Tivoli® IBM Tivoli Monitoring

Version 6.2.0

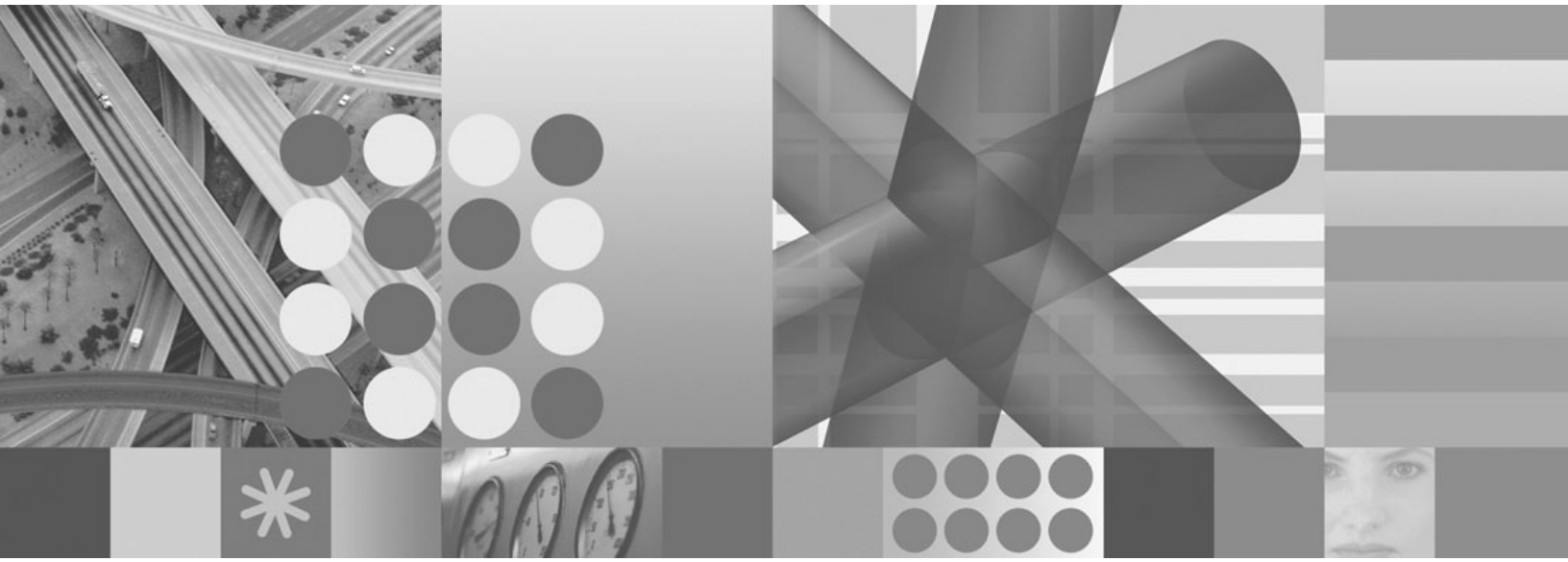


Installation and Setup Guide

GC32-9407-01

Tivoli® IBM Tivoli Monitoring

Version 6.2.0



Installation and Setup Guide

GC32-9407-01

Note
Before using this information and the product it supports, read the information in Appendix J, "Notices," on page 463.

This edition applies to version 6.2.0 of IBM Tivoli Monitoring (product number 5724-C04) and to all subsequent releases and modifications until otherwise indicated in new editions.

© Copyright International Business Machines Corporation 2005, 2007. All rights reserved.
US Government Users Restricted Rights – Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.

Contents

Figures xi

Tables xiii

Part 1. Planning your installation . . 1

Chapter 1. Overview of IBM Tivoli Monitoring 3

Components of the monitoring architecture 3
Tivoli Enterprise Monitoring Server. 5
Tivoli Enterprise Portal 5
Tivoli Enterprise Monitoring agents. 6
Tivoli Data Warehouse 7
Event synchronization component 7
New in this release 8
Changes to installation media. 9
Changes to runtime prerequisites and platform support. 10
Changes to the Tivoli Data Warehouse 10
Authentication Using LDAP 10
Help for the Tivoli Enterprise Portal presented by the IBM Eclipse Help Server 10
Event forwarding and synchronization for Tivoli Enterprise Console and Netcool/OMNIbus . . . 10
Support for /3GB boot option on 32-bit Windows 10
Common Event Console view for events from multiple event servers 11
Remote installation of application support files using Manage Tivoli Monitoring Services on Linux 11
Flexible scheduling of Summarization and Pruning agent 11
Validation of monitoring server protocols and standby configuration 11
Support for License Manager 11
Support for UNIX agents in Solaris local zones 11

Chapter 2. Planning your deployment 13

Overview of the design process. 13
Assessing the existing environment 14
Physical perspective 14
Network factors 15
Managed systems factors 15
Organizational perspective 15
Designing your deployment 16
Determining the number of monitoring servers needed 16
Determining server placement 18
Security considerations 18
Determining when to use the remote deployment feature 19
Planning considerations for the Tivoli Data Warehouse. 19
Estimating the required size of your database . . 19
Step 1: Determine the number of detailed records per day for the attribute group . . . 20
Step 2: Determine the hard disk drive footprint for the attribute group 20
Step 3: Determine the amount of detailed data for the attribute group. 20
Step 4: Calculate the amount of aggregate data for the attribute group. 21
Step 5: Determine the estimated size of your database 22
Understanding the disk requirements for your database 24
Increasing the size of your database (DB2 only) 25
Planning considerations for the Tivoli Enterprise Portal client 26
Sample deployment scenarios 27
Scenarios for small, medium, and large environments. 27
Small monitoring environment 27
Medium monitoring environment 29
Large monitoring environment: single hub installation 30
Large monitoring environment: multiple hub installation 32
High availability scenarios 34
Using Hot Standby 37
Hub monitoring servers 37
Remote monitoring servers 38
Monitoring agents 38
Portal server 38
Failover scenario 38
Using clustering 41
Clustering configurations 42
Setting up Tivoli Monitoring components in a clustered environment 45
What to expect from the Tivoli Management Services infrastructure in a clustered environment 49
Event integration scenarios 52
Event integration with Tivoli Enterprise Console. 52
One or more hub monitoring servers and a single event server 53
A single hub monitoring server and multiple event servers 54
Multiple hub monitoring servers and multiple event servers in a hub and spoke configuration 54
Event integration with Netcool/OMNIbus . . 55
One or more hub monitoring servers and a single event server 56
A single hub monitoring server and multiple event servers 57

Chapter 3. Preparing for installation . . 59

© Copyright IBM Corp. 2005, 2007

Overview of the installation process 59
Specific information to have ready. 59
Information to gather for event forwarding . . . 60
Naming your monitoring server 61
Required order of installation or upgrade of IBM Tivoli Monitoring component products 61
Windows installation considerations 61
User authority 61
Installation using a Citrix client. 61
Linux or UNIX installation considerations 62
Changes in the behavior of the autostart scripts 62
Create an IBM Tivoli account for installing and maintaining the installation directory 64
Host name for TCP/IP network services. 64
Use of fully qualified path names 64
Multiple network interface cards 64
Installing into an NFS environment 64
Installing into Solaris zones 65
Architecture and product codes. 66
Increasing virtual memory 66
File descriptor (maxfiles) limit 66
Understanding security options. 67
Securing communications between components 67
Global Security Tool Kit 68
Authorizing users to log in to the Tivoli Enterprise Portal. 68
User authentication using LDAP 69
Securing the SOAP server 70
Hardware and software requirements. 70
Supported operating systems 70
Supported databases for Tivoli Enterprise Portal Server and Tivoli Data Warehouse 77
Registering the DB2 product license key using the db2licm command 79
Required hardware for distributed systems . . . 80
Processor requirements 80
Memory and disk requirements. 81
Additional requirements 81
Required hardware for System z 82
Required software 82
Required software for event integration with Netcool/OMNIbus 83

Part 2. Installation and initial configuration of base components and agents 85

Chapter 4. Upgrading from a previous installation 87

Upgrade scenarios 87
Planning your upgrade 88
Platforms no longer supported for IBM Tivoli Monitoring V6.2 88
Prerequisites for IBM Tivoli Monitoring V6.2 . . 89
IBM Tivoli Monitoring V6.2 coexistence and interoperability 89
Determining what components to upgrade . . . 90
Required order of upgrade 91
Migrated information when upgrading from a previous version. 91
Backing up IBM Tivoli Monitoring. 92
Backing up a UNIX or Linux installation . . 92
Backing up a Windows installation 93
Backing up your portal server and Tivoli Data Warehouse databases 94
Backing up your portal server database . . . 94
Backing up your Tivoli Data Warehouse database 95
Upgrading the warehouse 95
Upgrading from IBM Tivoli Monitoring V6.1 . . . 96
Overview of the upgrade process 96
Required Java JRE 97
Upgrading from OMEGAMON Platform V350 and V360. 97
Overview of the upgrade process 98
Considerations 99
Terminology changes 99
When to run the upgrade. 99
Installation directory for upgraded components 99
Configuration settings for upgraded agents. . 99
Candle Management Workstation coexistence 100
Additional unsupported OMEGAMON functions 100
CandleNet Portal database 100
Required Java JRE. 100
Migrating data from an existing Warehouse Proxy database 101
Before you run the tool 101
Configuring the migration tool 101
Running the warehouse migration tool . . . 103
Status tables. 103
Using existing OMEGAMON and other monitoring agents with IBM Tivoli Monitoring . 103

Chapter 5. Installing IBM Tivoli Monitoring on one computer. 105

Prerequisites for the single computer installation 105
Installation procedure 106
Post-installation procedures. 111

Chapter 6. Installing IBM Tivoli Monitoring. 113

Installing and configuring the hub Tivoli Enterprise Monitoring Server 114
Windows: Installing the hub monitoring server 115
Linux or UNIX: Installing the hub monitoring server 119
Installing the monitoring server 119
Configuring the hub monitoring server. . . 120
Adding application support to the hub monitoring server 122
Command-line procedure 122
GUI procedure 122
Installing and configuring the remote monitoring servers 123
Windows: Installing a remote monitoring server 124

Linux or UNIX: Installing a remote monitoring server 127
Configuring the remote monitoring server 128
Installing the Tivoli Enterprise Portal Server . . . 129
Windows: Installing the portal server 130
Linux or AIX: Installing the portal server . . . 136
Installing the portal server on Linux or AIX 137
Configuring the portal server on Linux or AIX: command-line procedure. 139
Configuring the portal server on Linux or AIX: GUI procedure 143
Starting the portal server 148
Installing monitoring agents 148
Windows: Installing a monitoring agent . . . 149
Linux or UNIX: Installing a monitoring agent 152
Installing the monitoring agent 152
Configuring the monitoring agent 153
Changing the file permissions for agents . . 155
Starting the monitoring agents. 155
Installing the Tivoli Enterprise Portal desktop client 156
Windows: Installing the desktop client 156
Linux: Installing the desktop client 158
Linux: Configuring the desktop client . . . 159
Installing and enabling application support . . . 159
Selecting the correct support media 161
Configuring application support for agents on the Base DVD 164
Configuring application support for non-Base monitoring agents. 164
Installing application support on monitoring servers 165
Windows: Installing application support on a monitoring server 166
Linux or UNIX: Installing application support on a monitoring server 168
Installing application support on the Tivoli Enterprise Portal Server 170
Windows: Installing application support on a portal server 171
Linux or AIX: Installing application support on a portal server 172
Installing application support on the Tivoli Enterprise Portal desktop client 174
Windows: Installing application support on a desktop client 174
Linux: Installing application support on a desktop client 176
Configuring application support on non-local monitoring servers 177
Configuring application support on a non-local monitoring server from a Windows system 178
Copying the CAT and ATR files to the non-local monitoring server 178
Adding application support (SQL files) to a non-local hub. 178
Configuring application support on a non-local monitoring server from a Linux or UNIX system 179
Copying the CAT and ATR files to the non-local monitoring server 180
Adding application support (SQL files) to a non-local hub. 181
Installing application support files on a computer with no monitoring server . . 182
Installing language packs 183
Configuring the browser client 185
Specifying the browser used for online help . . . 185
Windows: Specifying the browser location. . . 186
UNIX and Linux: Specifying the browser location 186
Web Start: Specifying the browser location . . 187
Starting the Tivoli Enterprise Portal client 188
Starting the desktop client 188
Starting the browser client 189
Using Web Start to download and run the desktop client 189
Installing the IBM JRE 189
Windows: Installing the IBM JRE. 189
Linux: Installing the IBM JRE 190
Enabling tracing for the JRE 191
Downloading and running the desktop client 191
Manually creating a shortcut for the Web Start client 193

Chapter 7. Deploying monitoring agents across your environment . . . 195
Populating your agent depot 195
Populating the agent depot from the installation image 196
Windows: Populating the agent depot during installation 196
Base IBM Tivoli Monitoring installation image 196
Application agent installation image. . . 197
Linux and UNIX: Populating the agent depot during installation. 197
Populating the agent depot with the tacmd addBundles command 198
Managing your agent depot 199
Sharing an agent depot across your environment 199
Deploying OS agents. 200
Requirements for the tacmd createNode command 201
Using the tacmd createNode command. . . . 202
Deploying non-OS agents 202
Deploying through the portal 203
Deploying through the command line 203
Deploying a Universal Agent 203

Part 3. Post-installation configuration and customization . 205

Chapter 8. Configuring IBM Tivoli Monitoring components 207
Starting Manage Tivoli Monitoring Services . . . 207
Starting Manage Tivoli Monitoring Services on Windows computers 207
Starting Manage Tivoli Monitoring Services on Linux or UNIX computers 208

Changing the configuration of the Tivoli Enterprise Monitoring Server 208
Configuring or changing the monitoring server connection for agents 209
Starting and stopping components 210
Configuring user authentication 211
Windows: Configuring user authentication . . 212
Linux or UNIX: Configuring user authentication 215
Running ldapsearch with LDAP configuration 219
ldapsearch command-line options 219
Sample **ldapsearch** command (no SSL) . . . 220
Sample **ldapsearch** command (with SSL) . . 220
Configuring failover support 221
Configuring the Hot Standby feature for hub monitoring servers 221
Windows: Configuring the Hot Standby feature for hub monitoring servers 222
Configuring the Primary Hub 222
Configuring the Secondary Hub 223
Linux or UNIX: Configuring the Hot Standby feature for hub monitoring servers 224
Configuring the Primary Hub 224
Configuring the Secondary Hub 225
Configuring the Hot Standby feature for remote monitoring servers 225
Windows: Configuring the Hot Standby feature for remote monitoring servers . . . 225
Linux or UNIX: Configuring the Hot Standby feature for remote monitoring servers . . . 226
Configuring the Hot Standby feature for monitoring agents 227
Verifying that failover support is working . . . 227
Specifying network interfaces 228
Controlling port number assignments 228
Configuring port number assignments for the monitoring server 228
Configuring port number assignments for the portal server. 228
Changing the port number for browser client connections to the portal server 229
Changing the port number for desktop client connections to the portal server 229
Configuring port number assignments for monitoring agents 230
Example 231
Adding the KDE_TRANSPORT environment variable 231
Configuring the heartbeat interval 232

