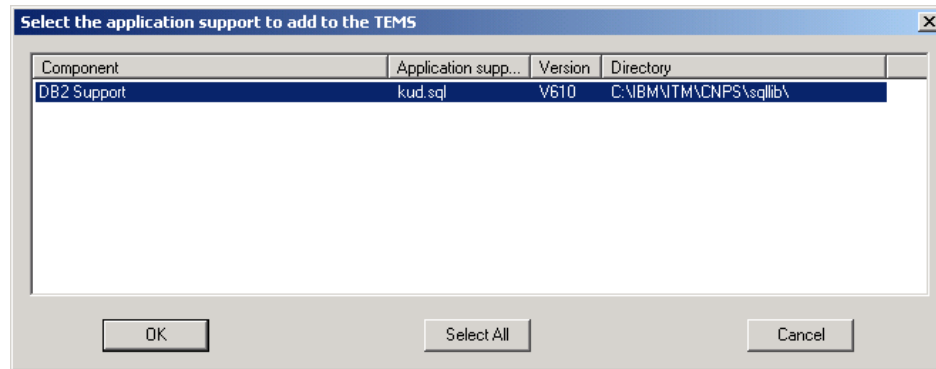


Figure 5-23 Select the application support to add to the TEMS

15. Click **Next** in Application support addition complete, that window shows the installation status, the rc:0 (Figure 5-24) indicates that no error has occurred.

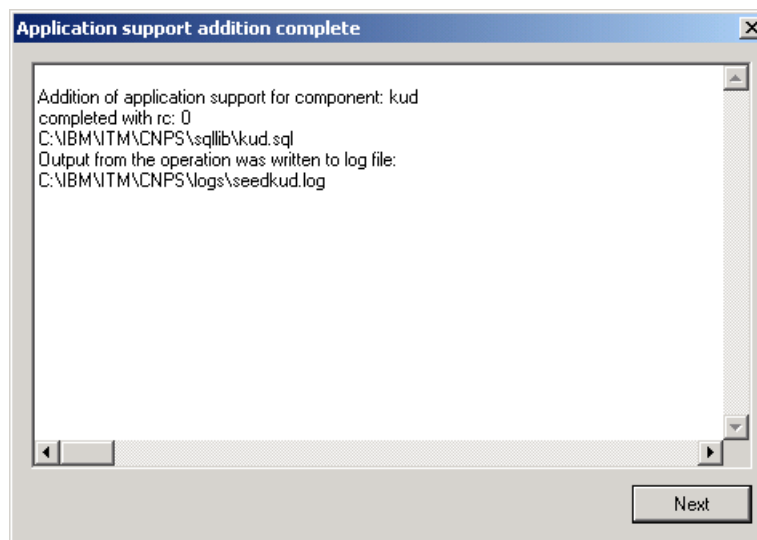


Figure 5-24 Application support addition complete

16. Select **OK** in Configuration Defaults for Connecting to a TEMS server and **OK** in Configuration Defaults for Connecting to a TEMS IP.PIPE Settings.
17. The IBM Tivoli Monitoring Services will be recycled and we can click **Finish**.

After finishing the installation, the Tivoli Enterprise Monitoring Services windows pops up. You will notice a new line as shown in Figure 5-25, but there is no

✚ (running man) next to it and the Task/SubSystem column shows *Template* for this item. We use this item to configure a database instance.

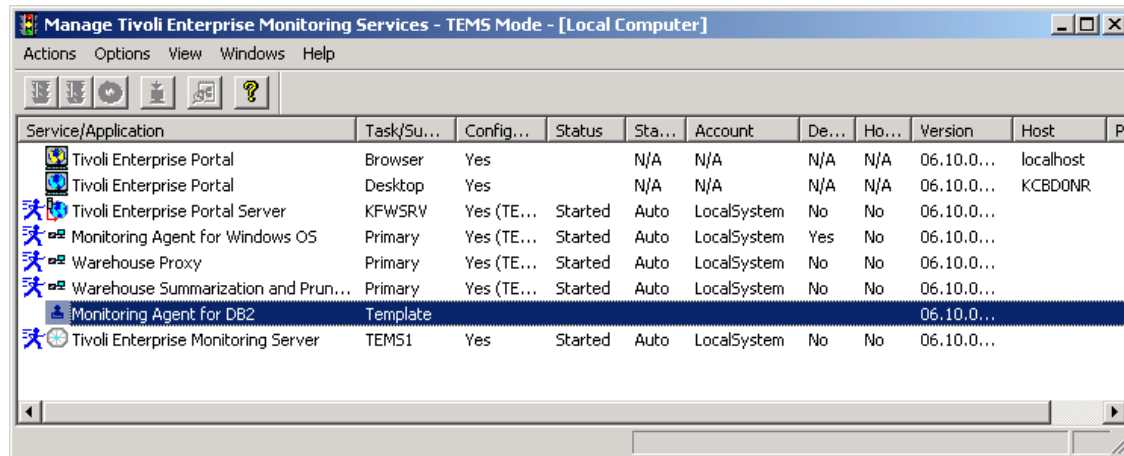


Figure 5-25 Monitoring Agent for DB2 Template

### Configuring IBM Tivoli Monitoring Agent for Databases DB2

To configure the agent do the following:

1. Right click the **Monitoring Agent for DB2** and select **Configure Using Defaults**.
2. In Monitoring Agent for DB2 type DB2 as the name of DB2 instance name and click **OK** as shown in Figure 5-26 on page 260.

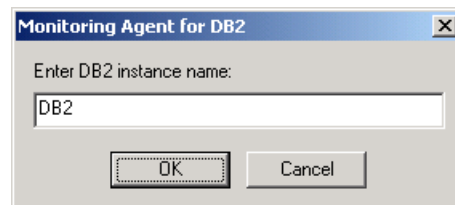


Figure 5-26 Enter DB2 instance name

3. Now, we will see another service in Manage Tivoli Enterprise Monitoring Service, as shown in Figure 5-27.

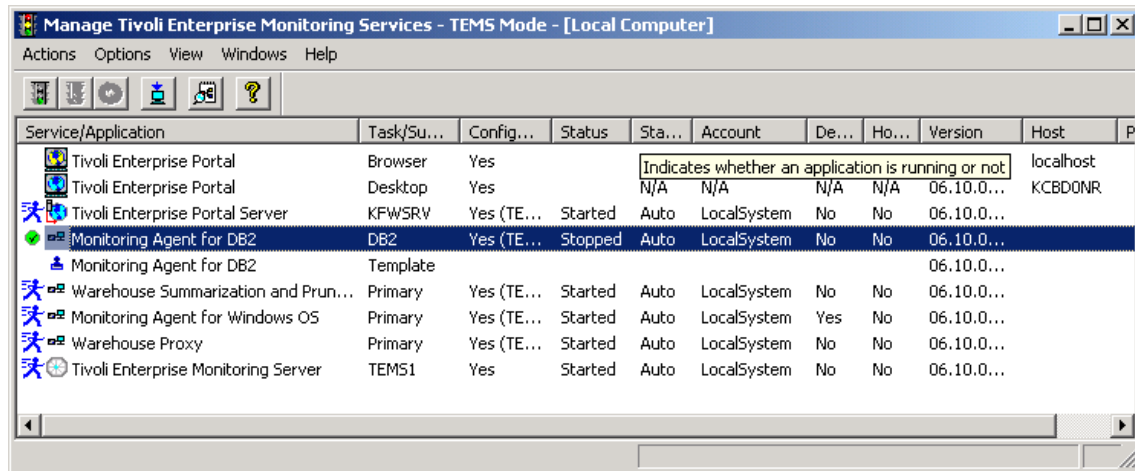


Figure 5-27 Monitoring Agent for DB2 instance DB2

4. We need start the new Monitoring Agent for DB2. Right click **Monitoring Agent** for DB2 and select **Change Startup...** , as shown in Figure 5-28.

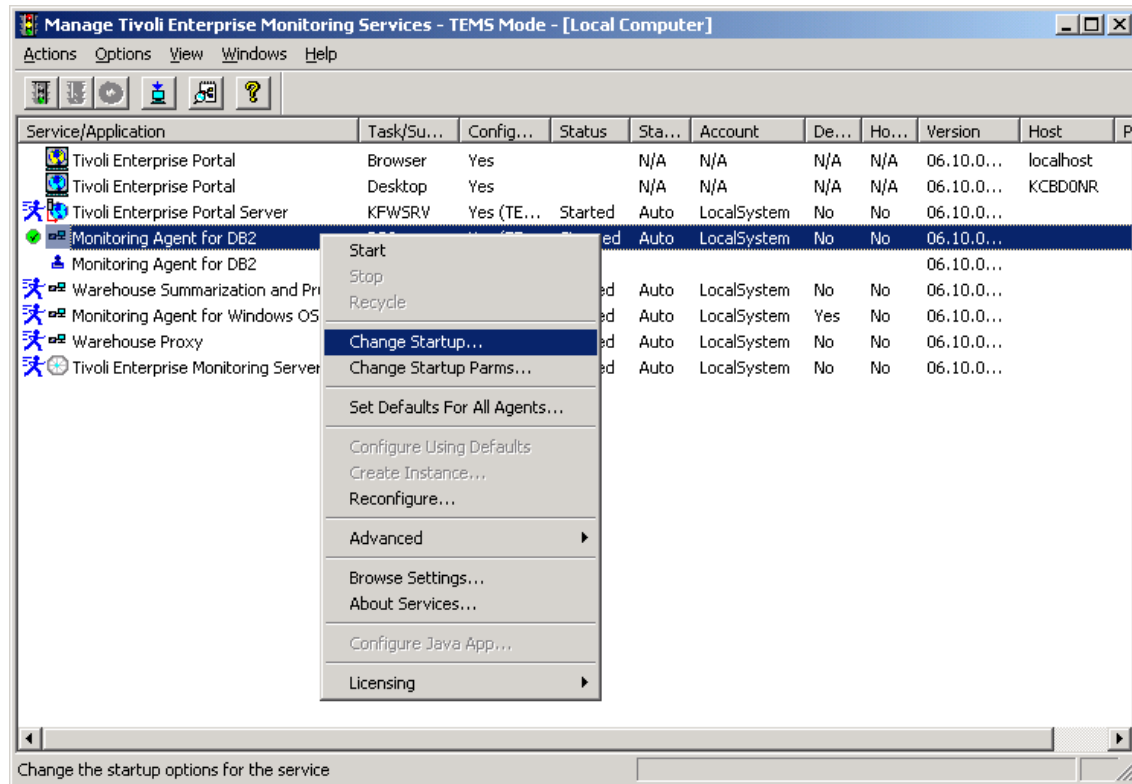


Figure 5-28 Change Startup

5. In Service Startup for Monitoring Agent for DB2 click on **This Account**, enter the User ID db2admin, Password itm61rbdg and click **OK** as shown in Figure 5-29.

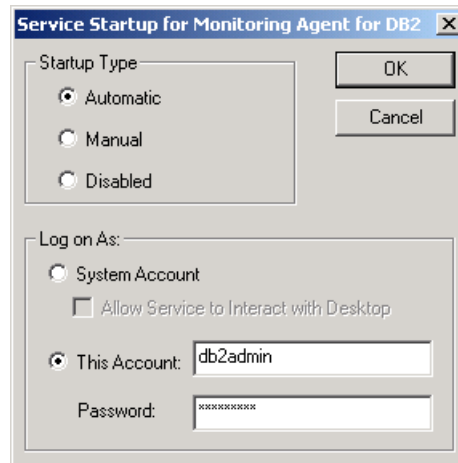


Figure 5-29 Service Startup for Monitoring Agent for DB2

6. The Service On Change message will pop up (Figure 5-30) explaining that service will start with another account, click **OK**.

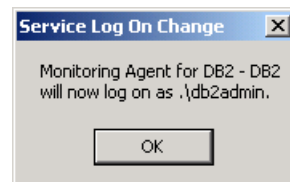


Figure 5-30 Service Log On Change

7. Double click **Monitoring Agent for DB2** to start it.

Now we come back to Tivoli Enterprise Portal client. Notice that a green icon appears in Navigator view (Figure 5-31). It means that we have updates pending in the Navigator tree.

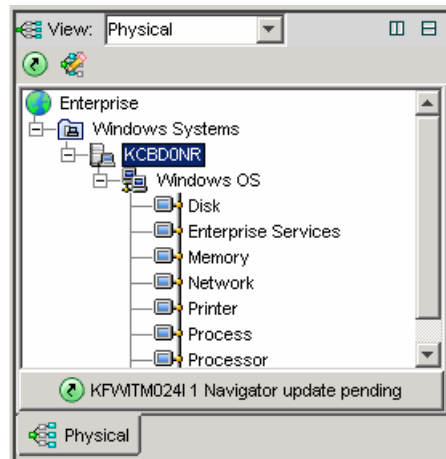


Figure 5-31 Navigator update pending

When one Monitoring Agent is added or deleted we have to refresh the Navigator, just click in to **Refresh**. You can see that there is a new agent listed in Navigator, as shown in Figure 5-32.

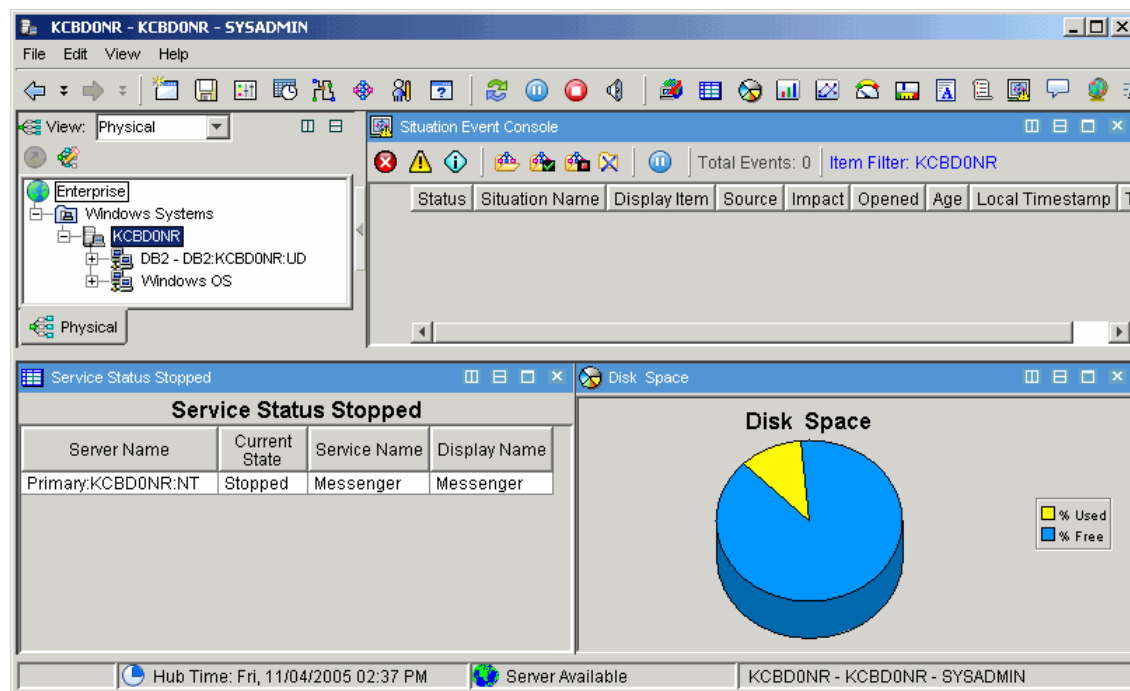







Figure 5-32 New agent add to Navigator





Finally, we can add a table view with some information about Monitoring Agent for Databases. Before we do that, we need create another view. In the view toolbar, we have these tools for creating the view.

-  Split view horizontally
-  Split view vertically
-  Maximize the view
-  Close the view

Follow these instructions in order to divide and add this new view:

1. Click on  to split the Service Status Stopped view horizontally.

**Note:** We have two views with the same query, before we add a table view, we need to clean the previous query, we can add a  Notepad view to clean it.

2. Click in  **Notepad** view and click on **Service Status Stopped.1** view. Now we have a Notepad view as show in Figure 5-33.

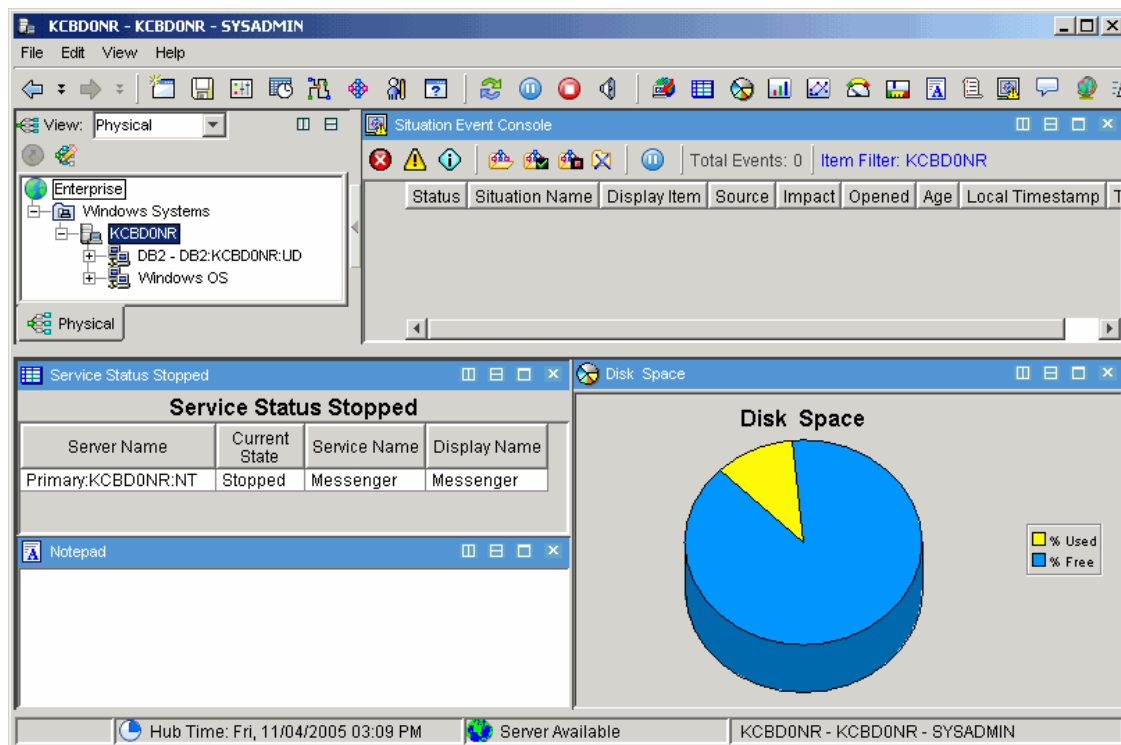



Figure 5-33 Notepad view

3. Select  **Table** view and click on **Notepad** view.
4. Click **Yes** for the “Assign query now” question.
5. In Properties window, click **Click here to assign a query**.
6. In the Query editor expand **DB2** → **KUDINFO00** → **System Overview** and click **OK**.
7. Select the **Filters** tab.
8. In Filters, select only **Node Name**, **db2 status** and **db2start time** as shown in Figure 5-34.

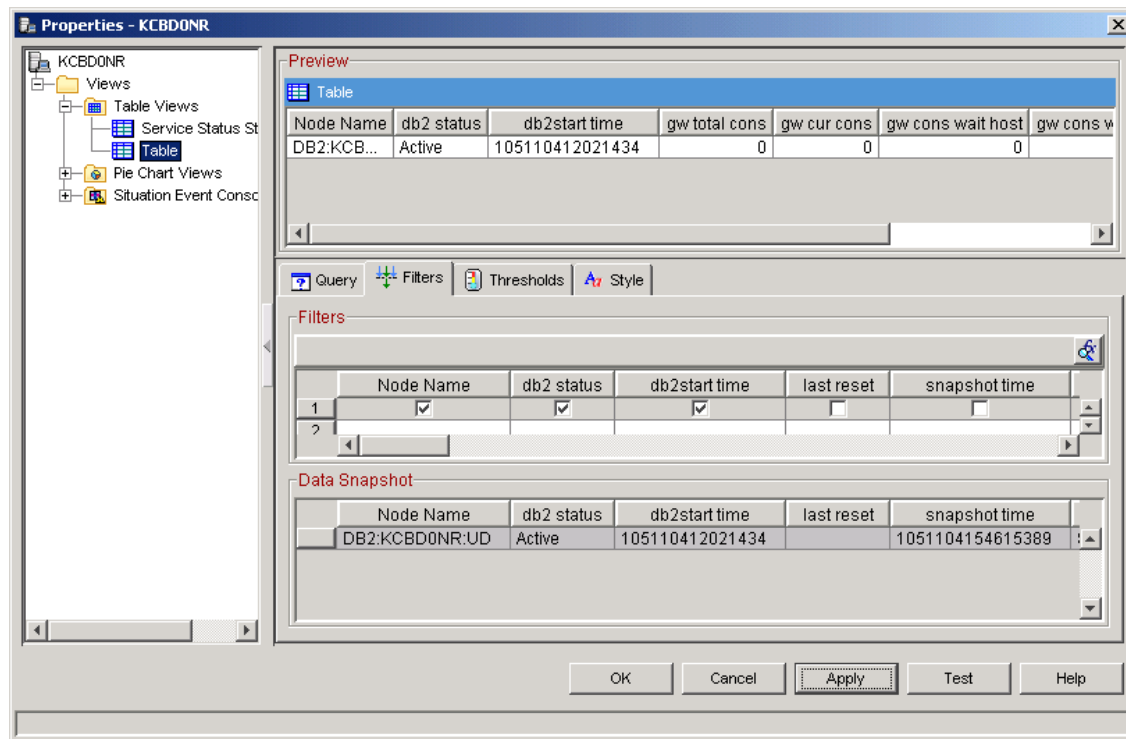


Figure 5-34 Selecting Filters

9. In the Style tab, select **Show** checkbox and type DB2 Status in the Title.
10. Click **OK** to see the new view as shown in Figure 5-35.

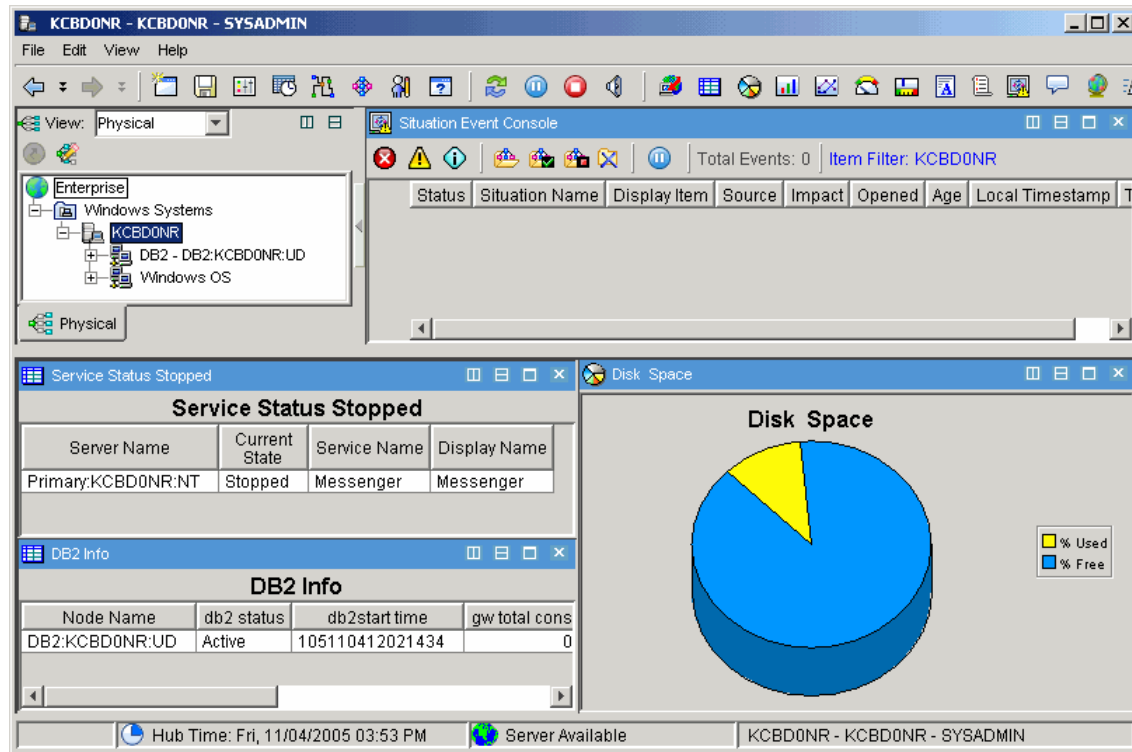


Figure 5-35 DB2 Info view

### Working with thresholds

In Table views, we can add thresholds to highlight cells, whose values meet the threshold set. We also can have thresholds for Circular Gauge charts and Linear Gauge charts.