Chapter 9. Additional Linux and UNIX configuration 235
Disabling fsync() calls 235
Configuring permissions for a monitoring server on a non-NIS Solaris 235
Increasing virtual memory on AIX for large environments 235

Chapter 10. Additional Tivoli Enterprise Portal configuration 239
Using SSL between the portal server and the client 239
Enabling and disabling SSL for the Tivoli Enterprise Portal Server 240
Setting up asymmetric encryption 240
Creating a new key database 241
Creating a new public-private key pair and certificate request 241
Using a temporary self-signed certificate . . 242
Receiving the CA-signed certificate 242
Save the password to a stash file 243
Disabling SSL 243
Configuring an external Web server to work with Tivoli Enterprise Portal 243
Configuring Internet Information Server V5.0 243
Configuring Internet Information Server V6.0 244
Configuring IBM HTTP Server on Linux . . . 245
Configuring a portal client connection to an external Web server 246
Browser client 246
Desktop client 246
Updating the IOR for Windows 246
Updating the IOR for Linux 246
Firewall network address translation (NAT) or multiple network interface cards 247
Defining a Tivoli Enterprise Portal Server interface on Windows 247
Defining a Tivoli Enterprise Portal Server interface on Linux or UNIX 248
Firewall scenarios for Tivoli Enterprise Portal . . 249

Chapter 11. Configuring IBM Tivoli Monitoring Web Services (SOAP Server) 255
Defining hubs 255
Windows: Defining hubs 255
UNIX and Linux: Defining hubs (GUI procedure) 256
UNIX and Linux: Defining hubs (CLI procedure) 257
Adding users 258
Windows: Adding users 259
UNIX or Linux: Adding users (GUI) 259
UNIX or Linux: Adding users (CLI) 260
Verifying the configuration 260

Part 4. Setting up data warehousing 263

Chapter 12. Tivoli Data Warehouse solutions 265
New in V6.2. 265
Planning assumptions 266
Preliminary planning is complete. 266
This is not a single computer installation . . . 266
The data warehouse is remote from the portal server 266
Agent warehouse database upgrade 267
Firewall considerations for the Tivoli Data Warehouse 267
Next steps 267

Summary of supported operating systems 268

Chapter 13. Tivoli Data Warehouse solution using DB2 273

Supported components 273
Prerequisite installation 275
Implementing a Tivoli Data Warehouse solution using DB2 276
Assumptions 276
Solution steps 276
Step 1: Create the Tivoli Data Warehouse database 278
Creating the warehouse database on DB2 . . . 278
Creating a warehouse user on Windows . . . 279
Creating a warehouse user on Linux or UNIX 279
Limiting the authority of the warehouse user 280
Setting database and instance configuration values 282
Activating the DB2 listeners on a UNIX DB2 server 282
Step 2: Install and configure communications for the Warehouse Proxy agent. 283
Cataloging a remote data warehouse 284
Configuring an ODBC data source for a DB2 data warehouse 285
Before you begin 285
Procedure 286
Configuring a Warehouse Proxy agent on Windows (ODBC connection) 286
Configuring a Warehouse Proxy agent on Linux or AIX (JDBC connection) 288
Starting the Warehouse Proxy 290
Step 3: Configure communications between the Tivoli Enterprise Portal Server and the data warehouse 292
Configuring a Windows portal server (ODBC connection) 292
Before you begin 292
Procedure 292
Configuring a Linux or AIX portal server (DB2 CLI connection) 294
Starting the portal server 295
Step 4: Install and configure communications for the Summarization and Pruning agent 297

Chapter 14. Tivoli Data Warehouse solution using Microsoft SQL Server . 299

Supported components 299
Prerequisite installation 301
Implementing a Tivoli Data Warehouse solution using Microsoft SQL Server. 302
Assumptions 302
Solution steps 302
Step 1: Create the Tivoli Data Warehouse database 304
Step 2: Install and configure communications for the Warehouse Proxy agent. 305
Configuring an ODBC data source for a Microsoft SQL data warehouse 306
Configuring a Warehouse Proxy agent on Windows (ODBC connection) 307
Configuring a Warehouse Proxy agent on Linux or AIX (JDBC connection) 309
Starting the Warehouse Proxy agent 311
Step 3: Configure communications between the Tivoli Enterprise Portal Server and the data warehouse 312
Configuring the portal server (ODBC connection) 312
Step 4: Install and configure communications for the Summarization and Pruning agent 314

Chapter 15. Tivoli Data Warehouse solution using Oracle 315

Supported components 315
Prerequisite installation 317
Implementing a Tivoli Data Warehouse solution using Oracle. 318
Assumptions 318
Solution steps 318
Step 1: Create the Tivoli Data Warehouse database 320
Creating the warehouse database on Oracle . . 320
Step 2: Install and configure communications for the Warehouse Proxy agent. 322
Creating a TNS Service Name 323
Configuring an ODBC data source for an Oracle data warehouse 324
Configuring a Warehouse Proxy agent on Windows (ODBC connection) 325
Configuring a Warehouse Proxy agent on Linux or AIX (JDBC connection) 326
Starting the Warehouse Proxy 329
Step 3: Configure communications between the Tivoli Enterprise Portal Server and the data warehouse 330
Configuring a Windows portal server (ODBC connection) 330
Configuring a Linux or AIX portal server (JDBC connection) 331
Starting the portal server 333
Step 4: Install and configure communications for the Summarization and Pruning agent 334

Chapter 16. Tivoli Data Warehouse solutions: common procedures . . . 337

Configuring the Summarization and Pruning agent (JDBC connection) 337
Starting the Summarization and Pruning agent . . 347
Installing and configuring multiple Warehouse Proxy agents 347
Installing and configuring the proxy agents . . 348
Setting a permanent socket address for a proxy agent 350
Verifying the configuration 350
Testing the connection between the portal server and the Tivoli Data Warehouse 351
Tuning the performance of the Warehouse Proxy 354
Database initialization 354
Work queue 354
Connection pool 355
RPC threads and export requests 355

Timeout values 355
WAREHOUSELOG and WSAREHOUSEAGGRLOG tables 356

Part 5. Integrating event management systems 359

Chapter 17. Setting up event forwarding to Tivoli Enterprise Console 361
Installing event synchronization on your event server 362
Installing from a wizard 363
Installing from the command line 366
Installing from the command line using a silent installation 371
Manually importing the event synchronization class files and rule set 374
Creating a new rule base 375
Creating a new rule base and importing an existing rule base into it 375
Modifying an existing rule base 376
Installing monitoring agent .baroc files on the event server 377
Configuring your monitoring server to forward events 378
Starting and stopping the Situation Update Forwarder process 379
Changing the configuration of the event synchronization component on the event server . . 379
Defining additional monitoring servers to the event server 380
Changing the TCP/IP timeout setting on your event server 380
Upgrading to Tivoli Event Synchronization component version 2.0.0.0 381
Upgrading from a wizard 381
Upgrading from the command line 383
Upgrading from the command line using a silent installation 384

Chapter 18. Setting up event forwarding to Netcool/OMNIbus . . . 387
Installing the event synchronization component 388
Installing from a wizard 388
Installing from the command line 391
Installing from the command line using a silent installation 394
Configuring the Netcool/OMNIbus event server 397
Configuring the OMNIbus server for program execution from scripts 398
Updating the OMNIbus db schema 398
Configuring the EIF probe 400
Configuring error event flow to OMNIbus (optional) 402
Configuring the monitoring server 402
Customizing the OMNIbus configuration 403
Defining additional monitoring servers to the event server 403
Verifying installation and configuration. 404
Starting and stopping the situation update forwarder 405

Part 6. Appendixes 407

Appendix A. Installation worksheets 409
Windows hub monitoring server worksheet . . . 410
Linux or UNIX hub monitoring server installation worksheet 411
Windows remote monitoring server worksheet . . 412
Linux or UNIX remote monitoring server installation worksheet 413
Windows portal server worksheet 414
Linux portal server worksheet 415
Generic Windows monitoring agent worksheet . . 416
Generic Linux or UNIX monitoring agent worksheet 417
Windows portal desktop client worksheet 418
Linux portal desktop client worksheet 419
Monitoring server communications protocol details worksheet 420

Appendix B. Performing a silent installation of IBM Tivoli Monitoring . 421
Creating and using a Windows response file . . . 421
Running the silent installation from the command line with parameters 422
Using SMS 422
Performing a silent installation on a Linux or UNIX computer 423
Installing components with a response file . . 423
Configuring components with a response file 425

Appendix C. Firewalls 427
Determining which option to use. 427
Flow of connection establishment. 427
Permission at the firewall 427
Server address continuity 428
Number of internet zones 428
Basic (automatic) implementation. 429
Implementation with ephemeral pipe 429
Implementation with partition file 430
Sample scenarios 430
Scenario 1: Hub monitoring server INSIDE and monitoring agents OUTSIDE. 431
Scenario 2: Hub and remote monitoring servers INSIDE and monitoring agents OUTSIDE 431
Scenario 3: Hub monitoring server INSIDE, remote monitoring server and agents OUTSIDE 431
Creating or modifying the partition file in Manage Tivoli Monitoring Services 432
Windows: Editing the partition file 432
UNIX and Linux: Editing the partition file 433
Creating the partition file manually 433
Sample partition file 434
Implementation with firewall gateway 434

Appendix D. IBM Tivoli product codes 437

Appendix E. Maintaining the EIB on Linux or UNIX 439

Appendix F. Securing your Linux or UNIX IBM Tivoli Monitoring installation 441
Usage 441
Examples 442
Scenario with secureMain 442

Appendix G. Uninstalling IBM Tivoli Monitoring 443
Uninstalling the entire IBM Tivoli Monitoring environment. 443
Uninstalling the environment on Windows . . 443
Uninstalling the environment on Linux or UNIX 445
Uninstalling an individual IBM Tivoli Monitoring agent or component 446
Uninstalling a component on Windows. . . . 446
Uninstalling a component on Linux or UNIX 447
Uninstalling OMEGAMON agents 447
Removing an agent through the Tivoli Enterprise Portal 449
Uninstalling the Warehouse Proxy 449
Removing the ODBC data source connection 450
Uninstalling the event synchronization component 450
Uninstalling event synchronization manually . . . 451

Appendix H. Documentation library 455
IBM Tivoli Monitoring library 455
Documentation for the base agents 456
Related publications 457
Other sources of documentation 457

Appendix I. Support for problem solving 459
Using IBM Support Assistant 459
Obtaining fixes 459
Receiving weekly support updates 460
Contacting IBM Software Support 461
Determining the business impact 461
Describing problems and gathering information 462
Submitting problems 462

Appendix J. Notices 463
Trademarks 464

Index 467

Figures

1. IBM Tivoli Monitoring environment 4
2. Event synchronization overview 8
3. Small IBM Tivoli Monitoring environment 28
4. Medium IBM Tivoli Monitoring environment 29
5. Large deployment of IBM Tivoli Monitoring: single hub installation 31
6. Large deployment of IBM Tivoli Monitoring: multiple hub installation 32
7. IBM Tivoli Monitoring configuration with hot standby 37
8. Configuration after failover 40
9. Separate component clusters 43
10. Separate component clusters, with the Warehouse Proxy and Summarization and Pruning agents outside the data warehouse cluster 44
11. One cluster for the hub, portal server, and data warehouse 45
12. One or more hub monitoring servers connecting to a single event server 53
13. Single hub monitoring server and multiple event servers 54
14. Multiple hub monitoring servers and multiple event servers in a hub and spoke configuration 55
15. One or more hub monitoring servers connecting to a single event server 56
16. Single hub monitoring server and multiple event servers 57
17. Configuration window for the portal server database using DB2 107
18. Configuration window for the Tivoli Data Warehouse database using DB2 109
19. Configuration window for the Tivoli Data Warehouse database using Microsoft SQL Server 109
20. Tivoli Enterprise Monitoring Services window 111
21. Configuration window for the portal server database using DB2 133
22. Registering the portal server with the Tivoli Enterprise Monitoring Server 145
23. Configuring database connections for the portal server 146
24. IBM Tivoli Monitoring for Databases: application support packages 167
25. LDAP configuration window 213
26. Tivoli Enterprise Monitoring Server Configuration window: Primary Hub configuration 222
27. Specifying the Secondary Hub as a backup or standby server for the Primary Hub 223
28. Tivoli Enterprise Monitoring Server Configuration window: Secondary Hub configuration 224
29. Specifying the Primary Hub as a backup or standby server for the Secondary Hub . . . 224
30. Configuring Hot Standby for a remote monitoring server 226
31. Configuring a monitoring agent to connect to a standby hub monitoring server 227
32. Hierarchy for the heartbeat interval 233
33. Intranet with integral Web server 249
34. Intranet with external Web server 250
35. Intranet with integral Web server; Internet with external Web server. 251
36. Intranet and Internet with integral and external Web servers 252
37. Two host addresses, intranet and Internet, with integral and external Web servers . . . 253
38. Summary of support for the Tivoli Data Warehouse 268
39. Tivoli Data Warehouse solution using DB2 274
40. Configure DB2 Data Source for Warehouse Proxy window 287
41. Configure Warehouse Proxy window (TEMS Connection tab) 289
42. Configure Warehouse Proxy window (Agent Parameters tab) 289
43. Configure DB2 Data Source for Warehouse Proxy window 293
44. Configuring the connection to a DB2 data warehouse 295
45. Tivoli Data Warehouse solution using Microsoft SQL Server 300
46. Configure SQL Data Source for Warehouse Proxy window 308
47. Configure Warehouse Proxy window (TEMS Connection tab) 309
48. Configure Warehouse Proxy window (Agent Parameters tab) 310
49. Configure SQL Data Source for Warehouse Proxy window 313
50. Tivoli Data Warehouse solution using Oracle 316
51. Configure Oracle Data Source for Warehouse Proxy window 326
52. Configure Warehouse Proxy window (TEMS Connection tab) 327
53. Configure Warehouse Proxy window (Agent Parameters tab) 328
54. Configure Oracle Data Source for Warehouse Proxy window 331
55. Configuring the connection to an Oracle data warehouse 332
56. Sources tab of Configure Summarization and Pruning Agent window 340
57. Scheduling tab of Configure Summarization and Pruning Agent window 342
58. Work Days tab of Summarization and Pruning Agent configuration window . . . 343
59. Log Parameters tab of Summarization and Pruning Agent configuration window . . . 345