In this example, we will split vertically the DB2 Info table to add another table view and work with a threshold.

1. Click on to split the DB2 Info view horizontally.
2. Click on **Notepad** view and click on **DB2 Info.1**.
3. Select **Table** view and click on **Notepad** view.
4. Click **Yes** for Assign query now question.
5. In Properties window click **Click here to assign a query**.
6. In the Query Editor expand **Windows OS** → **NT Process** → **Process Overview** and click **OK**.
7. Select the **Filters** tab.

8. In the Filters windows, select only **Process Name**, **ID Process** and **%User Time** time as shown in Figure 5-36.

	Process Name	ID Process	% User Time
1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Figure 5-36 Filters

9. Select **Thresholds** tab.
10. Now set the Thresholds values for **%User Time** as show in Figure 5-37.




		Process Name	ID Process	% User Time
1	 Critical			> 20
2	 Warning			> 10
3	 Informational	abc == Idle		< 5

Figure 5-37 Thresholds values

11. Click on the **Style** tab and select **Show** checkbox and type Process %User Time for the Title.
12. Click **OK** to add this new view.
13. In Process %User Time click **%User Time** to order the values, now we can see the thresholds working as shown in Figure 5-38.

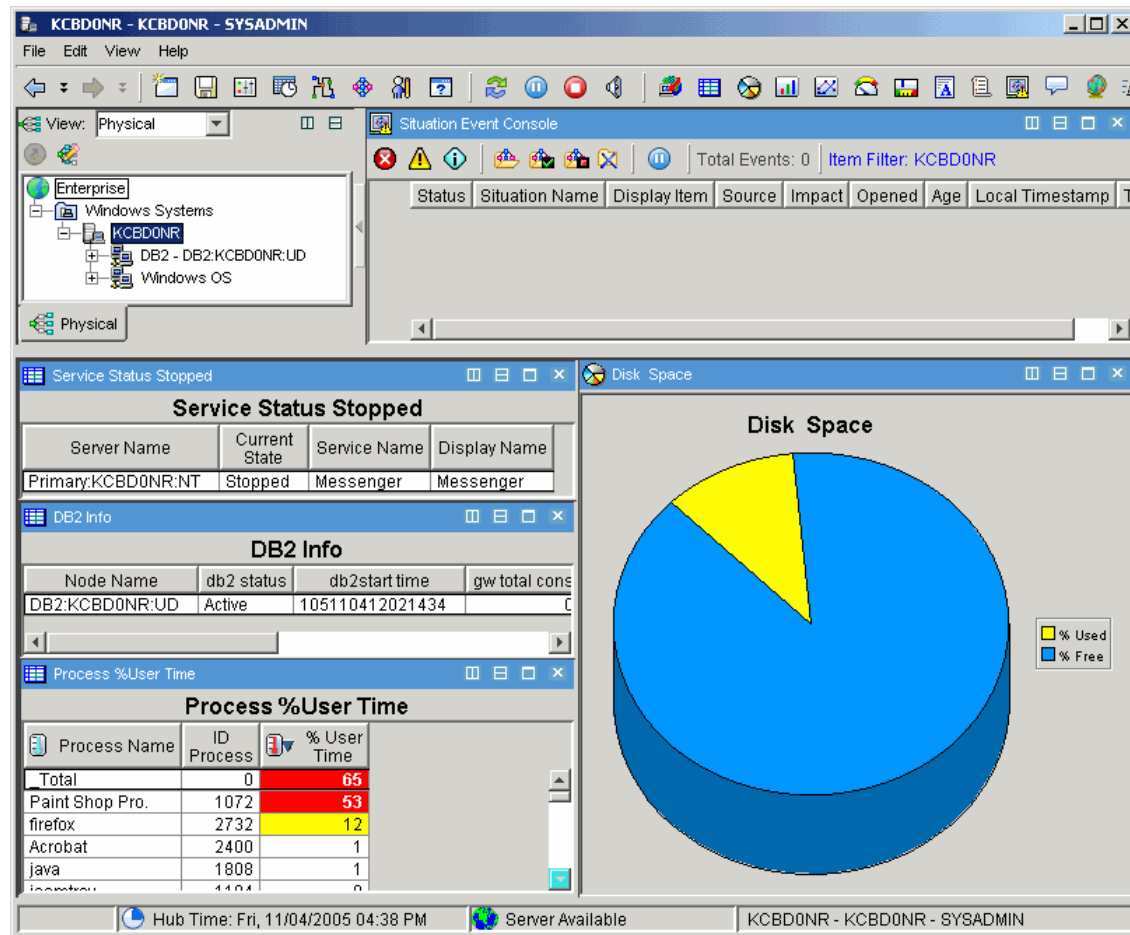


Figure 5-38 Thresholds

### 5.2.3 Working with a situation and events

A situation describes conditions you want to test on a managed system. When you start a situation, Tivoli Enterprise Portal compares the situation with the values collected by the Tivoli Enterprise Monitoring Agent and registers an event if the conditions are met. You are alerted to events by indicator icons that appear in the Navigator.








#### Create a situation

Each Tivoli Enterprise Monitoring Agents have a set of predefined situations ready to use. You can also create and customize your own situations to monitor

specific conditions in your enterprise. If a situation already exists that is similar to one you want, you can copy the original and edit the copy.



### ***Open the Situation editor***

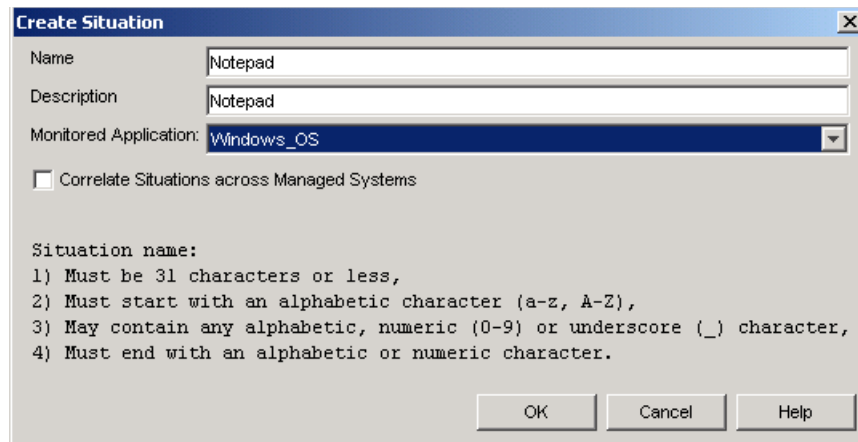
We have several ways to open the Situation editor:

- ▶ In Tivoli Enterprise Portal Toolbar, click  **Situation**.  
When opened through the tool bar, the Situation editor has no connection with the Navigator. You can see all situations available in your monitored network, you can edit or delete any of them, create new situations, and distribute a situation. Distribution to a managed system means the situation is running on that system. But you cannot associate situations with Navigator items or change their state or sound.
- ▶ Right-click a Navigator item and click  **Situation**.  
The Situations tree shows the situations associated with the Navigator. The    state and the sound for the situation is also associated with the Navigator item. You can give the same situation a different state for different Navigator item associations.
- ▶ Right-click the event item in the Navigator and click  **Edit Situation**.  
The situation opens in the Situation editor for reviewing and editing.
- ▶ Right-click an open event in the event console view or in the event flyover list and click  **Edit Situation**.  
The situation opens in the Situation editor for reviewing and editing. You cannot disassociate (or associate) the situation with a Navigator item, nor can you change its state or sound here.

### ***Creating a situation***

We can create a situation that verifies whether Notepad is running.

1. Open Tivoli Enterprise Portal,
2. In Navigator select **KCBD0NR**, this opens the workspace that we have been working.
3. Right-click **KCBD0NR** in the Navigator and click and click  **Situation...**
4. In the Situation for **KCBD0NR** select  **Create new Situation**.
5. This opens the Create Situation window. In the Name field type Notepad, in the Description field enter Notepad and select **Windows\_OS** in Monitored Application as in Figure 5-39.



The image shows a 'Create Situation' dialog box with a blue title bar and a close button. It contains three input fields: 'Name' with 'Notepad', 'Description' with 'Notepad', and 'Monitored Application' with a dropdown menu showing 'Windows\_OS'. Below these is an unchecked checkbox labeled 'Correlate Situations across Managed Systems'. A section titled 'Situation name:' lists four rules: 1) Must be 31 characters or less, 2) Must start with an alphabetic character (a-z, A-Z), 3) May contain any alphabetic, numeric (0-9) or underscore (\_) character, and 4) Must end with an alphabetic or numeric character. At the bottom are 'OK', 'Cancel', and 'Help' buttons.

**Create Situation**

Name: Notepad

Description: Notepad

Monitored Application: Windows\_OS

☐ Correlate Situations across Managed Systems

Situation name:

- 1) Must be 31 characters or less,
- 2) Must start with an alphabetic character (a-z, A-Z),
- 3) May contain any alphabetic, numeric (0-9) or underscore (\_) character,
- 4) Must end with an alphabetic or numeric character.

OK Cancel Help

Figure 5-39 Create Situation

6. Click **OK**.
7. In Select condition window, select Condition Type **Attribute Comparison**, Attribute Group **NT Process** and Attribute Item **Process Name** as in Figure 5-40.

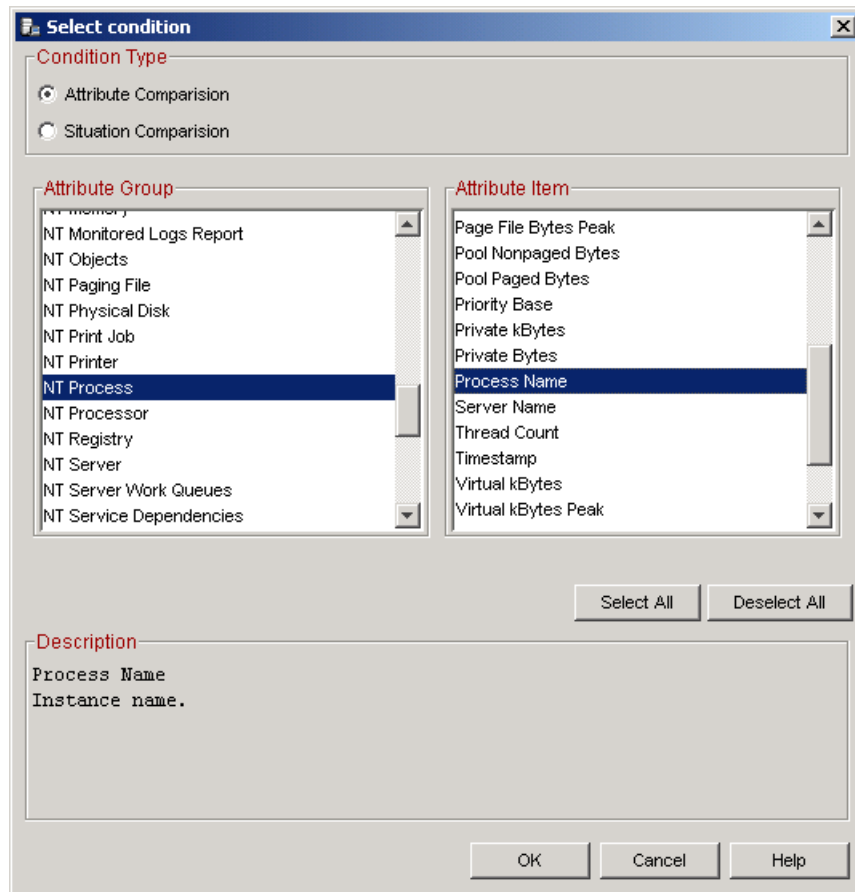


Figure 5-40 Select condition

8. Click **OK**.
9. Click in the first row of the Formula.
10. By default, it starts the equation with the Value of Expression Equal to. Click in the first argument and change it to .
11. Type notepad and click **OK**. Make sure that notepad is shown as in Figure 5-41, otherwise the situation will not work.

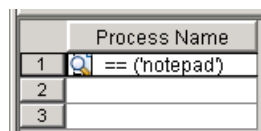


Figure 5-41 Process Name



12. Decrease the Sampling Interval to 2 minutes and change the State to **Informational**.

**Note:** This checks if the process name notepad.exe is running or not. When this process starts, an event appears in Situation Event Console.

13. Select the **Distribution** tab.
14. We need distribute it to the Managed System. Select **NT\_SYSTEM** and move it to the Assigned box, as shown in Figure 5-42.

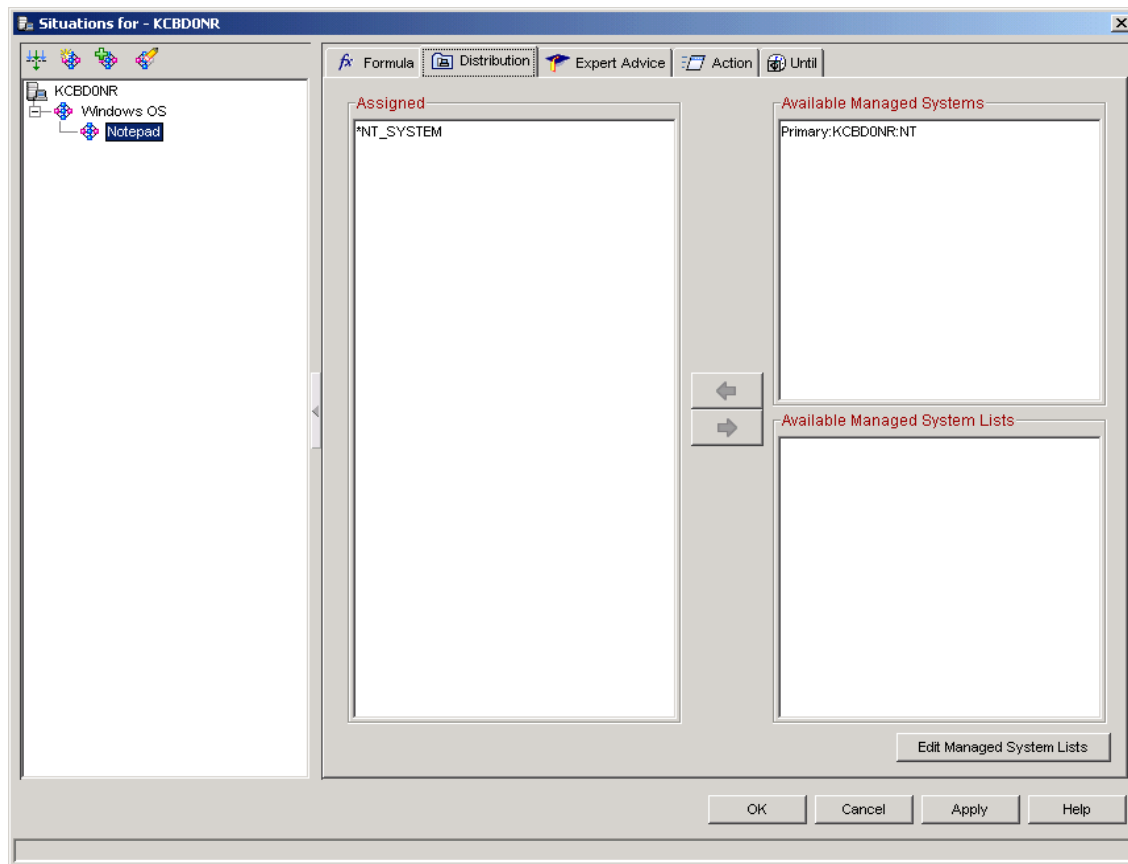


Figure 5-42 Distribution Tab

15. Select **Expert Advice** tab. Here we can send an advice what to do when the situation occurs. Type "Notepad is not running".
16. Click **OK** to save this situation.

### Testing the situation

Since the Notepad is not running, as soon as we save the situation one event indication appears in the Situation Event Console, as shown in Figure 5-43.

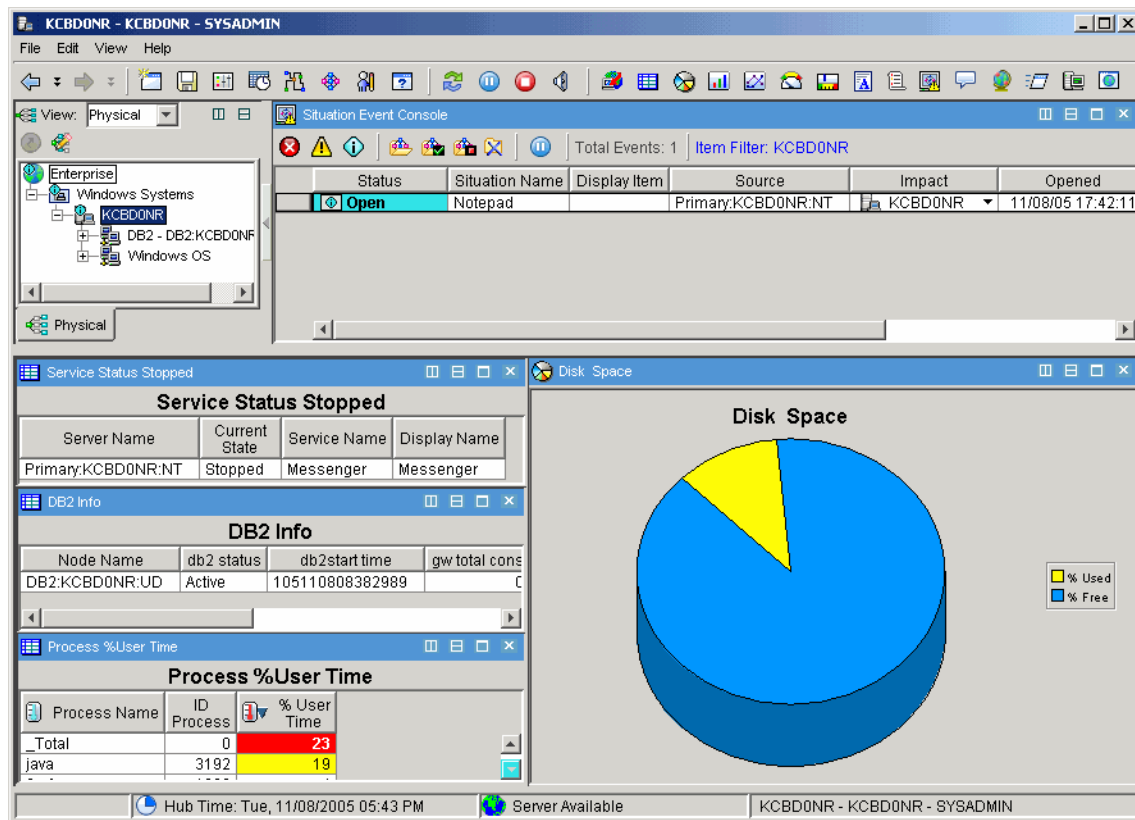


Figure 5-43 Situation Event Console triggered.

If we start the Notepad, this event will close automatically. We can test this using the Launch Application feature in Tivoli Enterprise Portal.

### Launching an application

Sometimes we need to launch an application in the Monitoring Agent, we can do that as follows.

1. In the Navigator, right-click **KCB00NR** and select **Launch....**
2. In Create or Edit Launch Definitions, click **Create New**.
3. In Name: type Launch Notepad.
4. In Target: type notepad.exe.

5. Click **Apply**.
6. Now we have one Existing Launch Definitions, we can select **Launch Notepad** it and click **Launch**.
7. Click **OK** to close Create or Edit Launch Definitions.

Wait for 2 minutes after starting the Notepad. You will see that note in Situation Event Console about the Notepad Situation is not there anymore.

## 5.2.4 Policies for automation

Tivoli Enterprise Portal enables you to automate a situation by including a Take Action command that runs when the situation fires (becomes true). You also have a workflow window for designing and managing policies. A policy is a collection of activities that provide the capability of automating responses to events or routine operator tasks.

Automation with policies enables you to implement more complex workflow strategies than you can create by adding take action commands to a situation. It combines complex automated system processes using policies, with operator intervention and decision-making. You can do the following:

- ▶ Monitor multiple conditions simultaneously on any number of systems
- ▶ Have selected activities take place when conditions occur
- ▶ Notify appropriate user groups and offer them activity choices at specified points in the automated process


After an activity is completed, Tivoli Enterprise Portal receives return code feedback and advanced automation logic responds with subsequent activities prescribed by the feedback.

### Working with Workflow editor

The IBM Tivoli Monitoring 6.1 uses the Workflow editor to work with the policies. Lets see how this works and create one policy as example.


#### *Opening Workflow editor*

Following these steps to start the Workflow editor.

1. Launch the Tivoli Enterprise Portal desktop client.
2. In Navigator select **KCBD0NR**, this opens the workspace that we have been working.
3. In Tool Bar click in  **Workflow Editor** button.

## Analyzing an Existing Policy

We can analyze the defaults policies to get familiarized with Workflow Editor.

1. In Policy Details click in  **Edit Workflow** column at left of **NT\_Process\_Memory** row. This opens the NT\_Process\_Memory - Grapher View as in Figure 5-44.

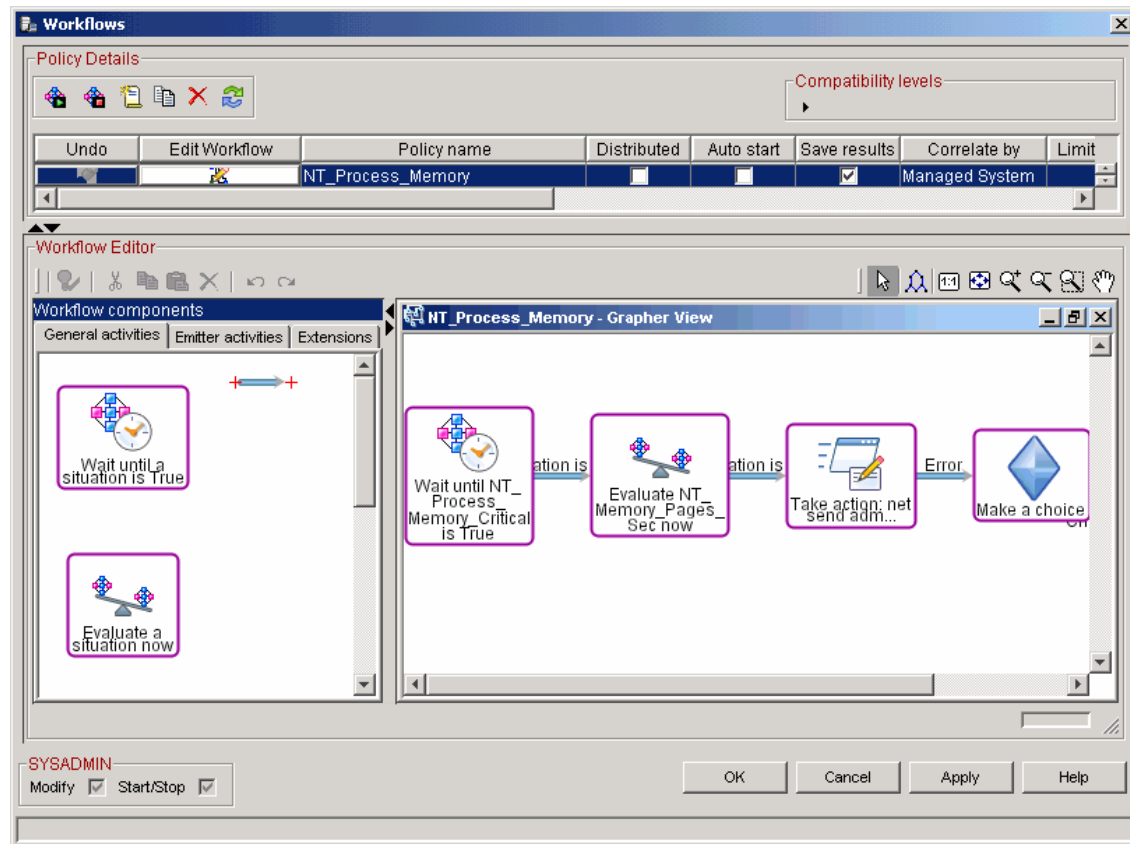


Figure 5-44 Edit Workflow

2. Double-click the **Wait until NT\_Process\_Memory\_Critical is true** workflow component. Now we can see the Select a Situation window, in this case the situation is NT\_Process\_Memory\_Critical but we can select other situations.
3. Double-click the first **connector**. Notice that connectors are policy elements.
4. Follow the workflow and click the components and connectors to see their details and information provided.
5. Expand the **NT\_Process\_Memory - Grapher View** (Figure 5-45). If the NT Process Memory is Critical situation is true, the workflow evaluates if NT

Memory Pages per second situation is occurring in the same Managed System. If the second situation is also true, the system Take an action, in that case it sends a message using **net send** command.