© Copyright IBM Corp. 2005, 2007

60. Additional Parameters tab of Summarization and Pruning Agent configuration window . . 346
61. Create Query window 352
62. Assigning the WAREHOUSELOG query to a workspace 353
63. Window shown when no Tivoli Enterprise Console event server is found. 363
64. Upgrade data collection window 382
65. Event flow and synchronization between Tivoli Monitoring and Netcool/OMNIbus . . 387
66. Uninstalling IBM Tivoli Monitoring 443
67. Confirming the uninstallation 444
68. Stopping Tivoli components prior to uninstallation 444
69. Removing the portal database 444
70. Database information 444
71. Uninstallation progress window 445
72. GSKit uninstallation 445
73. Successful uninstallation 445

Tables

1. IBM Tivoli Monitoring base monitoring agents 3
2. Planning a deployment of IBM Tivoli Monitoring 13
3. Overview of the design process 13
4. Description of four factors that affect the number and types of monitoring servers required in simple and complex environments . 16
5. Determining the number and type of monitoring servers based on the number of monitoring agents 17
6. Tivoli Data Warehouse database size estimation worksheet 23
7. Database size examples 24
8. Options for Tivoli Monitoring components resiliency 34
9. Resiliency characteristics of Tivoli Monitoring components and features 35
10. Basic steps to set up Tivoli Monitoring on a cluster 46
11. Control interface publishing 47
12. Installation and configuration steps 59
13. User security configuration method 69
14. Supported Windows operating systems 71
15. Supported UNIX, i5/OS, and z/OS operating systems 71
16. Supported Linux operating systems 74
17. Operating system requirements for IBM GSKit 77
18. Supported databases for the portal server 77
19. Supported databases for the Tivoli Data Warehouse 78
20. Estimated memory and disk storage for IBM Tivoli Monitoring components on distributed systems 81
21. Required software for IBM Tivoli Monitoring 82
22. Upgrading from IBM Tivoli Monitoring V6.1 to IBM Tivoli Monitoring V6.2 97
23. Upgrading from OMEGAMON Platform 350 or 360 98
24. OMEGAMON to IBM Tivoli Monitoring terminology 99
25. Unsupported OMEGAMON functions 100
26. KHDENV_MIG file variables for warehouse migration 102
27. Configuration information for the portal server database 107
28. Configuration information for the Tivoli Data Warehouse database 109
29. IBM Tivoli Monitoring high-level installation steps 114
30. Communications protocol settings for the hub monitoring server 117
31. Steps for installing a hub monitoring server on a Linux or UNIX computer 119
32. UNIX monitoring server protocols and values 121
33. Parameters for the itmcmd manage command 123
34. Remote monitoring server communications protocol settings 126
35. Steps for installing a remote monitoring server on a Linux or UNIX computer . . . 128
36. UNIX monitoring server protocols and values 128
37. Configuration information for the portal server database 133
38. Steps for installing a portal server on a Linux or AIX computer 137
39. Hub monitoring server protocols and values 140
40. Parameters for the itmcmd manage command 144
41. Configuration information for the Tivoli Enterprise Portal Server database 146
42. Communications protocol settings 151
43. Steps for installing a monitoring agent on Linux or UNIX 152
44. UNIX monitoring server protocols and values 154
45. Procedures for installing and enabling application support 161
46. Product support on the IBM Tivoli Monitoring V6.2.0 Base DVD 162
47. Product support on the Agent Support for Tivoli Enterprise Portal Server on AIX DVD . 163
48. Product support on the Agent Support for Tivoli Enterprise Monitoring Server on HP-UX on Itanium DVD 163
49. Product support on the Agent Support for Tivoli Enterprise Portal Server for DB2 9.1 DVD 163
50. Installation media and instructions for installing application support for non-Base monitoring agents 165
51. Locations of CAT and ATR files for the monitoring server 178
52. Locations of application support files on a Linux or UNIX monitoring server. 179
53. Locations of CAT and ATR files for the monitoring server 181
54. Language support included on IBM Tivoli Monitoring V6.2.0 Language Support DVD . 183
55. File locations for changing application properties for UNIX and Linux 186
56. Remote agent deployment tasks 195
57. Agent depot management commands 199
58. Configuration tasks available through Manage Tivoli Monitoring Services 207
59. Parameters for the itmcmd manage command 208
60. Communications protocol settings 208
61. Communications protocol settings 209
62. **ldapsearch** command line options and corresponding monitoring server configuration parameters 219
63. Using COUNT and SKIP variables to assign port numbers 231
64. Setting up asymmetric encryption. 240
65. Overview of SOAP Server configuration steps 255

© Copyright IBM Corp. 2005, 2007

66. TCP/IP Fields in Hub Specification dialog 256
67. SNA Fields in Hub Specification dialog 256
68. SOAP hub configuration values 258
69. SOAP methods associated with access privileges 258
70. Goals for creating a Tivoli Data Warehouse solution using DB2. 273
71. Information topics related to installation of prerequisite software for a Tivoli Data Warehouse solution 276
72. Tasks for creating the Tivoli Data Warehouse database 278
73. Default values for Tivoli Data Warehouse parameters 279
74. Script for creating required bufferpool and tablespaces for the Tivoli Data Warehouse . . 281
75. Tasks for installing and configuring communications for the Warehouse Proxy agent 283
76. Configuration information for the Tivoli Data Warehouse database on DB2 287
77. Tasks for configuring communications between the portal server and a DB2 data warehouse 292
78. Configuration information for the Tivoli Data Warehouse database on DB2 293
79. Configuration information for the Tivoli Data Warehouse database on DB2 295
80. Tasks for installing and configuring communications for the Summarization and Pruning agent 297
81. Goals for achieving a Tivoli Data Warehouse solution using Microsoft SQL Server 299
82. Information topics related to installation of prerequisite software for a Tivoli Data Warehouse solution 302
83. Default values for Tivoli Data Warehouse parameters 304
84. Tasks for installing and configuring communications for the Warehouse Proxy agent 305
85. Configuration information for the Tivoli Data Warehouse database on Microsoft SQL Server. 308
86. Tasks for configuring communications between the portal server and a Microsoft SQL Server data warehouse. 312
87. Configuration information for the Tivoli Data Warehouse database on Microsoft SQL Server. 313
88. Tasks for installing and configuring communications for the Summarization and Pruning agent 314
89. Goals for achieving a Tivoli Data Warehouse solution using Oracle 315
90. Information topics related to installation of prerequisite software for a Tivoli Data Warehouse solution 317
91. Tasks for creating the Tivoli Data Warehouse database 320
92. Default values for Tivoli Data Warehouse parameters 320
93. Tasks for installing and configuring communications for the Warehouse Proxy agent 322
94. Configuration information for the Tivoli Data Warehouse database on Oracle. 326
95. Tasks for configuring communications between the portal server and an Oracle data warehouse 330
96. Configuration information for the Tivoli Data Warehouse database on Oracle. 331
97. Configuration information for a Tivoli Data Warehouse database on Oracle. 332
98. Tasks for installing and configuring communications for the Summarization and Pruning agent 334
99. Where to obtain the JDBC driver files for the Summarization and Pruning agent 338
100. Tivoli Data Warehouse URLs 341
101. JDBC driver names 341
102. Tivoli Enterprise Console event synchronization installation and configuration steps 361
103. IBM Tivoli Enterprise Console event synchronization configuration fields 364
104. IBM Tivoli Enterprise Console event synchronization configuration fields, continued. 364
105. Options for rule base modification 365
106. IBM Tivoli Enterprise Console event synchronization configuration values . . . 372
107. Netcool/OMNIbus event synchronization configuration fields 389
108. Netcool/OMNIbus event synchronization configuration fields, continued. 390
109. Netcool/OMNIbus event synchronization configuration values 394
110. Mapping of situation attributes to OMNIbus attributes 400
111. Windows hub monitoring server installation worksheet. 410
112. Linux or UNIX hub monitoring server installation worksheet. 411
113. Windows remote monitoring server installation worksheet. 412
114. Linux or UNIX remote monitoring server installation worksheet. 413
115. Windows portal server worksheet. 414
116. Linux portal server worksheet 415
117. Generic Windows monitoring agent worksheet. 416
118. Generic monitoring agent for a Linux or UNIX computer worksheet 417
119. Windows portal desktop client worksheet 418
120. Linux portal desktop client worksheet 419
121. Monitoring server communications protocol details worksheet 420
122. Installation and configuration steps 421
123. Silent installation parameters for UNIX 424
124. Component product codes for infrastructure components and base monitoring agents . . 437
125. EIB Files 439

126. Candle OMEGAMON Release 04R1 448
127. Candle OMEGAMON Release BIV110 449

Part 1. Planning your installation

The chapters in this section describe the architecture of the IBM® Tivoli® Monitoring products and provide information to help you plan your deployment and prepare to install or upgrade the base components of the product. To minimize problems during deployment, you should read these chapters carefully.

Tivoli Monitoring products use a set of service components (known collectively as Tivoli Management Services) that are shared by a number of other product suites, including IBM Tivoli OMEGAMON® XE monitoring products, IBM Tivoli Composite Application Manager products, System Automation for z/OS®, Web Access for Information Management, and others. The information in this section is also relevant to these products.

Chapter 1, "Overview of IBM Tivoli Monitoring," on page 3, describes the base components of the product and new features for V6.2 that affect deployment, installation, or base configuration.

Chapter 2, "Planning your deployment," on page 13, contains information that assists you in assessing your environment and planning the deployment of product components. It also contains scenarios that illustrate deployments in small, medium, and large environments; deployments that provide high availability; and deployments that provide integration between events managed through Tivoli Management Services and those managed by Tivoli Enterprise Console® or Netcool/OMNIbus.

Chapter 3, "Preparing for installation," on page 59, helps you collect the information you will need during installation and configuration and details the hardware and software requirements for various components and configuration. It also addresses special considerations for the installation of the Tivoli Data Warehouse and Tivoli Enterprise™ Portal clients.

© Copyright IBM Corp. 2005, 2007

Chapter 1. Overview of IBM Tivoli Monitoring

IBM Tivoli Monitoring products monitor the performance and availability of distributed operating systems and applications. These products are based on a set of common service components, referred to collectively as Tivoli Management Services. Tivoli Management Services components provide security, data transfer and storage, notification mechanisms, user interface presentation, and communication services in an agent-server-client architecture (Figure 1 on page 4). These services are shared by a number of other products, including IBM Tivoli OMEGAMON XE mainframe monitoring products and IBM Tivoli Composite Application Manager products, as well as other IBM Tivoli Monitoring products such as Monitoring for Applications, Monitoring for Databases, Monitoring for Cluster Managers, and Monitoring for Messaging and Collaboration.

This book contains information on deploying, installing and configuring the common services components and the monitoring agents that comprise the base IBM Tivoli Monitoring product (Table 1) on distributed systems. If you purchased a product other than IBM Tivoli Monitoring that uses Tivoli Management Services, use this book to install and configure the common components. Do not install the base agents unless you have purchased IBM Tivoli Monitoring as a separate product. If you purchased additional IBM Tivoli Monitoring products, refer to their documentation for agent-specific installation and configuration information.

Table 1. IBM Tivoli Monitoring base monitoring agents

IBM Tivoli Monitoring 5.x Endpoint

Linux OS

UNIX Logs

UNIX OS

Windows OS

i5/OS

Universal Agent

IBM Tivoli Monitoring V6.2 products are enabled for use with IBM Tivoli License Manager. Tivoli Management Services components and Monitoring agents provide inventory signature files and usage definitions that allow License Manager to report installed products and product usage by computer. License Manager support is an optional capability that requires License Manager version 2.2 or later.

Components of the monitoring architecture

Tivoli Monitoring products, and other products that share Tivoli Management Services, participate in a server-client-agent architecture. Monitoring agents for various operating systems, subsystems, databases, and applications (known collectively as Tivoli Enterprise Monitoring Agents) collect data and send it to a Tivoli Enterprise Monitoring Server. Data is accessed from the monitoring server by Tivoli Enterprise Portal clients. A Tivoli Enterprise Portal server provides presentation and communication services for the clients. Several optional components such as an historical data warehouse extend the functionality of the framework. Figure 1 on page 4 shows the configuration of an IBM Tivoli Monitoring environment.

© Copyright IBM Corp. 2005, 2007

Before deciding where to deploy the components of the Tivoli Monitoring product in your environment, you should understand the components of the product, the roles that they play, and what affects the load on these components.

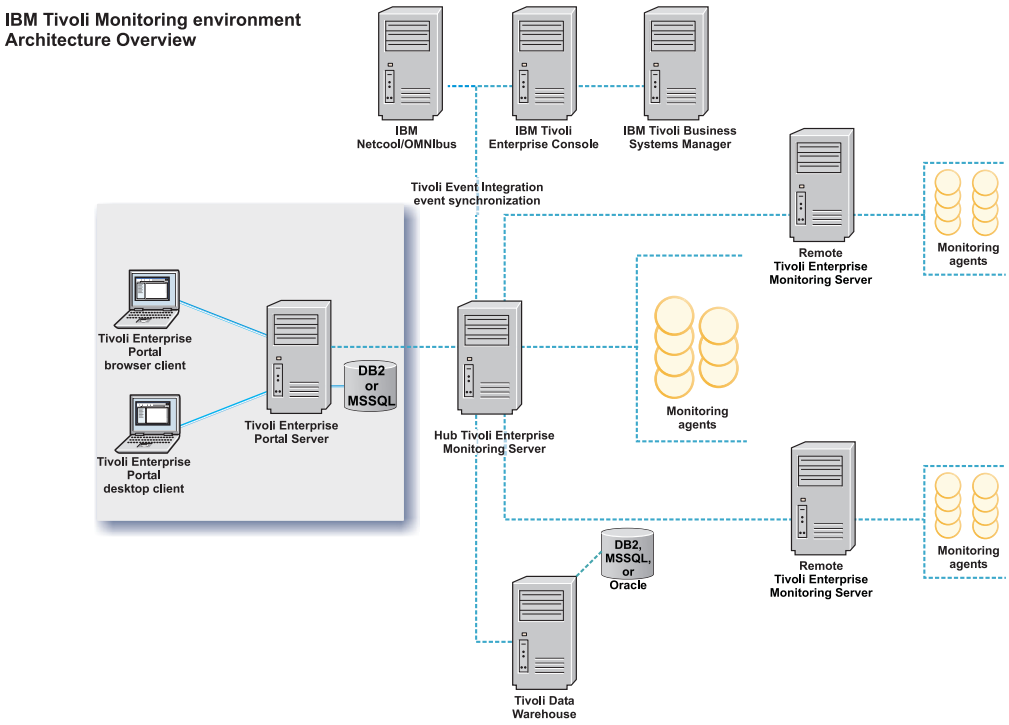


Figure 1. IBM Tivoli Monitoring environment

Every installation requires the following components:

- One or more Tivoli Enterprise Monitoring Servers, which act as a collection and control point for alerts received from the agents, and collect their performance and availability data. The monitoring server also manages the connection status of the agents. One server in each environment must be designated as the *hub*.
- A Tivoli Enterprise Portal Server, which provides the core presentation layer for retrieval, manipulation, analysis, and pre-formatting of data. The portal server retrieves data from the hub monitoring server in response to user actions at the portal client, and sends the data back to the portal client for presentation. The portal server also provides presentation information to the portal client so that it can render the user interface views suitably.
- One or more Tivoli Enterprise Portal clients, with a Java-based user interface for viewing and monitoring your enterprise. Tivoli Enterprise Portal offers two modes of operation: desktop and browser.
- Tivoli Enterprise Monitoring Agents, installed on the systems or subsystems you want to monitor. These agents collect data from monitored, or managed, systems and distribute it to a monitoring server.
- z/OS only: Tivoli Management Services:Engine (TMS:Engine) provides common functions, such as communications, multithreaded runtime services, diagnosis (dumps), and logging (RKLVLOG), for the Tivoli Enterprise Monitoring Server, monitoring agents, and OMEGAMON components of OMEGAMON XE products on z/OS.
- IBM Eclipse Help Server for presenting help for the portal and all monitoring agents for which support has been installed.