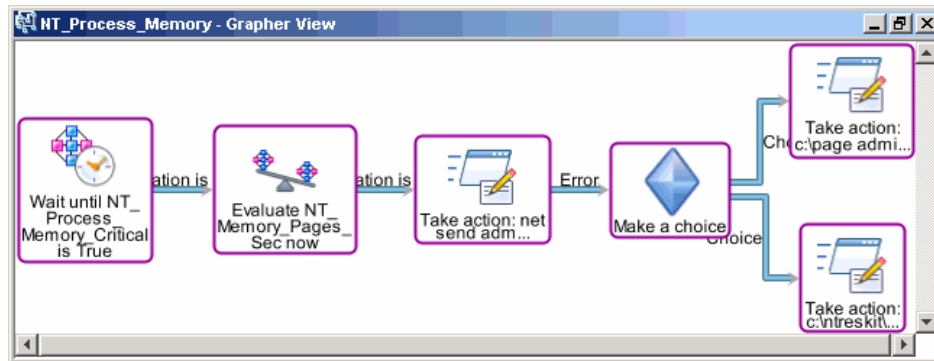


Figure 5-45 NT\_Process\_Memory - Grapher View

There are two possible choices for the connector between the Take Action and Make a choice workflow components. Here we can see additional capability of a policy over a regular situation. In a regular situation, we don't specify alternate actions based on the success or failure of the action. In this case, if the action did not succeed, the next step is to make a choice based on the error.

Double clicking on the Make a choice workflow components, opens User Choice Settings windows. Here, we select the work group that would receive the error notice, and the group that will receive an escalation notice if the problem is not solved in 5 minutes.

The Take Actions workflow components on the right of Make Choice are the choices that the different personnel in each group will be presented with.



### ***Creating a policy***

In this topic we will create a policy that monitors two process existence. If both are not running, the policy will start a program.

Before we create the policy, we need create another situation monitoring mspaint, as described in Section , "Creating a situation" on page 270. Name this situation MSPaint. Also, test the situation, as described in Section , "Testing the situation" on page 274.

With both situations working lets move to the next step.

1. Launch the Tivoli Enterprise Portal desktop client.

2. In Navigator select **KCBD0NR**, this opens the workspace that we have been working.
3. In Tool Bar click in  **Workflow Editor** button to open Workflows.
4. In Policy Details click  **New Policy**. The New\_Policy - Grapher View opens in the Workflow Editor view.
5. In Policy Name type application\_test, check **Distributed**. This opens Change Policy Distribution.
6. Select **NT\_System** and move it to the left under Assigned, as shown in Figure 5-46.

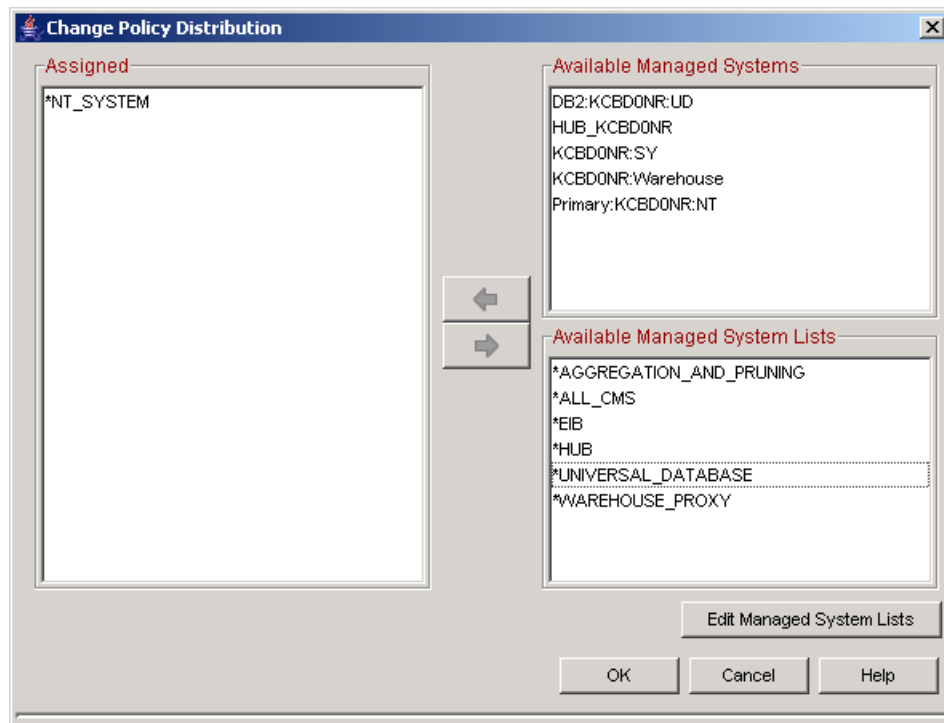


Figure 5-46 Change Policy Distribution

7. Click **OK**. Now we can edit application\_test policy, as shown in Figure 5-47.

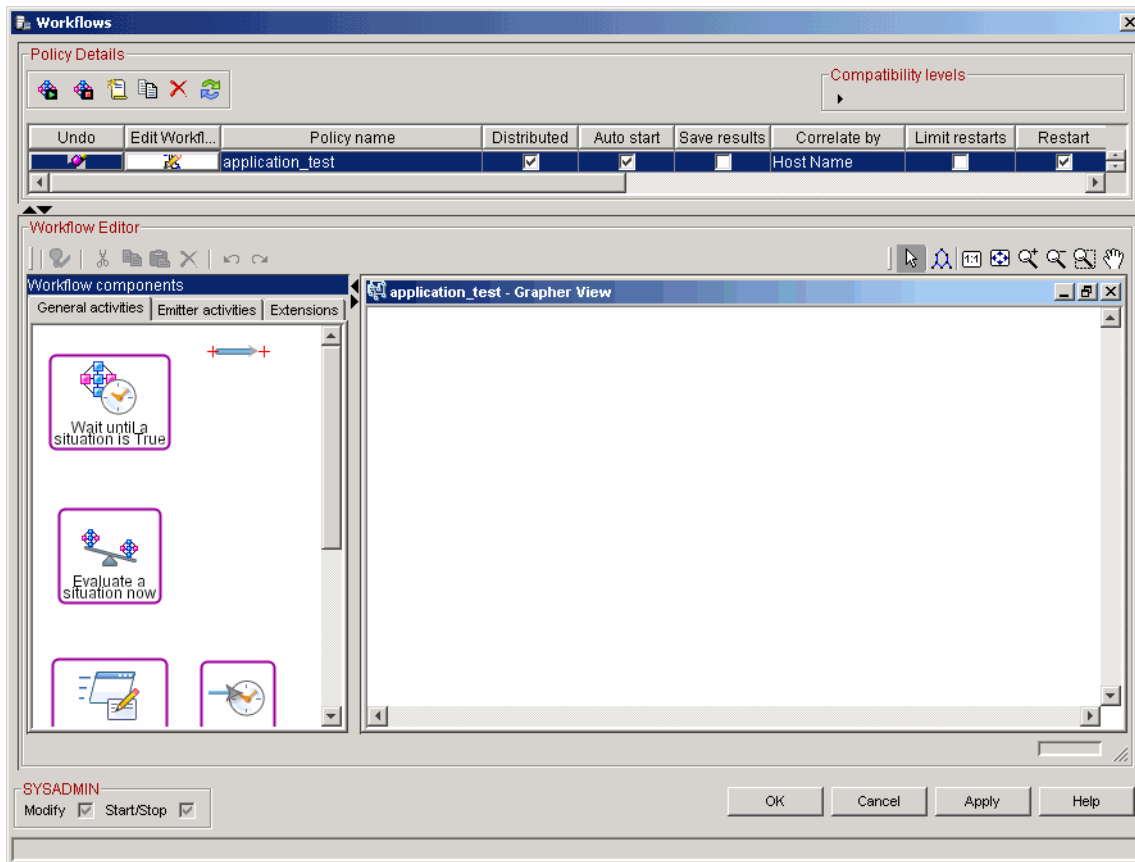


Figure 5-47 Workflow Editor - application\_test

8. In the Workflow Editor, click and drag **Wait until Situation is True** from Workflow components to application\_test - Graph View. This opens the Select a Situation window. Select **Notepad** situation from the list and click **OK**.
9. Click and drag a second **Wait until Situation is True** from Workflow components to application\_test - Graph View and select **MSPaint** in the Select a Situation window.
10. Click **OK**. Now we have two “Wait until Situation is True” icons, as shown in Figure 5-48.

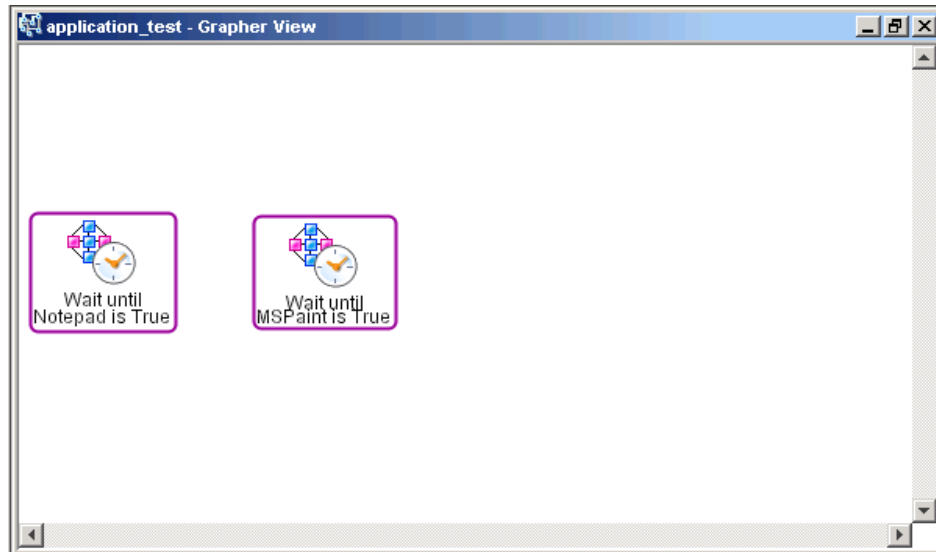


Figure 5-48 Wait until situation is True components.

11. Now click and drag **Take Action or Write a message** workflow component. Actions Settings window will be opened, as shown in Figure 5-49.

**Note:** The Figure 5-49 shows the Actions Settings window, after we have pressed the **More Options**. This allow us to deal with multiple data items and be able specify where to run the command.



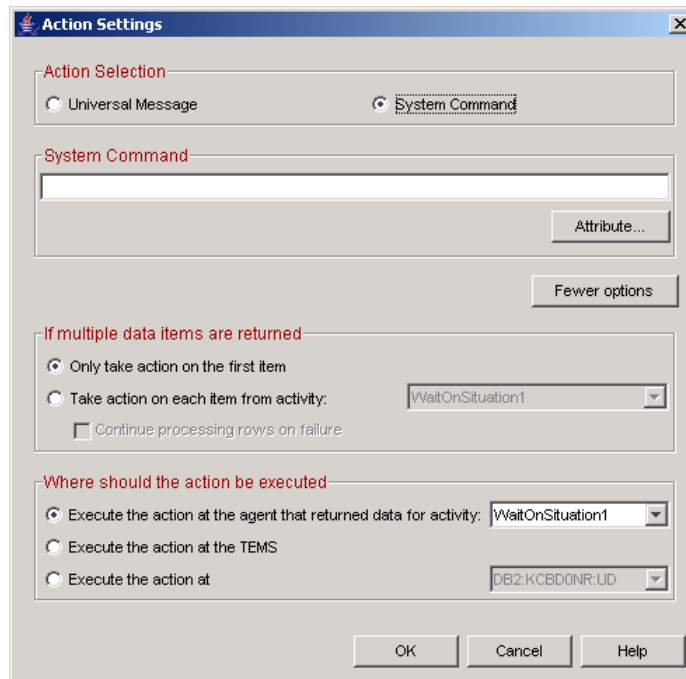


Figure 5-49 Actions Settings

12. In the System Command type write.exe, select **Execute the action at the TEMS** and click **OK**.
13. Now we are going to connect the workflow components. In the Workflow components, click the **+ connector1**. Now, click over the **Wait until Notepad is true** (notice the workflow component turns to red) and click on the **Wait until MSPaint is True**. In the Select a link condition window, select **Situation is True** and click **OK**.
14. Connect the **Wait until MSPaint is true** to **Take action: write.exe**. Click **Apply** button to put the policy in place as shown in Figure 5-50 on page 282.

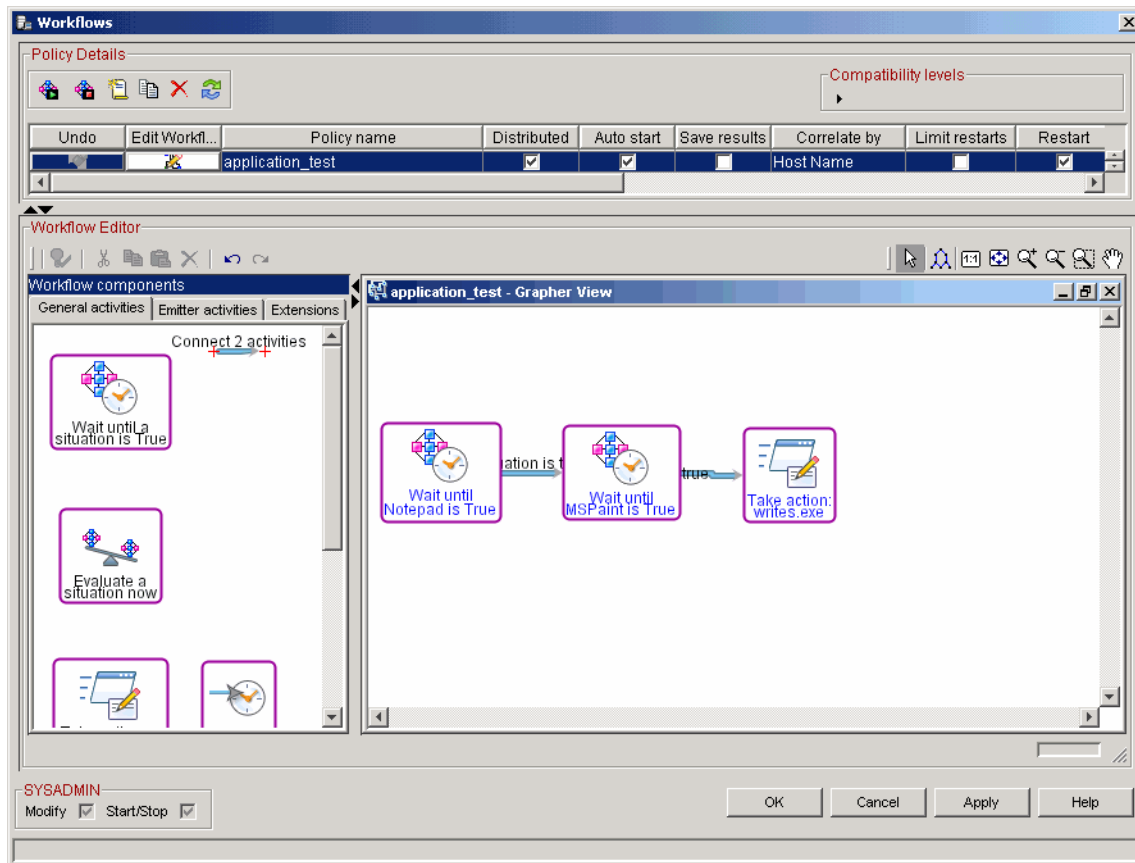


Figure 5-50 application\_test

15. Click **OK** to close Workflow Editor.

In order to test the policy we need close Notepad and mspaint programs. After a while we can see the write.exe program starting.

## 5.3 Working with Tivoli Data Warehouse

With Tivoli Data Warehouse, we can analyze historical trends from monitoring agents. The Tivoli Data Warehouse uses a DB2, Oracle, or Microsoft® SQL Server database to store historical data collected across the environment. We can generate warehouse reports for short term and long term data through the Tivoli Enterprise Portal. We can also use third-party warehouse reporting software, such as Crystal Reports or Brio, to generate long term data reports.

Warehouse reports provide information about the availability and performance of monitoring environment over a period of time. The Tivoli Data Warehouse uses the Warehouse Proxy agent to move data from monitoring agents or the monitoring server to the data warehouse database. The Warehouse Proxy is an ODBC export server for warehousing historical data. It is a special agent that uses an ODBC connection to transfer historical data collected from agents to a database. We can then analyze this data using the workspaces in the Tivoli Enterprise Portal or any third-party software.


The Warehouse Summarization and Pruning agent provides the ability to customize the length of time for which to save data (pruning) and how often to compress data (summarization).

## Configuring the Tivoli Data Warehouse

In “Section 3.2.1, “Installing IBM Tivoli Monitoring, V6.1” on page 71”, we installed and configured the Warehouse Summarization and Pruning agent and Warehouse Proxy agent. In this topic, we will work with the Tivoli Data Warehouse.

### *Historical Collection*

We can use the Historical Collection component to configure which groups collect data and how the data is collected, summarized and pruned.

1. Launch the Tivoli Enterprise Portal desktop client.
2. In Navigator, select **KCBD0NR**, this opens the workspace that we have been working.
3. In Tool Bar click in  **Historical Configuration....**
4. In Select a product select Windows OS, as shown in Figure 5-51.

**History Collection Configuration**

Select a product:  
Windows OS

Select Attribute Groups

Group	Collection	Collection Interval	Collection Location	Warehouse Interval	Summarize Yearly	Prune Yearly	Summarize Quarterly	Prune Quarterly	Summarize Monthly	Prune Monthly	Summarize Weekly
Active_Server_Pages											
DHCP_Server											
DNS_Dynamic_Update											
DNS_Memory											
DNS_Query											
DNS_WINS											
DNS_Zone_Transfer											
FTP_Server_Statistics											
FTP_Service											
Gopher_Service											
HTTP_Content_Index											
HTTP_Service											
ICMP_Statistics											
IS_Statistics											
Indexing_Service											

**Configuration Controls**

**Collection Interval**

☐ 5 minutes  
☒ 15 minutes  
☐ 30 minutes  
☐ 1 hour

**Collection Location**

☒ TEMA  
☐ TEMS

**Warehouse Interval**

☐ 1 hour  
☒ 1 day  
☐ Off

**Summarization**

☐ Yearly  
☐ Quarterly  
☐ Monthly  
☐ Weekly  
☐ Daily  
☐ Hourly

**Pruning**

☐ Yearly keep  Years  
☐ Quarterly keep  Years  
☐ Monthly keep  Months  
☐ Weekly keep  Months  
☐ Daily keep  Days  
☐ Hourly keep  Days  
☐ Detailed data keep  Days

Configure Groups   Unconfigure Groups   Show Default Groups   Start Collection   Stop Collection   Refresh Status

Close   Help

Figure 5-51 Historical Collection Configuration

- Click twice on the header of **Collection**. You will notice that we are already collecting data for some groups as shown in Figure 5-52.

Select Attribute Groups																	
Group	Collection	Collection Interval	Collection Location	Warehouse Interval	Summarize Yearly	Prune Yearly	Summarize Quarterly	Prune Quarterly	Summarize Monthly	Prune Monthly	Summarize Weekly	Prune Weekly	Summarize Daily	Prune Daily	Summarize Hourly	Prune Hourly	Prune Detailed
Network_Interface	Started	5 minutes	TEMA	1 hour	On	3 Years	On	3 Years	On	3 Years	On	2 Years	On	1 Years	On	3 Months	7 Days
NT_Processor	Started	5 minutes	TEMA	1 hour	On	3 Years	On	3 Years	On	3 Years	On	2 Years	On	1 Years	On	3 Months	7 Days
NT_Logical_Disk	Started	5 minutes	TEMA	1 hour	On	3 Years	On	3 Years	On	3 Years	On	2 Years	On	1 Years	On	3 Months	7 Days
NT_Memory	Started	5 minutes	TEMA	1 hour	On	3 Years	On	3 Years	On	3 Years	On	2 Years	On	1 Years	On	3 Months	7 Days
NT_Physical_Disk	Started	5 minutes	TEMA	1 hour	On	3 Years	On	3 Years	On	3 Years	On	2 Years	On	1 Years	On	3 Months	7 Days
NT_Server	Started	5 minutes	TEMA	1 hour	On	3 Years	On	3 Years	On	3 Years	On	2 Years	On	1 Years	On	3 Months	7 Days
NT_System	Started	5 minutes	TEMA	1 hour	On	3 Years	On	3 Years	On	3 Years	On	2 Years	On	1 Years	On	3 Months	7 Days
Active_Server_Pages																	
DHCP_Server																	
DNS_Dynamic_Update																	
DNS_Memory																	
DNS_Query																	
DNS_WINS																	
DNS_Zone_Transfer																	
FTP_Server_Statistics																	
FTP_Service																	

Figure 5-52 Groups collecting data

This list shows the attribute groups for the selected product for which historical data collection can be configured. Not all groups support the historical data collection. If you select one group, the configuration controls in the window change to reflect the settings for that group. If you select multiple groups, the controls do not change. Each entry shows the following:

- Group

The name of the group or table for which historical data will be collected.
- Collection

The status of whether data collection is started or stopped. If the value of this field is Started, click the entry to display a list of the monitoring servers where collection is started.
- Interval

The collection interval currently specified for the group, or Off.
- Location

The collection location currently specified for the group.
- Warehouse Interval

The frequency at which historical data is rolled off to the data warehouse. Set to Off, if you do not want data warehousing. The summarization and pruning configuration is disabled.
- Summarize Yearly

If you selected yearly summarization, the value is On.
- Prune Yearly

If you selected yearly pruning, the time periods that are specified for the group. The time interval is numerical, 1-99999. For example, if you want to keep 2 years of data, you would enter a 2 in the interval field and choose Years as the unit.
- Summarize Quarterly

If you selected quarterly summarization, the value is On.
- Prune Quarterly

If you selected quarterly pruning, the time periods that are specified for the group. The time interval is numerical, 1-99999. For example, if you want to keep 2 years of

quarterly data, you would enter a 2 in the interval field and choose Years as the unit.

- Summarize Monthly** If you selected monthly summarization, the value is On.
- Prune Monthly** If you selected monthly pruning, the time periods that are specified for the group. The time interval is numerical, 1-99999. For example, if you want to keep 2 months of data, you would enter a 2 in the interval field and choose Months as the unit.
- Summarize Weekly** If you selected weekly summarization, the value is On.
- Prune Weekly** If you selected weekly pruning, the time periods that are specified for the group. The time interval is numerical, 1-99999. For example, if you want to keep 2 weeks of data, you would enter a 2 in the interval field and choose Weeks as the unit.
- Summarize Daily** If you selected daily summarization, the value is On.
- Prune Daily** If you selected daily pruning, the time periods that are specified for the group. The time interval is numerical, 1-99999. For example, if you want to keep 2 days of data, you would enter a 2 in the interval field and choose Days as the unit.
- Summarize Hourly** If you selected hourly summarization, the value is On.
- Prune Hourly** If you selected hourly pruning, the time periods that are specified for the group. The time interval is numerical, 1-99999. For example, if you want to keep 2 hours of data, you would enter a 2 in the field and choose Hours as the unit.
- Prune Detailed** If you selected prune detailed, the time periods that are specified for the group.

Also we have the Configurations Controls, we can configure an attribute group(s), or groups if they should have the same control settings, then use these controls to adjust the settings for data collection and warehousing. For some of the sets of attribute groups, the configuration is hard coded by the product. These attribute groups will display a (fixed) in the Collection and Warehouse Interval cells of the Select Attribute Groups table.