An installation optionally includes the following components:

- Tivoli Data Warehouse for storing historical data collected from agents in your environment. The data warehouse is located on a DB2, Oracle, or Microsoft SQL database. To store data in this database, you must install the Warehouse Proxy agent. To perform aggregation and pruning functions on the data, you must also install the Summarization and Pruning agent.
- Event synchronization component that sends updates to situation events that are forwarded to a Tivoli Enterprise Console event server or a Netcool/OMNIbus Netcool/Objectserver® back to the monitoring server.

The following sections describe each of these components in more detail.

Tivoli Enterprise Monitoring Server

The Tivoli Enterprise Monitoring Server (referred to as the *monitoring server*) is the first component to install to begin building the Tivoli Management Services foundation. The monitoring server is the key component on which all other architectural components directly depend.

The monitoring server is the collection and control point for performance and availability data and alerts received from monitoring agents. It is also responsible for tracking the online or offline status of monitoring agents.

Because of the number of functions the monitoring server performs, large-scale environments include a number of monitoring servers to distribute the load. One of the monitoring servers is designated the hub monitoring server, and the remaining servers are termed remote monitoring servers. Each remote monitoring server must be located on its own computer and have a unique monitoring server name (node), but the architectures of various remote monitoring servers might differ from each other and from the hub monitoring server. In other words, a remote monitoring server running on UNIX can report to a hub monitoring server running on Windows. The portal server communicates with the hub, which in turn controls the remote servers, as well as any monitoring agents that might be connected to it directly.

The monitoring server storage repository is a proprietary database format (referred to as the Enterprise Information Base, or EIB). The hub holds the master copy of the EIB, while the remote servers maintain a subset of the EIB relevant to them, which is synchronized with the hub.

Tivoli Enterprise Portal

Tivoli Enterprise Portal is the interface to your monitoring products. The Tivoli Enterprise Portal consists of the Tivoli Enterprise Portal Server and one or more clients.

The Tivoli Enterprise Portal Server (referred to as the *portal server*) manages data access through user workspace consoles (the clients). The portal server is configured to connect to a hub monitoring server. It retrieves data from the hub in response to user actions at a portal client, and sends the data back to the portal client for presentation. The portal server also provides presentation information to the portal client so that it can render the user interface views suitably.

The portal server uses a DB2 or Microsoft SQL database to store various artifacts related to presentation at the portal client.

The portal client provides access to the Tivoli Enterprise Portal. There are two kinds of portal client:

- Browser client interface (automatically installed with Tivoli Enterprise Portal Server): In your Internet browser, to start Tivoli Enterprise Portal browser client, you can enter the URL for a specific Tivoli Enterprise Portal browser client installed on your Web server. Running the browser client is supported only on Windows computers.
- Desktop client interface: A Java-based graphical user interface on a Windows or Linux workstation. After the desktop client is installed and configured, you can use it to start Tivoli Enterprise Portal in desktop mode. You can also download and run the desktop client using Java Web Start.

See "Planning considerations for the Tivoli Enterprise Portal client" on page 26 for a discussion of the comparative advantages of each type of portal client.

Tivoli Enterprise Monitoring agents

Monitoring agents are data collectors. Agents monitor systems, subsystems, or applications, collect data, and pass the data to Tivoli Enterprise Portal through the monitoring server. The agents pass commands from the user to the system, subsystem, or application. An agent interacts with a single system or application and, in most cases, is located on the same computer where the system or application is running.

There are two types of monitoring agents:

- Operating system (OS) agents that monitor the availability and performance of the computers in your monitoring environment. An example of an OS agent is the Monitoring Agent for Windows OS, which monitors Windows XP, Windows 2000, and Windows 2003 operating systems.
- Other agents (referred to as *application agents* or *non-OS agents*) that monitor the availability and performance of systems, subsystems, and applications. An example of a non-OS agent is IBM Tivoli Monitoring for Microsoft Exchange, which monitors the Microsoft Exchange Server.

IBM Tivoli Monitoring also provides a customizable agent called the Universal Agent. You can use the Universal Agent to monitor any data that you collect in your environment. For example, you can use the Universal Agent to monitor the status of your company Web site to ensure that it is available. For more information about the Universal Agent, see the *IBM Tivoli Monitoring Universal Agent User's Guide*.

Use the IBM Tivoli Monitoring Base product DVD to install the monitoring agents in the following list. This is the same DVD that you use to install the monitoring servers, portal server, and portal desktop clients.

IBM Tivoli Monitoring 5.x Endpoint

Windows OS

Linux OS

UNIX OS

UNIX Logs

Universal Agent

Warehouse Proxy

Summarization and Pruning

The Base DVD also includes application support for a small number of non-base distributed monitoring agents. See “Selecting the correct support media” on page 161 for more information.

Tivoli Data Warehouse

With Tivoli Data Warehouse, you 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 your environment. You can generate warehouse reports for short-term or long-term data through the Tivoli Enterprise Portal. Warehouse reports provide information about the availability and performance of your monitoring environment over a period of time. You can also use third-party warehouse reporting software, such as Crystal Reports or Brio, to generate reports.

Two specialized agents interact with the Tivoli Data Warehouse:

- The Warehouse Proxy agent receives data collected by monitoring agents and moves it to the Tivoli Data Warehouse database.
- The Summarization and Pruning agent provides the ability to customize the length of time for which to save data (pruning) and how often to aggregate granular data (summarization) in the Tivoli Data Warehouse database.

The Warehouse Proxy and the Summarization and Pruning agents, and support for those agents, are installed from the *IBM Tivoli Monitoring V6.2 Base DVD*.

Event synchronization component

The event synchronization component sends updates to situation events that are forwarded to a Tivoli Enterprise Console event server or a Netcool/OMNIbus Objectserver back to the monitoring server. Figure 2 on page 8 shows the flow of situation events from the monitoring server to the event server as Event Integration Facility (EIF) events and the flow of updates to the situation events back to the monitoring server. The Situation Event Console, the Common Event Console and the Tivoli Enterprise Console event views are synchronized with the updated status of the events.

If you are monitoring event data from a supported event management system in the Tivoli Enterprise Console event view or the Common Event Console view, you can filter out forwarded events. See the *IBM Tivoli Monitoring: Administrator's Guide*.

Note: Event forwarding is not supported from z/OS monitoring servers.

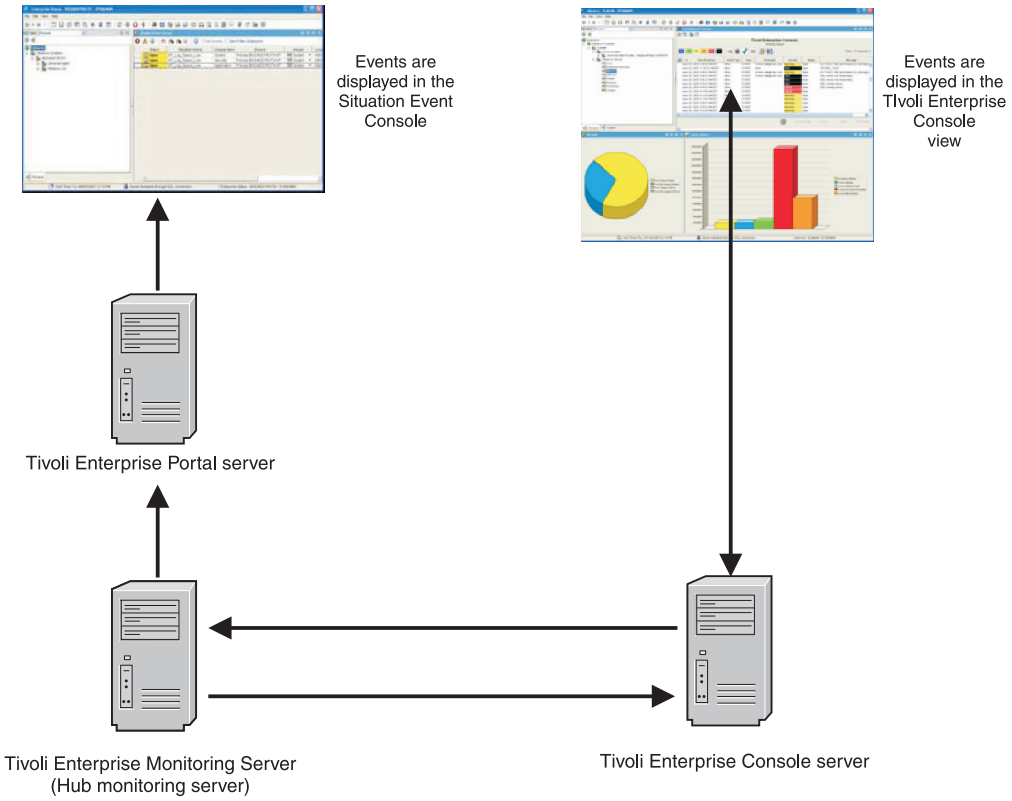


Figure 2. Event synchronization overview

For information about the various configurations of monitoring servers and event servers that you can have in your environment, see Part 5, "Integrating event management systems," on page 359.

New in this release

The following are changes in this release that affect installation or configuration. For complete list of new product features, see the *IBM Tivoli Monitoring: Administrator's Guide*.

Note: Some of these features were introduced in fix packs or as special solutions posted on the IBM Tivoli Open Process Automation Library Web site.

- "Changes to installation media" on page 9
- "Changes to runtime prerequisites and platform support" on page 10
- "Changes to the Tivoli Data Warehouse" on page 10
- "Authentication Using LDAP" on page 10
- "Help for the Tivoli Enterprise Portal presented by the IBM Eclipse Help Server" on page 10
- "Event forwarding and synchronization for Tivoli Enterprise Console and Netcool/OMNIbus" on page 10
- "Support for /3GB boot option on 32-bit Windows" on page 10
- "Common Event Console view for events from multiple event servers" on page 11
- "Remote installation of application support files using Manage Tivoli Monitoring Services on Linux" on page 11

- "Flexible scheduling of Summarization and Pruning agent" on page 11
- "Validation of monitoring server protocols and standby configuration" on page 11
- "Support for License Manager" on page 11
- "Support for UNIX agents in Solaris local zones" on page 11

Changes to installation media

IBM Tivoli Monitoring distributed components and base agents are now shipped on two DVDs:

- *IBM Tivoli Monitoring V6.2 Base DVD* (C60FMEN). This DVD contains the IBM Tivoli Monitoring base product components, the operating system agents for both Windows and UNIX, as well as application support for the operating system agents and a selected set of IBM Tivoli Monitoring 6.x based distributed monitoring agents.
- *IBM Tivoli Monitoring Tools DVD* (C60FNEN). This DVD contains the IBM Tivoli Monitoring 5.1.2 Migration Toolkit, the Distributed Monitoring Upgrade Toolkit, the Agent Builder and the Tivoli Event Integration event synchronization component.

Application support for additional V6.x-based distributed monitoring agents is provided on three DVDs:

- *IBM Tivoli Monitoring V6.2: Agent Support for Tivoli Enterprise Portal Server on AIX*
- *IBM Tivoli Monitoring V6.2: Agent Support for Tivoli Enterprise Management Server on HP-UX on Itanium*
- *IBM Tivoli Monitoring V6.2: Agent Support for Tivoli Enterprise Portal Server for DB2 9.1*

CDs are still available by request. See "Installing and enabling application support" on page 159 for information on the products for which support is available on the Base DVD and the three Agent Support DVDs. The **IBM Tivoli Monitoring V6.2.0 Quick Start CD** (C00YPML) contains a guide to help you get started with IBM Tivoli Monitoring.

Language support for the agents on the Base DVD is provided on the following DVDs:

- *IBM Tivoli Monitoring V6.2 Language Support 1 of 3* (C60FPML). This DVD contains the national language versions of the help and presentation files for the following languages: French, German, Italian, Portuguese Brazilian, Spanish.
- *IBM Tivoli Monitoring V6.2 Language Support 2 of 3* (C60FPML). This DVD contains the language support for the following languages: Japanese, Korean, Simplified Chinese, Traditional Chinese.
- *IBM Tivoli Monitoring V6.2 Language Support 3 of 3* (C60FPML). This DVD contains the language support for the following languages: Czech, Hungarian, Polish, Russian

Language support for the Tools DVD is provided on the following DVDs:

- *IBM Tivoli Monitoring V6.2 DM Upgrade Toolkit Language Support*
- *IBM Tivoli Monitoring V6.2 ITM 5.1.2 Migration Toolkit Language Support*
- *IBM Tivoli Monitoring V6.2 Agent Builder Toolkit Language Support*

Changes to runtime prerequisites and platform support

Runtime prerequisites have changed in several environments, especially AIX. Support for some platforms have been added and support for others have been dropped. Carefully review the information in "Hardware and software requirements" on page 70, especially the table footnotes, for V6.2 requirements and support.

Changes to the Tivoli Data Warehouse

For a list of changes to the Tivoli Data Warehouse, see "New in V6.2" on page 265. If you are upgrading from IBM Tivoli Monitoring V6.1, and you use the Tivoli Data Warehouse, you must migrate warehoused data. See "Upgrading the warehouse" on page 95.

Authentication Using LDAP

Support has been added to enable external authentication of Tivoli Enterprise Portal users with standards-based Lightweight Directory Access Protocol (LDAP) to shared registries. The hub monitoring server can now be configured to validate user IDs and passwords using either the local system registry or a central LDAP authentication and authorization system. This enhancement permits the sharing of user authentication information among products and prepares for future cross-product integration such as single sign-on. For more information, see "Understanding security options" on page 67 and "Configuring user authentication" on page 211.