- Collection Interval** Specifies the time between data collections.
- Collection Location** Determines whether data is collected at the TEMA (Tivoli Enterprise Monitoring Agent) or the TEMS (Tivoli Enterprise Monitoring Server). Collect data at the agent to minimize performance impact on the monitoring server

from historical data management. Once you have started data collection, you may lose data if you switch the Collection Location.

- Warehouse Interval** Indicates how often data should be rolled off to the warehouse. Set this to Off if you do not have a data warehouse.
- Summarization** Specifies the time period for data aggregation.
- Pruning** Specifies the time period to prune data.

**Note:** The controls show the default settings when you first open the window. As you select attribute groups from the list, the controls do not change for the selected group but remain static. If you change the settings for a group, those changes continue to display no matter which group you select while the window is open. This enables you to adjust the configuration controls once and apply the same settings to any number of attribute groups (one after the other, or use Ctrl+click to select multiples or Shift+click to select all groups from the first one selected to this point). The true configuration settings are shown in the group list above.

- Configure Groups** Adds the configuration controls you chose to the selected attribute group.
- Unconfigure Groups** Deletes the configuration controls from the selected attribute group.
- Show Default Groups** Selects the default groups in the product and scrolls the table to the first row.
- Start Collection** Starts historical data collection for the group or groups selected in the Select Attribute Group table. Collection will continue until the agent or monitoring server is stopped or recycled. Once you have added or changed the configuration controls, click this button to start the collection. If you have more than one Tivoli Enterprise Monitoring Server for an attribute group, when you click **Start Collection**, the Select TEMS window displays with a list of the local and remote servers from which you can select to start collection.

**Note:** If this is the first time you started historical data collection for an attribute group and the workspace includes views from that group, click **Refresh** after closing this window so you can see the Time Span tool for the view.

**Stop Collection**


Stops historical data collection for the group or groups selected in the Select Attribute Groups table. If you have more than one Tivoli Enterprise Monitoring Server for an attribute group, click on the **Collection** column in the Attribute Groups table. The Select TEMS window displays with a list of the servers so you can choose a server from which to stop collection. In order to change the configuration controls for a particular Attribute Group, you must first stop the collection with this button.

**Refresh Status**

Refreshes the view with the latest configuration settings. If you started data collection for several attribute groups, it might take a short time for the monitoring server to process the requests and report back to the console that data collection has started. Click **Refresh Status** again if history collection does not show as started for any of the groups you had chosen.

***Historical reporting***

Now that the data is already collected, we can display it using Tivoli Enterprise Portal.

1. Launch the Tivoli Enterprise Portal desktop client.
2. In Navigator select **KCB00NR**, this opens the workspace that we have been working.
3. In Disk Space, click in  **Specify Time Span for Query**.

**Note:** If we select any Attribute Group that have historical collections started, we can see the Specify Time Span for Query.

4. In Select the Time Span we have Real time Settings as default setting, so the real time is displayed in graph. To see the historical data select **Last** and specify **1 hour** for historical data, as shown in Figure 5-53 on page 289.



**Select the Time Span**

☐ Real time

☒ Last

**Last parameters**

☒ Use detailed data  
Time Column

☐ Use summarized data  
Shift   
Days

☐ Custom

**Custom parameters**

☐ Use detailed data  
Time Column

☒ Use summarized data  
Interval   
Shift   
Days

Start Time  End Time

☐ Apply to all views associated with this view's query

OK Cancel Help

Figure 5-53 Select the Time Span

5. Click **OK**. The graphic in Figure 5-54 reports the disk space each 5 minutes in the last 1 hour.

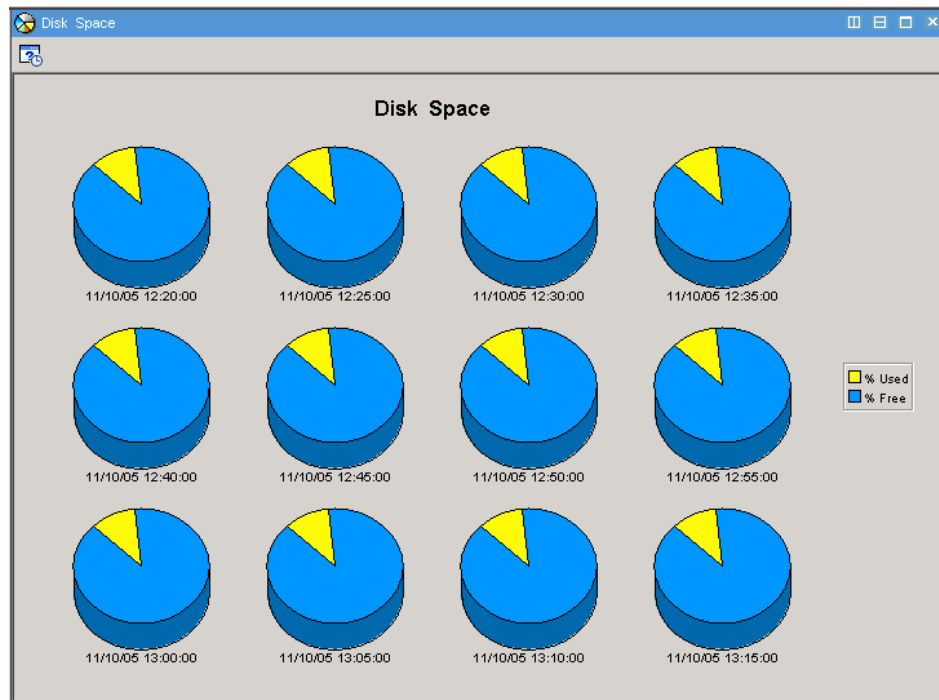


Figure 5-54 Disk Space Historical Data

# Related publications

The publications listed in this section are considered particularly suitable for a more detailed discussion of the topics covered in this redbook.

## IBM Redbooks

For information on ordering these publications, see “How to get IBM Redbooks” on page 292. Note that some of the documents referenced here may be available in softcopy only.

- ▶ *Getting started with IBM Tivoli Monitoring Version 6.1 on Distributed environments*, SG24-7143

## Other publications

These publications are also relevant as further information sources:

- ▶ *Introducing IBM Tivoli Monitoring, V6.1.0*, GI11-4071
- ▶ *IBM Tivoli Monitoring Version 6.1.0, User's Guide*, SC32-9409
- ▶ *IBM Tivoli Monitoring Version 6.1.0 ,Administrator's Guide*, SC32-9408
- ▶ *IBM Tivoli Monitoring, V6.1 Installation and Setup Guide*, GC32-9407

## Online resources

These Web sites and URLs are also relevant as further information sources:

- ▶ DB2 Fix Pack web site  
<http://www-306.ibm.com/software/data/db2/udb/support/downloadv8.html>
- ▶ Microsoft SQL server drivers web site  
<http://www.microsoft.com/sql/downloads/default.asp>
- ▶ Oracle ODBC drivers web site  
<http://www.oracle.com/technology/software/tech/windows/odbc/htdocs/utilsoft.html>
- ▶ IBM Java JRE web site  
<http://www-128.ibm.com/developerworks/java/jdk>

- IBM Tivoli Support web site

[ftp://ftp.software.ibm.com/software/tivoli\\_support/patches/](ftp://ftp.software.ibm.com/software/tivoli_support/patches/)

## How to get IBM Redbooks

You can search for, view, or download Redbooks, Redpapers, Hints and Tips, draft publications and Additional materials, as well as order hardcopy Redbooks or CD-ROMs, at this Web site:

[ibm.com/redbooks](http://ibm.com/redbooks)

## Help from IBM

IBM Support and downloads

[ibm.com/support](http://ibm.com/support)

IBM Global Services

[ibm.com/services](http://ibm.com/services)

# Index

## Symbols

\$DBDIR 117  
 \*IOSYSCFG 163  
 \*LOCAL 17  
 \*REMOTE 17  
 .NET 7

## A

agent bundles 55  
 Agent Configuration Toolkit 55  
 Agent Depot 54–55  
 agent upgradability 54  
 AIX 10  
 AIX R5.1 220  
 AIX R5.2 220  
 AIX R5.3 220  
 API 168  
 Application Agent 20  
 APPN report 169  
 Attribute Group 174

## B

Btrieve 128  
 bundle 54  
 business driving forces 2

## C

cache file 206–207  
     Maximum number 206  
 Candle Data Warehouse 7  
 CandleHome directory 114, 144, 147, 175, 228  
 CINFO Menu 149–150  
 Citrix 7  
 command line 115, 171  
 Common Information Model (CIM) 6  
 communication protocol 125, 142, 160, 222  
 compete effectively 2  
 config 135, 147, 150, 167, 177  
     file 210  
 Configuration file 135, 204  
 Configuring  
     Hot Standby 211

Hot Standby on a UNIX TEMS 212  
 Hub TEMS on a Windows server 117  
 Monitoring Agent for i5/OS 167  
 monitoring server to forward events 209  
 portal desktop client on Linux 177  
 Remote TEMS on a UNIX/Linux server 134  
 replacing a Hub TEMS server 225  
 Simple Object Access Protocol 198  
 Summarization and Pruning Agent 186  
 TEPS 135  
 UNIX TEMS based scenario 221  
 Warehouse Proxy 178  
 Warehouse Proxy agent 180  
 Windows TEMS based scenario 117  
 Corporate mergers 3  
 COUNT parameter 41  
 cron jobs 111

## D

data collection 168  
 data source 139, 184, 186  
 data warehouse 6–7, 13, 136, 141, 178–179, 185  
 DB2 database 136, 139, 179  
 default listening ports 40  
 Deployment Controller 56  
 Deployment Controller commands 55  
 deregulation 3  
 desktop client 110, 146, 174–176  
 Domain Name System (DNS) 111  
 driving forces 2

## E

encryption key 119, 131, 137, 145–146  
 Enterprise Information Base 17  
 Ephemeral pipe 44  
 error message 118, 131  
 ETL1 13  
 Event Server 135, 138, 196–197, 202  
     Event Synchronization 232  
 event server  
     port number 135, 210, 224  
     tec\_installdir/TME/TEC/.tec\_config file 210  
 event storms 2

Event synchronization 107, 110, 135, 143, 196, 224, 232  
 event update 210–211  
 existing rulebase 208–209  
     existing rule base 209  
 Exit CINFO 149–150

## F

file systems 111  
 firewall 125, 129, 133, 148, 159  
 firewall restrictions 45  
 Firewall with NAT 44

## G

graphical user interface (GUI) 110, 138, 171, 175, 202  
 GSKit 146, 219, 229

## H

host files 111  
 Host name 112, 115, 125–126, 134  
 HP-UX 11i 11  
 HTTP header 56  
 hub monitoring 125, 129, 133–134, 142, 175, 199, 211  
 hub monitoring server 125–126, 128–129, 133  
     Hot Standby 211  
     IP address 125–126  
     listening port 125  
     port number 142  
 hub standby 211  
 Hub TEMS 11–12, 17, 19, 29–30, 35, 107–108, 113, 115, 117, 119, 125  
     CANDLEHOME directory 228  
     environment 218, 228  
     installation 131, 209  
     name 224  
     server 225  
     Simple Object Access Protocol 197–198, 224  
     type 200

## I

i5/OS collection services 168  
 i5/OS computer 166  
 IBM Tivoli  
     account 114  
     Data Warehouse 13

Enterprise 6–7, 9  
 Enterprise Console 9  
     Monitoring 1, 3–4, 6–7  
     Monitoring component 9  
     Monitoring solution 4  
 IBM Tivoli Enterprise  
     Monitoring Server 197  
 IBM Tivoli Monitoring (ITM) 105–106, 110–112, 114  
 IBM Tivoli Monitoring, V6.1  
     Business driving forces 2  
     components 9  
     Differences with Distributed Monitoring 3.7 7  
     event storms 2  
     IBM Tivoli Data Warehouse 2.1 13  
     integration of Tivoli products 5  
     ITIL 9  
     modules 4  
         IBM Tivoli Monitoring for Applications 4  
         IBM Tivoli Monitoring for Business Integration 4  
         IBM Tivoli Monitoring for Databases 4  
         IBM Tivoli Monitoring for Messaging and Collaboration 4  
     solid foundation 4  
     solutions 3  
     TEMA 10  
     TEMS 11  
     TEP 12  
     TEPS 12  
     Tivoli Monitoring Services 9  
     uninstalling 228  
     value proposition 7  
     visualization of monitoring data 5  
 increase revenues 2  
 information delivery 3  
 installation medium 118, 131, 136, 138, 150, 174  
     setup.exe file 118, 131, 150  
 installation wizard 118, 131, 136, 143, 150  
     Event Synchronization 202  
 Installations with firewalls 43  
 Installing  
     Creating a deployment plan 112  
     Defining the architecture 112  
     Desktop client on a Linux machine 175  
     Event Synchronization 196  
     Expertise required 111  
     Hardware and software configuration 106  
     IBM Tivoli Monitoring, V6.1 components 110

- Installing TEMA on a Window Server 150
- Lab architecture of scenario-1 107
- Lab architecture scenario-2 108
- Microsoft Exchange Agent 173
- Remote TEMS 131
- Remote TEMS on a UNIX/Linux 134
- Remote TEMS on a Window 131
- Summarization and Pruning Agent 186
- TEMA on a Linux server 143
- TEMA on an OS/400 server 162
- Tivoli desktop client 174
- Tivoli Enterprise Monitoring Agent 143
- Tivoli Enterprise Portal Server 135
- Warehouse Proxy 178
- Internet Explorer 12
  - browser 12
  - Web browser 200
- intranet 3
- IOP-related data 168
- IP address 116, 125–126, 142, 144
- IP.PIPE protocol 39
- IP.UDP protocol 129
- IT Infrastructure Library 9
- itmcmd agent
  - start cj 178
  - start lz 149
  - stop pc 229
- itmcmd config 147, 150, 177, 213, 221

**J**

- Java Runtime Environment (JRE) 138, 144, 148, 150, 177
- JDBC driver 188

**K**

- KDC\_DEBUG 44
- KDC\_FAMILIES 44
- KDC\_PARTITION 43
- KDCB0\_HOSTNAME 42
- KDEB\_INTERFACELIST 43
- KMSPARM(KBBEV) 168

**L**

- language ID 2924 166
- less secure zone 45
- license agreement 118, 131, 136, 145–146
- Linux computer 114

- Linux system 196
- log file 116, 209–210
- LU name 126
- LU6.2 LOGMODE 126

**M**

- Managed Node 117
- managed system 10, 171, 173
- maximum number 205–206
- Microsoft SQL
  - Server website 189
- Microsoft SQL Server agent 173
- Microsoft Windows 2000 Server 111
- Microsoft Windows 2003 Server 111
- Microsoft Windows administrator 111
- Microsoft Windows XP 111
- migrate-export.bat facility 227
- monitoring agent 9–10, 143, 146–147, 150, 154
  - CCCINST library 165
  - i5/OS CCCINST library 165
  - network connections 167
  - previous versions 162
- monitoring server 16, 110, 112–113, 116, 118
  - communication protocol fields 134
  - communications protocol 125, 133
  - default host name 134
  - listening port 125–126
  - transaction program name 126
- monitoring solution 6, 10–11
- MS SQL 131, 136, 152, 178
  - Server 189
  - Server 2000 12

**N**

- NIS 115

**O**

- ODBC connection 46, 136
- OMEGAMON XE 7
- omegamon.rls 208
- operating system (OS) 107, 146–147, 150, 162
- OS agent 167, 170, 173
- OS/400 11

**P**

- plugins 13
- port number 113, 125–126, 134–135

portal server 110, 135–140, 142  
     host name 175  
 Primary Hub TEMS 125–126, 211, 214, 216  
 Primary TEMS 160, 215–216  
 product CD (PC) 165  
 product code 173, 224, 229  
     numbered list 229, 232  
 Protocol 1 125, 129, 133, 159, 213  
 Protocol 2 125, 129, 133, 148, 159

## Q

qopt object link 166

## R

RDBMS 111, 135–136, 179–180  
 Redbooks Web site 292  
     Contact us xx  
 reduce costs 2  
 remote deployment 120–121, 132, 218  
 remote monitoring server seed 128  
 remote RDBMS 18  
 Remote TEMS 134  
     application agent 172  
 Replacing a Hub TEMS server 225  
 reverse lookup 115  
 RHEL 11  
 RPC 55  
 RSTLICPGM LICPGM 166  
 rule base 197, 209  
     existing rule base 209

## S

SAVF 166  
 Secondary TEMS 148–149, 160, 214–215  
     HostName 148, 216  
     IP Port Number 149  
     IP.PIPE Port Number 149  
     protocol 148  
     Protocol 2 148  
 Secure Socket Layer (SSL) 219  
 seeding 224  
 setup.exe file 118, 131, 136, 150, 174  
 Simple Object Access Protocol (SOAP) 135, 197–198, 200  
 situation event 126, 135, 204, 209, 224  
 Situation update forwarder (SUF) 210  
 SKIP parameter 41

SLES 11  
 SLES 9 11–12  
 SOAP interface 198  
 Solaris 11  
 Solaris R10 220  
 Solaris R8 220  
 Solaris R9 220  
 SQL1 55  
 Summarization and Pruning Agent (SPA) 107, 186, 188, 190

## T

tacmd login 171, 173  
 TCP/IP Host Table 164  
 TEMAs 143, 225  
 TEMS Host  
     Name 148, 213, 222  
 TEMS server 106–108, 210, 225  
 TEP 12  
 TEP desktop  
     configuration 177  
 TEP Server  
     Hostname 177  
 thin-client 3  
 time zone 194  
 Tivoli Administrator 111  
 Tivoli Data Warehouse (TDW) 6–7, 13, 178, 189  
 Tivoli Enterprise  
     Management Agent 9  
     Management Server 11  
     Monitoring Server 9, 11–12  
     Portal 6, 9, 12–13  
     Portal Server 9, 12  
 Tivoli Enterprise Portal 9, 12, 17–18, 22, 27–28, 146, 174, 196  
     Server 12, 174, 196  
 Tivoli Enterprise Portal Server  
     function 12  
     Host 189  
     service 216  
     support 146  
     V610R172 146, 176  
 Tivoli environment 112  
     deployment plan 112  
 Tivoli Management Framework, V4.1.1 26  
 Tivoli Management Region (TMR) 117  
 Tivoli Monitoring Service 9, 128, 139, 161, 175, 198–199



Tivoli product 5, 7  
     Enhanced integration 7  
 Tivoli region 117  
 Tivoli server 117  
 Traditional Enterprise Management 2  
 transaction program (TP) 126

## U

UDP communication 39  
 UDP protocol 39  
 uninstallation 229–233  
 Uninstalling  
     component on UNIX 232  
     component on Windows 231  
     entire environment 228  
         on UNIX 229  
         on Windows 229  
     IBM Tivoli Enterprise Console Event Synchroni-  
         zation 232  
     IBM Tivoli Monitoring agent 231  
     IBM Tivoli Monitoring, V6.1 228  
     uninstall.sh command 232  
 Uninstalling IBM Tivoli Monitoring 228  
 Universal Agent (UA) 10, 146, 150, 173, 176, 221  
 UNIX administrator 111  
 UNIX server 106, 114, 225–227  
     DB2 database 179  
     following procedure 226  
     Hub TEMS 212, 218  
     IBM Tivoli account 114  
     itmcmd command 226–227  
 UNIX System 187  
 Use timezone offset 194  
 userid 139, 141, 172, 184, 189, 208

## V

value proposition 7  
 Virtualization 8

## W

Warehouse Proxy 110, 178–181  
     Agent 178–180, 183–184, 186, 212, 225–226  
     agent Hub TEMS 183  
     agent installation 179  
     configuration 184  
     confirmation window configuration 215  
     Data source configuration window 185

    installation 178–179  
     Reconfigure 180  
 Warehouse Proxy Agent 50  
 warehouse traffic 46  
 wbkupdb 117  
 Web Health 6  
 Web Services Description Language (WSDL) 198  
 Windows 2003 111, 118, 131, 179, 197  
 Windows 2003 Server 64 bit platform 11  
 Windows computer 118, 131, 136, 229, 231  
     IBM Tivoli Monitoring 229  
     remote monitoring server 131  
     Tivoli Enterprise Portal Server 136  
 Windows Management Instrumentation (WMI) 6  
 Windows XP 11–12, 111, 118, 131, 198  
 Windows XP Pro 11  
 Work with Object Links 166  
 wproxy database instance 173



To determine the spine width of a book, you divide the paper PPI into the number of pages in the book. An example is a 250 page book using Plainfield opaque 50# smooth which has a PPI of 526. Divided 250 by 526 which equals a spine width of .4752". In this case, you would use the .5" spine. Now select the Spine width for the book and hide the others: **Special>Conditional Text>Show/Hide>SpineSize(--->Hide:)>Set** . Move the changed Conditional text settings to all files in your book by opening the book file with the spine.frm still open and **File>Import>Formats** the Conditional Text Settings (ONLY!) to the book files.

**7188spine.frm    299**



# Deployment Guide Series: IBM Tivoli Monitoring V 6.1

(1.5" spine)  
1.5"<=> 1.998"  
789 <=> 1051 pages



# Deployment Guide Series: IBM Tivoli Monitoring V 6.1

(1.0" spine)  
0.875"<=> 1.498"  
460 <=> 788 pages



# Deployment Guide Series: IBM Tivoli Monitoring V 6.1

(0.5" spine)  
0.475"<=> 0.875"  
250 <=> 459 pages



# Deployment Guide Series: IBM Tivoli Monitoring V 6.1

(0.2" spine)  
0.17"<=> 0.473"  
90 <=> 249 pages

(0.1" spine)  
0.1"<=> 0.169"  
53 <=> 89 pages

To determine the spine width of a book, you divide the paper PPI into the number of pages in the book. An example is a 250 page book using Plainfield opaque 50# smooth which has a PPI of 526. Divided 250 by 526 which equals a spine width of .4752". In this case, you would use the .5" spine. Now select the Spine width for the book and hide the others: **Special>Conditional Text>Show/Hide>SpineSize(->Hide:)>Set** . Move the changed Conditional text settings to all files in your book by opening the book file with the spine.frm still open and **File>Import>Formats** the Conditional Text Settings (ONLY!) to the book files.

**7188spine.frm 300**



**Redbooks**

# Deployment Guide Series: IBM Tivoli Monitoring V 6.1

(2.5" spine)  
2.5"<->nnn.n"  
1315<-> nnn pages



**Redbooks**

# Deployment Guide Series: IBM Tivoli Monitoring V 6.1

(2.0" spine)  
2.0"<-> 2.498"  
1052 <-> 1314 pages





Draft Document for Review November 21, 2005 1:28 pm

# Deployment Guide Series: IBM Tivoli Monitoring V 6.1



**Step-by-step  
deployment guide for  
IBM Tivoli Monitoring  
V 6.1**

**Covers small to large  
environments**

**Discusses best  
practices for a  
deployment plan**

The IBM Tivoli Monitoring Version 6.1 solution is the next generation of the IBM Tivoli family of products that help monitor and manage critical hardware and software in distributed environments. IBM Tivoli Monitoring, V6.1 has been emerged from the best of the IBM Tivoli Monitoring V5 and OMEGAMON technologies. Integration of these great products, gives us a unique and comprehensive solution to monitor and manage both z/OS and distributed environments.

IBM Tivoli Monitoring, V6.1 is easily customizable and provides real-time and historical data which allows you to quickly diagnose and solve issues with the new GUI via the IBM Tivoli Enterprise Portal component. This common, flexible and easy-to-use browser interface helps users to quickly isolate and resolve potential performance problems.

This redbook focuses on the planning and deployment of IBM Tivoli Monitoring Version 6.1 in small to medium and large environments.

The target audience for this redbook is IT Specialists, who will be working on new IBM Tivoli Monitoring, V6.1 installations.

## **INTERNATIONAL TECHNICAL SUPPORT ORGANIZATION**

### **BUILDING TECHNICAL INFORMATION BASED ON PRACTICAL EXPERIENCE**

IBM Redbooks are developed by the IBM International Technical Support Organization. Experts from IBM, Customers and Partners from around the world create timely technical information based on realistic scenarios. Specific recommendations are provided to help you implement IT solutions more effectively in your environment.

**For more information:**  
[ibm.com/redbooks](http://ibm.com/redbooks)