Help for the Tivoli Enterprise Portal presented by the IBM Eclipse Help Server

The online Help for the Tivoli Enterprise Portal is now presented using the IBM Eclipse Help Server. The Help Server is installed with the Tivoli Enterprise Portal Server and can only be started and stopped by starting and stopping the portal server.

Event forwarding and synchronization for Tivoli Enterprise Console and Netcool/OMNIbus

You can now forward events generated by Tivoli Enterprise Portal based agents to both Tivoli Enterprise Console and Netcool/OMNIbus event servers. Event forwarding is implemented using the Tivoli Event Integration Event Facility (EIF). Reverse synchronization for forwarded events (changes at the event server returned to the originating monitoring server) is provided by an event synchronization component (SitUpdateForwarder). If you want to forward events to either Tivoli Enterprise Console or Netcool/OMNIbus, you must enable event forwarding on the hub Tivoli Enterprise Monitoring Server and configure a default target event server. For more information, see "Event integration scenarios" on page 52 and Part 5, "Integrating event management systems," on page 359.

Support for /3GB boot option on 32-bit Windows

Typically, Windows 32-bit supports only 2 GB of virtual memory. The /3GB boot option, available on Windows 2000 Advanced Server and later, allows you to allocate 3 GB of virtual memory. The Tivoli Enterprise Monitoring Server and the Tivoli Enterprise Portal Server now support this option. For more details on this option and supported Windows versions, see http://technet.microsoft.com/en-us/library/e834e9c7-708c-43bf-b877-e14ae443ecbf.aspx.

Common Event Console view for events from multiple event servers

The Common Event Console enables you to view and manage events from the Tivoli Enterprise Monitoring Server in the same way as the situation event console. In addition, however, it incorporates events from the Tivoli Enterprise Console Event Server and the Tivoli Netcool/OMNIbus Objectserver if your managed environment is configured for those servers.

Event data is retrieved from an event system by a common event connector, which also sends user-initiated actions to be run in that event system. To have the events from a specific event system displayed in the common event console, you must configure a connector for that event system. During configuration of the Tivoli Enterprise Portal Server you can edit the default connector for the Tivoli Enterprise Monitoring Server and you can configure additional connectors for other event systems.

Remote installation of application support files using Manage Tivoli Monitoring Services on Linux

In previous versions, the Manage Tivoli Monitoring Services utility on Windows can be used to FTP application catalog and attribute files to non-local monitoring servers. The utility can also be used to transfer the .sql files required for application support on a hub non-local to a non-local monitoring server. In V6.2, these functions have been extended to Linux.

Flexible scheduling of Summarization and Pruning agent

The Summarization and Pruning agent has been enhanced to allow for flexible scheduling and to have the warehouse and warehouse aggregation logs trimmed automatically after a specified number of days, months, or years.

Validation of monitoring server protocols and standby configuration

In previous versions, there was no validation of hub and remote monitoring server protocols and standby configuration. In V6.2, the installer validates configuration values such as the local host name of address, the port number, and the communications protocols for hub, remote, and standby monitoring servers. You may see warnings if you enter incorrect values during configuration.

Support for License Manager

IBM Tivoli Monitoring V6.2 products are enabled for use with IBM Tivoli License Manager. Base components and Monitoring agents provide inventory signature files and usage definitions that allow License Manager to report installed products and product usage by computer. License Manager support is an optional capability that requires License Manager version 2.2 or later.

Support for UNIX agents in Solaris local zones

On Solaris, the UNIX OS monitoring agent running in a local zone and remote deployment to a local zone are now supported. See “Installing into Solaris zones” on page 65 for more information.

Chapter 2. Planning your deployment

This chapter provides information about planning your deployment of IBM Tivoli Monitoring. Table 2 describes the planning topics and where to find them in this publication.

Table 2. Planning a deployment of IBM Tivoli Monitoring

Goal	Where to find information
Understand the steps required to design your environment.	"Overview of the design process"
Understand the needs of your existing environment so that you can identify the components of IBM Tivoli Monitoring that you need.	"Assessing the existing environment" on page 14
Design your environment based on planning guidelines, the components you need, and security considerations.	"Designing your deployment" on page 16
Understand the requirements for the Tivoli Data Warehouse	"Planning considerations for the Tivoli Data Warehouse" on page 19
Decide the type of Tivoli Enterprise Portal client to use	"Planning considerations for the Tivoli Enterprise Portal client" on page 26
Review sample environment configurations.	"Scenarios for small, medium, and large environments" on page 27 "High availability scenarios" on page 34 "Event integration scenarios" on page 52

Overview of the design process

To create a monitoring design, you must know how the existing environment is organized, as well as the current status of platforms, networks, applications, procedures, and processes. With this information, you must determine what kind of monitoring is needed, and what resources can be made available to IBM Tivoli Monitoring software to provide the solution.

Table 3 describes the design tasks and where to find them in this publication.

Table 3. Overview of the design process

Goal	Additional information (if applicable)
Perform an assessment of the existing environment, including what needs to be monitored.	"Assessing the existing environment" on page 14
Determine the number and type of monitoring servers required.	"Determining the number of monitoring servers needed" on page 16
Decide where to locate the monitoring servers and portal server.	"Determining server placement" on page 18

© Copyright IBM Corp. 2005, 2007

Table 3. Overview of the design process (continued)

Goal	Additional information (if applicable)
Determine how to deploy the monitoring agents.	"Determining when to use the remote deployment feature" on page 19 Chapter 7, "Deploying monitoring agents across your environment," on page 195
Decide on the number and placement of Warehouse Proxy agents and the Summarization and Pruning agent.	"Scenarios for small, medium, and large environments" on page 27
Determine how to configure the Tivoli Data Warehouse server.	"Planning considerations for the Tivoli Data Warehouse" on page 19
Review the explanation of how firewalls are implemented in IBM Tivoli Monitoring.	Appendix C, "Firewalls," on page 427

Assessing the existing environment

Before selecting and installing the IBM Tivoli Monitoring components, fully review and document the environment you plan to monitor. You can create an optimal design only after carefully considering the organizational needs and limitations (for example hardware availability) and understanding the technical capabilities of the IBM Tivoli Monitoring software.

Understanding the following conditions accelerates your design efforts and ensures that the solution performs as expected:

- A thorough and accurate picture of your networking environment.
- The business goals for system monitoring in your environment and how Tivoli applications can achieve those goals.

The number of factors that need to be considered and their influence on the architecture vary for each organization. Viewing these factors from both a physical and organizational perspective offers a way to arrange factors into manageable groups.

The physical perspective is the network physical topology, such as available equipment and configuration of systems, in which IBM Tivoli Monitoring must operate. The existing environment influences how and where you deploy systems. In many ways, the physical environment forms baseline constraints for the entire design. The relation between physical factors and IBM Tivoli Monitoring deployment is particularly close.

The organizational perspective includes expectations and limitations derived from the way you do business, and the division of authority and control of the systems to be managed. Organizational factors can influence the goals and means to deploy a monitoring solution.

The factors in the following sections, ordered by priority, are not a comprehensive list. Additional factors might be important in your environment.

Physical perspective

The following sections provide information about the physical perspective for a monitoring environment.

Network factors

Prepare a network diagram or sketch of the network topology, if one is not already available for your organization. This network design information is necessary for the design process and should at a minimum provide details about the following critical and important considerations:

- Line speed of each network connection. The line speed impacts the number of hub monitoring servers and the placement of remote monitoring servers and the Tivoli Data Warehouse.
- Firewalls and Network Address Translation (NAT) divisions in the network
- Bandwidth restrictions. Determine if there are bandwidth restrictions that must be honored to share limited bandwidth with other applications. Also, determine if the available network bandwidth varies by time of day.
- Number of resources to be monitored at remote locations
- Network reliability
- Host and IP address naming conventions and schemes used to identify networking and computer equipment

Managed systems factors

Prepare a list of computers and applications to be monitored by IBM Tivoli Monitoring. Include details about the following considerations:

- Hardware configuration of the computers to be monitored. Include the vendor, memory available, CPU speed, and disk space available.
- Software configuration of the computers to be monitored. Include the operating systems, patch levels, and network configuration.
- The applications on each computer that need to be monitored. Include version levels and patch levels.
- The number of each type of computer (operating system) and application.
- The maximum failure detection interval needed for each computer and application (for configuring heartbeat intervals).
- The computers and applications that are mission critical.
- A contingency plan for your mission critical applications.

Organizational perspective

Prepare a list of organizational factors that might have an impact on the deployment. Include details about the following considerations:

- Organizational objective, business processes, IT processes, business needs, and future plans. This aspect has a great impact in the design process and needs to be looked at carefully from a physical perspective.
- Amount of growth anticipated for the environment. The growth could be in terms of an increase in the number of monitored systems within existing infrastructure or due to setting up of new offices.
- Internationalization considerations.
- Primary risks to this project.
- Number and responsibilities of existing system administrators.
- Major impediments to the IT service your organization offers.
- Immediate problems you are trying to solve with the deployment of IBM Tivoli Monitoring.
- Your immediate and long-term goals.

Designing your deployment

There are several different installation and configuration scenarios for IBM Tivoli Monitoring. Depending on the hardware configuration and monitoring parameter settings, IBM Tivoli Monitoring can be scaled to support thousands of agents per hub monitoring server. Several hub monitoring servers can be deployed to expand monitoring capability to meet the needs of your environment.

However, as the size of your environment grows, so does the load of data to be processed, which can negatively impact performance. The following sections provide information to help you plan your environment, based on the number of agents and monitoring servers in your environment and the types of monitoring that you want to do.

Determining the number of monitoring servers needed

Identifying the types and number of monitoring servers that you need in your environment depends on a number of factors, including:

- The number and type of agents to support
- The geography of your environment
- The speed of network connections between the different Tivoli Monitoring components
- The processor and memory capacity of the servers running the Tivoli Monitoring components
- The number of situations deployed, and the frequency and complexity of the situation evaluation
- The volume and frequency of events generated from situation evaluation
- The number of workflow policies, and the frequency and complexity of the policy automation
- The number of Tivoli Enterprise Portal clients, and the frequency and complexity of the client interaction with the monitoring servers
- The amount of historical data being collected by the monitoring agents, and the volume and frequency of upload requests to the Warehouse Proxy agents.

Consider each of these factors on a spectrum, ranging from simple to complex. For example, the following table describes how four of the factors might appear on the simple and complex sides of the spectrum.

Table 4. Description of four factors that affect the number and types of monitoring servers required in simple and complex environments

Factor	Simple side of spectrum	Complex side of spectrum
Type of agents	Small number of agent types: for example, Windows, UNIX, and Linux OS agents	Large number of agent types, including OS, database, and application agents for distributed and z/OS platforms
Geography	Monitored systems located in close geographic proximity	Monitored systems located across dispersed geographic locations
Network connections	LAN speed	Mix of LAN and slower speeds (for example, WAN, T1)

Table 4. Description of four factors that affect the number and types of monitoring servers required in simple and complex environments (continued)

Factor	Simple side of spectrum	Complex side of spectrum
Server capacity	Server hardware at or exceeding the recommended requirements described in "Required hardware for distributed systems" on page 80 or "Required hardware for System z" on page 82	Some server hardware slower or smaller than the recommended requirements described in "Required hardware for distributed systems" on page 80 or "Required hardware for System z" on page 82

With these factors in mind, you can use the number of monitoring agents as a guideline to determining the number of monitoring servers for your environment:

- If most factors for your environment fall on the simple side of the spectrum, you can expect a single monitoring server to manage between 500 and 1500 monitoring agents.
- If several factors for your environment fall on the complex side of the spectrum, you can expect a single monitoring server to manage fewer than 500 monitoring agents.

While these guidelines might be useful for configuration planning, it is important to monitor the CPU and memory usage of the monitoring servers after the monitoring environment is operational. You can monitor these attributes using the appropriate OS monitoring agents and by building a separate managed system list for the monitoring servers.

The desired result is low, steady-state CPU utilization by the monitoring servers. A reasonable target is 10% to 20% CPU utilization of a single processor averaged over time. Low utilization enables the monitoring server to perform well for transient spikes in workload, such as situation distribution or server restart. If CPU utilization for a monitoring server is low most of the time, and if the performance of the transient spikes in workload are acceptable, consider increasing the number of agents managed by the monitoring server.

The following table shows how you might determine the number and type of monitoring servers based on the number of monitoring agents and the complexity of your environment:

Table 5. Determining the number and type of monitoring servers based on the number of monitoring agents

Number and type of monitoring servers	Number of agents (simple side of spectrum)	Number of agents (complex side of spectrum)
Hub monitoring server, no remote monitoring servers	< 500 agents	< 250 agents
Hub monitoring server, one remote monitoring server	< 1500 agents	< 500 agents
Additional remote monitoring servers	For each additional 500 to 1500 monitoring agents	For each additional 250 to 500 monitoring agents
Multiple hub monitoring environments	For environments greater than 5000 to 10000 agents	For environments greater than 1500 to 5000 agents

Notes::

1. The Tivoli Enterprise Monitoring Server can now access up to 3 GB of memory in the 32-bit Windows environment with the /3GB option enabled. This option is available on Windows 2000 Advanced Server and later.

   The default settings for 32-bit Windows operating system allows a maximum of 2 GB of memory per process. The /3GB switch allows a maximum of 3GB of virtual memory. The /3GB option must be set in the boot.ini file. For details on setting boot.ini parameters, more details on this option and supported Windows versions, see http://technet.microsoft.com/en-us/library/e834e9c7-708c-43bf-b877-e14ae443ecbf.aspx .
2. Remember that a single monitored system can include several agents such as an OS agent (Windows®, UNIX®, or Linux®) and an application agent like the DB2® agent. For this reason, be sure to count the number of agents to be supported, not the number of monitored systems.

Determining server placement

Consider the following when determining the needs of your monitoring environment:

- Decide where (within the existing network topology, or geographically) you want to accumulate data generated by the agents. This is where you will install a monitoring server.
- Determine the amount of data you expect to collect. Depending on the complexity of your environment, the number of agents you install and the amount of data you choose to collect, you might need multiple monitoring servers. (Note that IBM Tivoli Monitoring does not support multiple monitoring servers on the same computer.)
- Determine where you want to run the user interface to look at data and interact with the system. This is where you install the portal server and portal client.
- Determine your need for high availability operation in your environment. If you need high availability operation, consider using the Hot Standby feature to ensure the high availability of your hub monitoring server and configuring backup servers for your remote monitoring servers.

A final factor to consider in determining the deployment of monitoring servers is geography. You can divide your agents between monitoring servers based on their geographical location. For example, if you have agents in two locations separated by a wide area network (WAN), the agents closest physically to the monitoring server have the best performance. The speed of the network connection between components affects the performance of your environment. A slower connection increases the client response time. To increase performance across the environment, you can set up two remote monitoring servers on either side of the WAN connection to service the agents close to them.

Security considerations

Firewalls and NAT translation require additional configuration steps (see Chapter 3, “Preparing for installation,” on page 59). If an agent is across a firewall from its monitoring server or from the Warehouse Proxy agent, then extra configuration is needed so that they know how to address each other. This configuration can be a lot of work; for example, if you have 500 agents across a firewall, you might consider giving them their own monitoring server to avoid this.

For additional information about IBM Tivoli Monitoring's implementation of firewalls, including firewalls between portal server and monitoring server, see Appendix C, “Firewalls,” on page 427.

Determining when to use the remote deployment feature

IBM Tivoli Monitoring has the ability to deploy resource monitoring across your environment from a central location, the monitoring server. You can use the remote deployment feature of IBM Tivoli Monitoring to deploy and configure monitoring agents, to deploy maintenance and upgrades to agents, and to start and stop agents.

The remote deployment feature in IBM Tivoli Monitoring can be used in all monitoring environments; however, the number of agents you want to deploy and the deployment capabilities that you require affect whether the remote deployment feature is the best choice for your environment. Consider using an enterprise deployment tool, such as IBM Tivoli Configuration Manager, if you need any of the following capabilities:

- Efficiently deploying a large number of agents in parallel, using caches that are geographically close to the distribution points
- Limiting the amount of bandwidth used for deployment actions through the use of network bandwidth throttling
- Restarting a failed deployment automatically

Planning considerations for the Tivoli Data Warehouse

In a large or enterprise environment, you have the option of using multiple databases for the Tivoli Data Warehouse or having all of your hub monitoring servers use one single database. The benefit of using one database across your environment is that the information is stored in one location, meaning that you can more easily and accurately generate reports that reflect your entire environment (as opposed to needing to collate reports from several different databases). However, because the amount of data that is generated during history collection across a large or enterprise environment can be immense, you need to carefully plan the scale and performance of that database.

In addition to the planning information below, the IBM Redbook *Tivoli Management Services Warehouse and Reporting*, SG24-7290, provides database performance tuning information. You can download the book at the following location: http://www.redbooks.ibm.com/abstracts/sg247290.html?Open.

Estimating the required size of your database

One of the factors to consider when planning the size of database that you need is the amount and type of information you will collect for agent history data collection. Each of the agent user's guides provide capacity planning information to help you calculate the amount of disk space required by data for each attribute group. Use this information to complete the following calculations to determine how large your data warehouse database needs to be:

- “Step 1: Determine the number of detailed records per day for the attribute group” on page 20
- “Step 2: Determine the hard disk drive footprint for the attribute group” on page 20
- “Step 3: Determine the amount of detailed data for the attribute group” on page 20

- "Step 4: Calculate the amount of aggregate data for the attribute group" on page 21

You can use the planning spreadsheet available in the IBM Tivoli Monitoring information center.

You might prefer to use the Warehouse Load Projection tool available in the IBM Tivoli Open Process Automation Library. (Search on "Warehouse Load Projects at the following site: http://www.ibm.com/software/tivoli/opal. The tool does all the calculations for you and includes data for nearly all of the V6.x based monitoring agents.

Step 1: Determine the number of detailed records per day for the attribute group

Determine the number of detailed records per day for each attribute group that you want to collect data for. Use the following equation:

```
(60 / collection interval) * (24) * (# instances at each interval)
```

where:

60 Represents the 60 minutes in an hour.

collection interval
The data collection interval, in minutes. This value can be 1, 5, 15, 30, 60, or 1440 (1 day).

24 Represents 24 hours in one day.

instances at each interval
The number of instances recorded at each interval. See the agent user's guide for this value.

Step 2: Determine the hard disk drive footprint for the attribute group

Determine the hard disk drive footprint for each attribute group. The result generated by this formula gives an estimate of the amount of disk space used for this attribute group for 24 hours worth of data for a single agent.

Use the following equation:

```
(# detailed records) * (attribute group detailed record size) / 1024)
```

where:

detailed records
The number of detailed records for the attribute. This is the value you calculated in "Step 1: Determine the number of detailed records per day for the attribute group."

attribute group detailed record size
The detailed record size for the attribute group. See the agent user's guide for this value.

1024 Represents 1 KB and causes the equation to generate a kilobyte number instead of a byte number.

Step 3: Determine the amount of detailed data for the attribute group

Determine the amount of detailed data in the warehouse database for each attribute group. Use the following equation:

```
attribute group disk footprint * (# of agents) * (# days of detailed data) / 1024
```

where:

attribute group disk footprint
The disk footprint for the attribute group. This is the value you calculated in "Step 2: Determine the hard disk drive footprint for the attribute group" on page 20.

of agents
The number of agents of the same agent type in your environment.

days of detailed data
The number of days for which you want to keep detailed data in the warehouse database.

1024 Represents 1 KB and causes the equation to generate a megabyte number.

Step 4: Calculate the amount of aggregate data for the attribute group

Determine the amount of aggregate data in the warehouse for each attribute group.

First, calculate the number of aggregate records per agent. Use the following equation:

```
(#hourly + #daily + #weekly + #monthly + #quarterly + #yearly)
     * (# instances at each interval)
```

where:

#hourly
The number of hourly records for the attribute group. For example, if you have hourly records for 60 days, the number of hourly records is 1440 (60 multiplied by 24 hours per day).

#daily The number of daily records for the attribute group. For example, if you have daily records for 12 months, the number of daily records is 365.

#weekly
The number of weekly records for the attribute group. For example, if you have weekly records for a 2-year period, the number of weekly records is 104 (2 multiplied by 52 weeks per year).

#monthly
The number of monthly records for the attribute group. For example, if you have monthly records for a 2-year period, the number of monthly records is 24.

#quarterly
The number of quarterly records for the attribute group. For example, if you have quarterly records for a 2-year period, the number of quarterly records is 8 (2 years multiplied by 4 quarters in a year).

#yearly The number of yearly records for the attribute group. For example, if you have yearly reports for a 10-year period, the number of yearly records is 10.

instances at each interval
The number of instances recorded at each interval. See the agent user's guide for this value.

Next, use the following equation to calculate the amount of attribute data in the warehouse for the attribute group:

```
(# aggregate records per agent) * (attribute group aggregate record size)
     * (# agents) / 1048576
```

where:

aggregate records per agent
The number of aggregate records per agent for the attribute group.

attribute group aggregate record size
The size of the attribute group aggregate group. See the agent user's guide for this value.

agents
The number of agents of the same agent type in your environment.

1048576
Represents 1 MB and causes the equation to generate a megabyte number.

Step 5: Determine the estimated size of your database

First, determine the total space required for each attribute group. Add the amount of detailed data and the amount of aggregate data for the attribute group. Use the following equation:

```
(detailed data size) + (aggregate data size)
```

Second, determine the total space required for all attribute groups for the agent. Add the total space for each attribute group that you want to collect. Use the following equation:

```
aggGroup1 + aggGroup2 + aggGroup3 ...
```

Third, determine the total space required for all agents. Add the total space for each agent. Use the following equation:

```
agent1 + agent2 + agent3 ...
```

Finally, to estimate the total disk space requirement for the database, multiplying the total amount of data (detailed + aggregate for all attribute groups) by 1.5 (to increase the number by 50%). Compare this number to the **Database data** row in Table 7 on page 24 to determine the number of disks you need for your database.

Use the following worksheet to estimate the size of your data warehouse database.

Table 6. Tivoli Data Warehouse database size estimation worksheet

Attribute group	Number of agents	Data from the User's Guide			Collection interval	Detailed records per day*	Attribute agent disk space (KB)*	Days of detailed data kept	Warehouse space - detailed (MB)*	Aggregate records	Warehouse space - aggregated (MB)*	Total warehouse space for attribute group (MB)
		Record size - detailed	Record size- aggregated	Interval instances								
Total warehouse data size (sum of all attribute group total warehouse space)												
Total database size (Total warehouse data size * 1.5)												
***:** Use the equations in "Estimating the required size of your database" on page 19 for these values.												

Understanding the disk requirements for your database

Consider the following factors when designing a disk subsystem to support your database processing:

- Disk crash: With sufficient funds and planning, you can build a system that can continue running without interruption or be recovered in a few hours, despite a system crash. You can provide disk protection by using some level of RAID on parts, or all, of the disk subsystem. Some of the more popular types of RAID include the following:
  - RAID 1, also known as *disk mirroring*, uses data mirroring to achieve a high level of redundancy. In a RAID 1 configuration, two copies of the data are kept on separate disks, each mirroring the other.
  - RAID 5 uses block-level striping with distributed parity. RAID 5 stripes both data and parity information across three or more drives.
- The database log needs disk protection to enable database recovery of recent transactions. The other disks can optionally be protected. If they are protected, you can eliminate downtime while data is recovered.
- Consider the OS and paging space disks.
- Also, consider including one or two additional disks to speed up recovery and reduce the risks while running after a disk failure.
- Because of the increasing capacity of disk drives, the configurations listed below result in excess disk capacity but increase the number of disks available for I/O throughput.

The following table provides some example sizes for a database:

Table 7. Database size examples

	Number of disks to use			
	Absolute minimum disks	**Small RDBMS**	**Small and safe RDBMS**	**Large RDBMS**
Operating System	1	1	1 + mirror	1
Paging and RDBMS code	Use above	1	1 + mirror	1
RDBMS data	1	1	1 + mirror	8
RDBMS indexes	1	1	1 + mirror	6
RDBMS temp	Use above	1	1 + mirror	6
RDBMS logs	1 + mirror	1 + mirror	1 + mirror	2
Database data	12 GB	24 GB	48 GB	108+ GB
Number of disks	5	7	12	24

The **Absolute minimum disks** column specifies the minimum number of disks for an RDBMS. In this column, the index and temporary space is allocated onto one disk. While not an ideal arrangement, this might work in practice because databases tend to use indexes for transactions or temporary space for index creation and sorting full table scan large queries, but not both at the same time. This is not a recommended minimum disk subsystem for a database, but it does have the lowest cost.

The **Small RDBMS** column represents a minimum disk subsystem, although there might be limits in I/O rates because of the data being placed on only one disk.

Striping the data, indexes, and temporary space across these three disks might help reduce these I/O rate limits. This disk subsystem arrangement does not include disk protection for the database or other disks (apart from the mandatory log disk protection for transaction recovery).

The **Small and safe RDBMS** column adds full disk protection and can withstand any disk crash with zero database downtime.

The **Large RDBMS** column represents a typical size database for a database subsystem. Disk protection is not included in these sizings but can be added to increase the stability of the database.

Increasing the size of your database (DB2 only)

DB2 Workgroup Edition has a default table size limit of 64 GB with a page size of 4 KB. To increase the capacity of your DB2 database, you can create a new tablespace, IBMDEFAULTGROUP, and choose a larger page size (up to 32 KB). This increases the capacity of the database up to 512 GB per table.

The following example creates the IBMDEFAULTGROUP tablespace with a page size of 16 K. This increases the table size capacity to 256 GB.

```
CREATE REGULAR TABLESPACE IBMDEFAULTGROUP IN DATABASE PARTITION GROUP IBMCATGROUP
PAGESIZE 16384 MANAGED BY DATABASE
  USING (FILE 'E:\DB2\NODE0000\SQL00001\IBMDEFAULTGROUP.001'1500000)
  EXTENTSIZE 32
  PREFETCHSIZE AUTOMATIC
  BUFFERPOOL IBM16KBP
  OVERHEAD 12.670000
  TRANSFERRATE 0.180000
  DROPPED TABLE RECOVERY ON
```

If 512 GB of space per table is not enough for your environment, move to DB2 Enterprise Edition and using physical or logical partitioning.

The following steps outline the process for using database partitioning with DB2 Enterprise Edition:

1. Add a new database partition to the DB2 instance by running the **db2ncrt** command.
2. Use the ALTER TABLE statement to add a partitioning key to the tables that you want to partition. For example:

   ```
   ALTER TABLE "CANDLE "."NT_System"     ADD PARTITIONING KEY ("Server_Name")
        USING HASHING
   ```

3. Use the ALTER DATABASE PARTITION GROUP statement to assign the new partition to the database partition group. You can do this either from the command line or from the DB2 Control Center.
4. Redistribute the data in the database partition group, using the Redistribute Data Wizard in the DB2 Control Center.

For additional information about database partitioning, see the following DB2 sources:

- *IBM DB2 Universal Database Administration Guide: Planning*
- *IBM DB2 Universal Database Administration Guide: Implementation*
- DB2 Information Center at http://publib.boulder.ibm.com/infocenter/db2help/index.jsp.

For additional database performance and tuning information, see the *IBM Tivoli Monitoring Administrator's Guide*.

Planning considerations for the Tivoli Enterprise Portal client

The Tivoli Enterprise Portal client provides access to the Tivoli Enterprise Portal, the user interface to your monitoring environment. The portal client is available as a browser client or a desktop client. You can install the desktop client from installation media or you can use IBM Java Web Start to download the desktop client from the Tivoli Enterprise Portal Server. Each of these alternatives has comparative advantages and disadvantages for you to consider when planning your installation.

- The browser client is automatically installed with the Tivoli Enterprise Portal Server (It is located on a Web server that is integrated with the portal server.) You can access the browser client from any Windows computer through Microsoft Internet Explorer by entering the URL for the client. There is no need for a special installation procedure.

  An advantage of the browser client is centralized administration from the server. The user does not need to perform special configuration procedures or maintenance updates. You benefit from the latest updates whenever you access the Tivoli Enterprise Portal from your browser. Another convenience of the browser client is that you can use the bookmark feature of your browser to quickly access particular workspaces and views in the Tivoli Enterprise Portal.

  One disadvantage of the browser client is that it is accessible only from a Windows computer. In addition, the browser client requires the IBM Java 1.5 runtime environment. If the JRE is not installed on the computer on which the browser is launched, you are prompted to download and install it. The Windows user account must have local administrator authority to download and install the JRE. Finally, the performance of the browser client is slower than the desktop client.

  Note: The browser client is supported only in Internet Explorer on Windows. However, see the IBM Tivoli Open Process Automation Library (OPAL) Web site at http://www.ibm.com/software/tivoli/opal for solutions for alternative browsers and platforms.
- The desktop client provides better performance than the browser client. You can install the desktop client from the IBM Tivoli Monitoring installation media or you can use IBM Web Start for Java to download the desktop client from the Tivoli Enterprise Portal Server.
- When the desktop client is installed from installation media, users must perform maintenance updates. Unless you want a very secure environment where there are no downloads, it is best to use IBM Web Start for Java as a vehicle for obtaining the desktop client.
- When you use IBM Web Start for Java to obtain and run the desktop client, you benefit from the performance advantage of the desktop client as well as the convenience of centralized administration from the server. On each startup of the desktop client, any maintenance updates are downloaded from the server. Unlike the browser client, which can run only from Windows, the desktop client can run on either Windows or Linux.

  To use Java Web Start to download the desktop client from the Tivoli Enterprise Portal Server, IBM Runtime Environment for Java 2, version 5.0 (also referred to as IBM JRE version 1.5) must be installed on the system to which you are downloading the client.

While the desktop client obtained through Java Web Start might seem to be a better choice than the browser client, the browser client retains some advantages. The browser client does allow you to bookmark workspaces. The browser client is *required* for launching products in context, such as IBM Tivoli Application Dependency Discovery Manager.

Note: Regardless of how you deploy it, if you are running the desktop client on Linux, or you want to view the online help with some browser other than Internet Explorer on Windows, you must configure the portal client with the location of the browser to use to display the online Help. See "Specifying the browser used for online help" on page 185.

Sample deployment scenarios

This section offers several types of scenarios.

- "Scenarios for small, medium, and large environments" provides examples of deployments tailored to the size of the monitored environment
- "High availability scenarios" on page 34 provides examples of deployments that incorporate Hot Standby or clustering to provide high availability and resilience.
- "Event integration scenarios" on page 52 illustrates deployments that include event integration with Tivoli Enterprise Console or Netcool/OMNIbus.

Scenarios for small, medium, and large environments

This section presents deployment example for small, medium, and large environments. In the interest of readability and understanding, these examples are simplified schematics rather than actual real-world solutions. They serve as a convenient starting point for deployment planning.

Note on terminology:
The term *hub environment* or *hub installation* refers to a single hub monitoring server and the management components with which it is associated: remote monitoring servers, portal server, Warehouse Proxy agents, Summarization and Pruning agent, and the Tivoli Data Warehouse. The monitoring environment of an enterprise can be described with one of the following terms:

Single hub installation
This term is a synonym for *hub installation* (or *hub environment*): a single hub monitoring server and its associated management components.

Multiple independent hub installations
This term refers to multiple single-hub installations that are *independent* of one another, meaning that long-term monitoring data and event data from each installation is not merged. Each installation retains a separate Tivoli Data Warehouse and dedicated event server (or servers).

Multiple hub installation (or multi-hub installation)
This term refers to multiple single-hub installations that are coordinated, meaning that long-term monitoring data and event data from each installation is merged. All hub installations share a single Tivoli Data Warehouse.

Small monitoring environment

You can deploy a small IBM Tivoli Monitoring environment on a single computer. This type of environment might be useful for a teaching environment, for advanced prototyping and testing of solutions, or for monitoring a small, but

critical, server environment. A single server environment with failover support might be built and dedicated to monitoring heartbeats from the mail servers within a medium size company.

Figure 3 shows a small monitoring environment. If you install all components on a Windows computer with a DB2 or Microsoft SQL Server database, the installation procedure described in Chapter 5, "Installing IBM Tivoli Monitoring on one computer," on page 105 automates the tasks involved in setting up data warehousing.

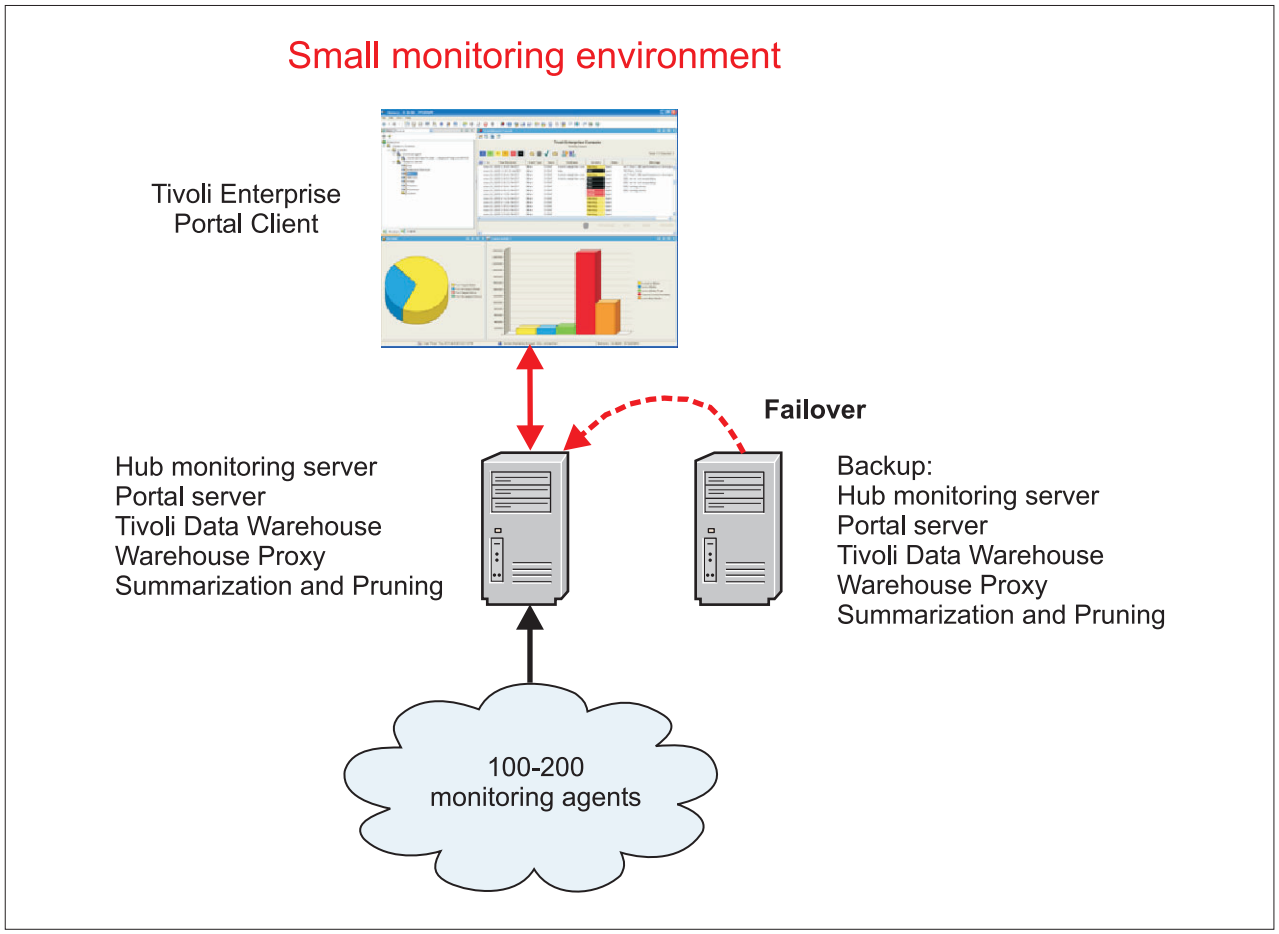


Figure 3. Small IBM Tivoli Monitoring environment

The small environment is limited to 100 to 200 agents. It can perform minimal historical data collection and does not use the IBM Tivoli Enterprise Console. Adding significant data collection or enterprise-wide event correlation requires additional servers.

The advantages of a small environment are that it is simple, the most reliable, and the least expensive.

The disadvantages of a small environment are that you can support only a small number of agents. Also, more than minimal historical data collection or a significant number of situation events could overwhelm capacity.

If you are going to use a small monitoring environment, choose a multiprocessor (2 or 4-way) for the monitoring server with at least 2 GB of memory. Configure the

software and begin monitoring CPU and memory usage during periods of both normal and high volumes of situation events. If CPU or memory usage is constrained, consider deploying a separate server for the Tivoli Data Warehouse, the Warehouse Proxy agent, and the Summarization and Pruning agent.

Medium monitoring environment

You can build a medium monitoring environment with five to ten computers. This level of deployment might be used in a medium-sized company, or it can be used within a large company to monitor different server groups independently according to organizational boundaries. For example, one hub installation might monitor the mail servers, while another installation monitors the HTTP servers, and a third monitors transaction servers. The departments responsible for each server group maintains control over the monitoring and historical data for that group.

Figure 4 shows a medium monitoring environment.

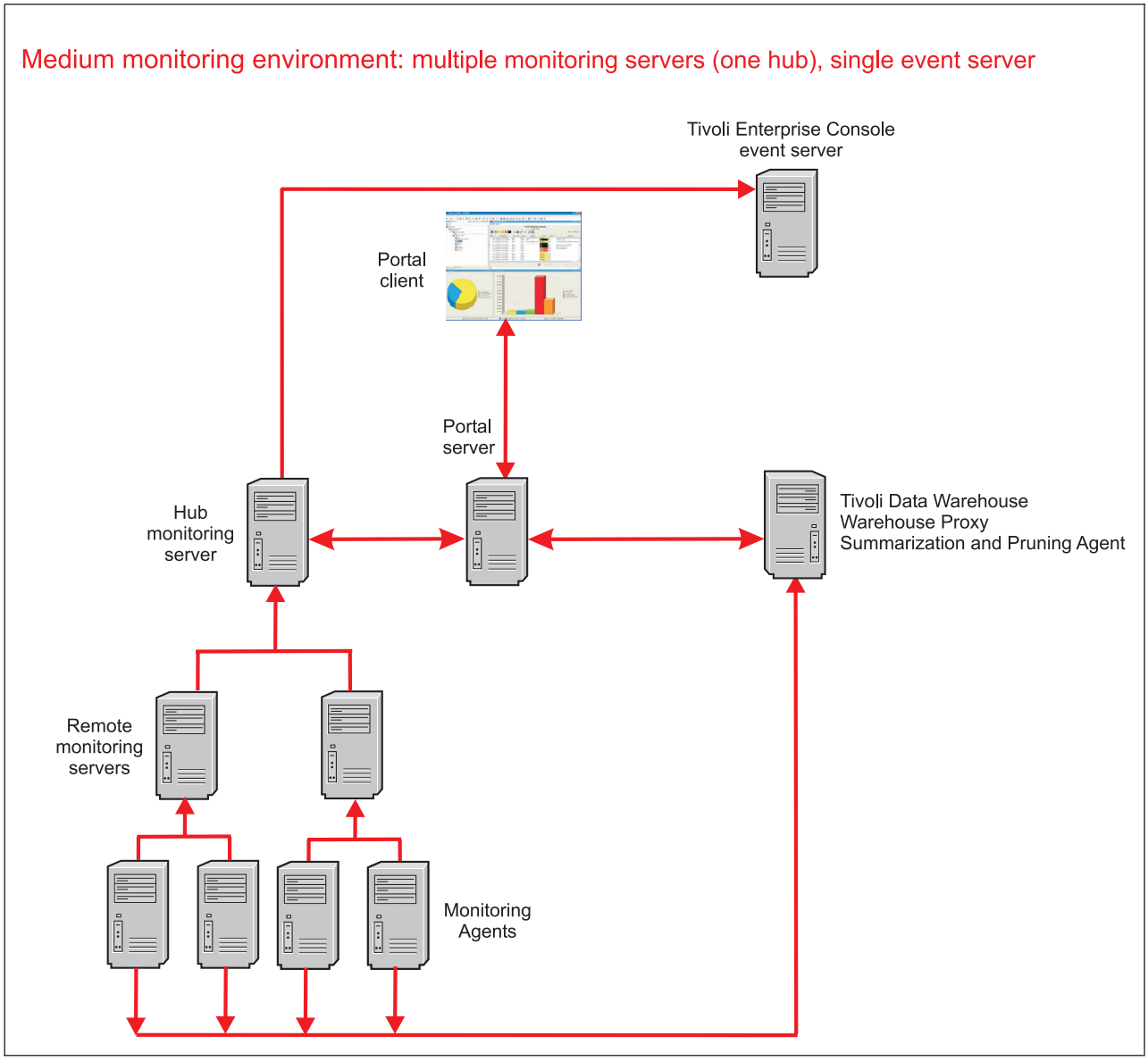


Figure 4. Medium IBM Tivoli Monitoring environment

The medium monitoring environment supports as many as 1000 to 1500 monitoring agents using a single hub monitoring server, a single Warehouse Proxy agent, and a few remote monitoring servers. Tivoli Enterprise Console is used to correlate events, and a Tivoli Data Warehouse server collects and saves historical data for debugging and reports.

The medium monitoring environment offers a number of advantages over the small monitoring environment: significant historical data collection and event correlation is possible across a large number of agents, complex database queries do not interfere with the performance of real-time monitoring tasks, and complex correlation is possible using Tivoli Enterprise Console.

The disadvantage of the medium monitoring environment is that if multiple independent hub installations are deployed, enterprise-wide historical database and event correlation is not available.

Follow these guidelines for the medium monitoring environment:

- When selecting hardware for the monitoring servers and portal server, use system configurations that meet or exceed the recommended hardware requirements. (See "Required hardware for distributed systems" on page 80 and "Required hardware for System z" on page 82.)
- Scale the Tivoli Data Warehouse server according to how much historical data you plan to collect and retain. (See "Planning considerations for the Tivoli Data Warehouse" on page 19.)
- A simple one-server Tivoli Enterprise Console deployment can handle the event correlation.
- Keep the Tivoli Data Warehouse, Warehouse Proxy, and Summarization and Pruning agent on the same computer to minimize server deployments, simplify configuration, and eliminate network transmission overhead.

Large monitoring environment: single hub installation

The large monitoring environment with a single hub monitoring server, shown in Figure 5 on page 31, is similar to the medium environment. The difference is that the large single hub installation contains multiple Warehouse Proxy agents and additional remote monitoring servers to support a larger number of agents. (The difference in the number of remote monitoring servers and agents is not represented in the diagram.) As with the medium monitoring environment, you can deploy a single hub installation or multiple independent hub installations to monitor different server groups according to organizational boundaries.

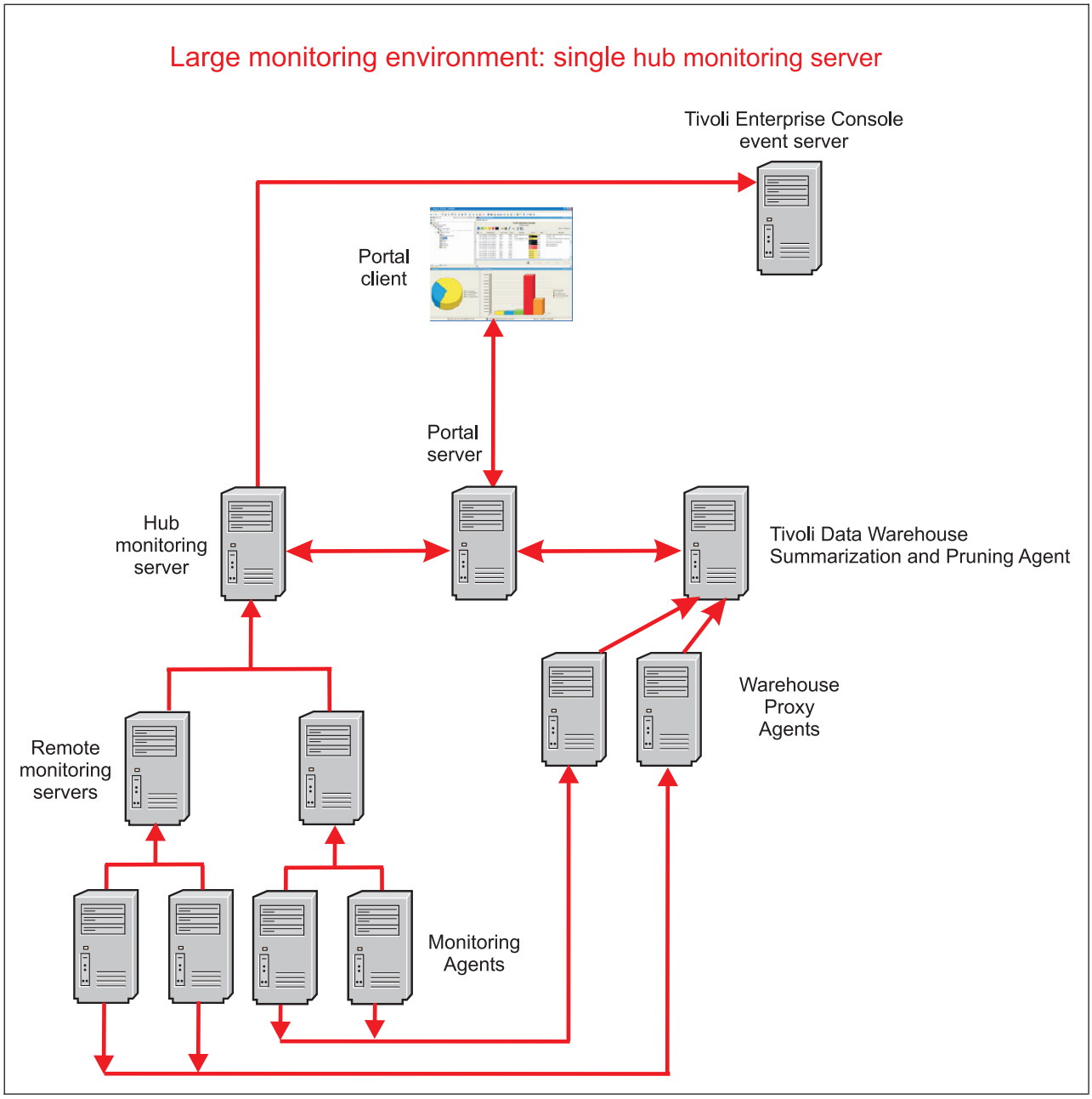


Figure 5. Large deployment of IBM Tivoli Monitoring: single hub installation

A large single-hub monitoring environment can support thousands of monitoring agents. The number of monitoring agents that can be managed from a single-hub environment depends on a number of factors, which are described in "Determining the number of monitoring servers needed" on page 16. Use Table 5 on page 17 to help determine the number of remote monitoring servers that are appropriate for a large environment. Install multiple Warehouse Proxy agents to spread the work of receiving historical data from the monitoring agents and inserting it into the warehouse database.

The advantage of the large single-hub monitoring environment over the medium environment is that it supports a larger number of monitoring agents.

The disadvantages are limitations of scale and, if multiple independent hub installations are deployed, enterprise-wide historical database and event correlation is not available. The multi-hub deployment described in the following section alleviates these disadvantages.

Follow these guidelines for the large single-hub monitoring environment:

- When selecting hardware for the monitoring servers and portal server, use system configurations that meet or exceed the recommended hardware requirements. (See "Required hardware for distributed systems" on page 80 and "Required hardware for System z" on page 82.)
- Scale the Tivoli Data Warehouse server according to how much historical data you plan to collect and retain. (See "Planning considerations for the Tivoli Data Warehouse" on page 19.)
- If you install the Tivoli Data Warehouse on a separate computer from the Summarization and Pruning agent, ensure that you have a high-speed network connection between them for best performance. You can install one of the Warehouse Proxy agents on the same computer as the Tivoli Data Warehouse. Additional Warehouse Proxy agents must be installed on separate computers.

Large monitoring environment: multiple hub installation

Figure 6 depicts a large multi-hub installation that is designed to handle enterprise-wide historical data collection and event correlation.

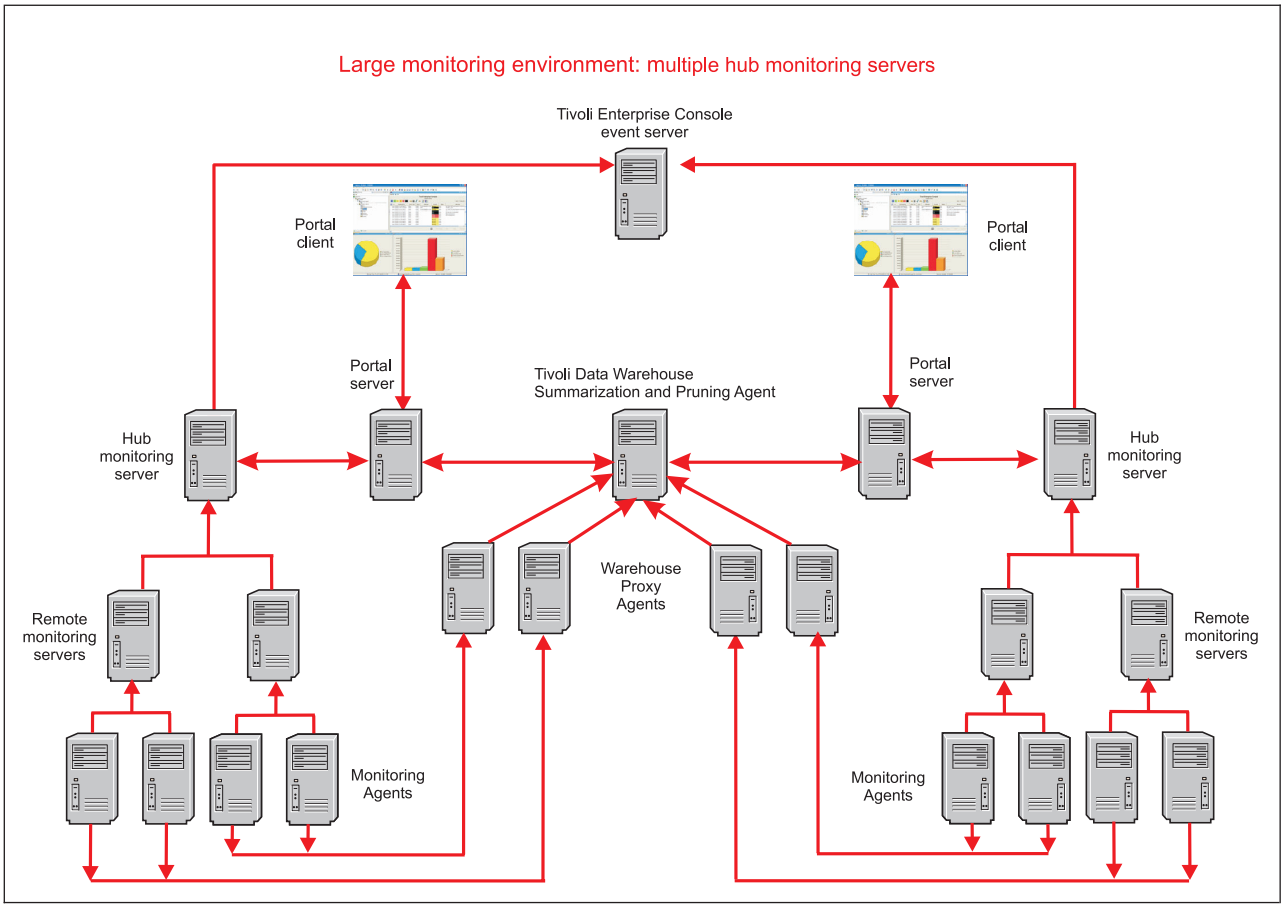


Figure 6. Large deployment of IBM Tivoli Monitoring: multiple hub installation

A large multi-hub environment can monitor a larger number of agents than a large single-hub environment. Tivoli Enterprise Console is used to correlate events across

all hub monitoring servers. A single Tivoli Data Warehouse server collects and saves historical data for debugging and reports.

The advantage of the large multi-hub monitoring environment is that historical data and event correlation is enterprise-wide. You can use complex database queries to access all data.

A disadvantage of this environment is that it is more difficult to debug. The possibility of failure increases as the number of servers grows. Failure recovery is also more complex.

Follow these guidelines for a large multi-hub monitoring environment:

- When selecting hardware for the monitoring servers and portal server, use system configurations that meet or exceed the recommended hardware requirements. (See "Required hardware for distributed systems" on page 80 and "Required hardware for System z" on page 82.)
- Scale the Tivoli Data Warehouse server according to how much historical data you plan to collect and retain. (See "Planning considerations for the Tivoli Data Warehouse" on page 19.)
- If you install the Tivoli Data Warehouse on a separate computer from the Summarization and Pruning agent, ensure that you have a high-speed network connection between them for best performance. You can install one of the Warehouse Proxy agents on the same computer as the Tivoli Data Warehouse. Additional Warehouse Proxy agents must be installed on separate computers.
- Identify one of the hub installations as the *primary* installation. (The *primary* installation is a logical designation only.)
  - If the hub monitoring servers are at different maintenance levels, designate the primary installation as the installation with the hub monitoring server at the highest maintenance level.
  - Configure the Summarization and Pruning agent to report to the hub monitoring server of the primary installation. (When you install the Summarization and Pruning agent, you identify the hub monitoring server that it communicates with. See "Installing monitoring agents" on page 148.)
  - Install application support for all agent types that exist in the multi-hub installation on the hub monitoring server, remote monitoring servers, portal server, and portal desktop clients that belong to the primary hub installation.

    For example, consider the following scenario: A multi-hub installation consists of two hubs (as in Figure 6 on page 32).

    - Hub A, designated as the primary hub, contains Windows, UNIX, and Linux agents.
    - Hub B contains z/OS and CICS agents.

    Install application support for all those agent types (Windows, UNIX, Linux, z/OS, and CICS) on the hub monitoring server, remote monitoring servers, portal server, and portal desktop clients that belong to Hub A (the primary hub installation). Install application support for the z/OS and CICS agents on the hub monitoring server, remote monitoring servers, portal server, and portal desktop clients of Hub B.

    For information about application support, see "Installing and enabling application support" on page 159.)

High availability scenarios

There are two primary technological approaches to configure resiliency or high availability for the Tivoli monitoring platform components. One approach exploits common, commercial high availability cluster manager software. (Examples are High-Availability Cluster Multi-Processing (HACMP) and System Automation-Multi Platform (SA-MP) from IBM, or Microsoft Cluster Server (MSCS).) An alternative approach may be applicable for some sites to make the hub monitoring server resilient to specific failure scenarios. This alternative approach is called Hot Standby in the Tivoli publications. The two approaches provide different resiliency and failover characteristics, depending on your requirements.

The first approach requires the use of a high availability cluster manager such as IBM's SA-MP, HACMP or Microsoft's MSCS. You are entitled to cluster management software with some operating systems and platforms. Using this approach, you can configure all of the components of the monitoring platform for resiliency in the case of component failure. IBM has produced white papers describing specific resiliency configurations using common commercial HA solutions. In addition, since so many users use such a wide range of customized HA solutions, we also provide a general description of Tivoli monitoring platform resiliency requirements that should suffice to set up any typical HA configuration. For more information about using IBM Tivoli Monitoring in a clustered environment, search for "Clustering IBM Tivoli Monitoring" at the IBM Tivoli Open Process Automation Library (OPAL) Web site.

For users primarily concerned with the availability of the hub monitoring server, the monitoring platform provides the built in Hot Standby option. This solution replicates selected state information between the hub monitoring server and a secondary hub monitoring server running in a listening standby mode, heart-beating the active hub and keeping current with much of the hub's environment information. In an appropriately configured environment, the secondary hub monitoring server takes over as the acting hub in the event that the primary hub fails. This solution operates without the requirement for shared or replicated persistent storage between the two monitoring server computers, and does not require cluster manager software. However, it only addresses the hub monitoring server component of the monitoring platform, and is therefore suited to customers without stringent resiliency requirements on the other components of the monitoring platform. See Table 8 for the failover options available for each monitoring component and Table 9 on page 35 for the resiliency characteristics for each option.

Table 8. Options for Tivoli Monitoring components resiliency

Component	Potential single point of failure?	Cluster failover available?	Hot Standby failover available?
Hub monitoring server	Yes	Yes	Yes
Portal server	Yes	Yes	No
Tivoli Data Warehouse database	Yes	Yes	No
Warehouse proxy	Yes, if single Warehouse Proxy in environment.	Yes	No
Summarization and Pruning agent	Yes	Yes	No

Table 8. Options for Tivoli Monitoring components resiliency (continued)

Component	Potential single point of failure?	Cluster failover available?	Hot Standby failover available?
Remote monitoring server	No. Another monitoring server can assume the role of a remote monitoring server for connected agents. This is known as "agent failover".	N/A	N/A
Agent	Not a single point of failure for the whole monitoring solution, but a specific point of failure for the specific resource being monitored.	Yes	No

Table 9. Resiliency characteristics of Tivoli Monitoring components and features

Component/ Feature	Characteristics on hub cluster failover	Characteristics on hub Hot Standby failover
Hub monitoring server	The hub monitoring server is restarted as soon as the cluster manager detects failure.	Communication failure between hubs causes the standby hub to start processing to establish itself as master.
Portal server	The portal server reconnects to hub as soon as it is restarted.	The portal server needs to be reconfigured to point to the new hub.
Tivoli Data Warehouse database	No relationship to hub	No relationship to hub
Warehouse proxy	As an agent, the Warehouse Proxy reconnects to its hub and continues to export data from agents to the Tivoli Data Warehouse.	As an agent configured with secondary connection to hub, the Warehouse Proxy connects to its secondary hub and continues to export data from agents to the Tivoli Data Warehouse.
Summarization and Pruning agent	As an agent, the Summarization and Pruning agent reconnects to its hub and continues to summarize and prune data from the Tivoli Data Warehouse.	As an agent configured with secondary connection to hub, the Summarization and Pruning agent connects to its secondary hub and continues to summarize and prune data from the Tivoli Data Warehouse.
Remote monitoring server	The remote monitoring server detects the hub restart and tries to reconnect, synchronizing with the hub.	When configured with secondary connection to hub, the remote monitoring server retries the connection with the primary hub and if unsuccessful tries to connect to the secondary hub. When the new hub has been promoted to master, the remote monitoring server detects the hub restart and tries to reconnect, synchronizing with the hub.

Table 9. Resiliency characteristics of Tivoli Monitoring components and features (continued)

Component/ Feature	Characteristics on hub cluster failover	Characteristics on hub Hot Standby failover
Agent	All agents directly connected to the hub reconnect to the hub after restart and begin synchronization.	When configured with secondary connection to hub, agents directly connected to the hub perceive the loss of connection and retry. With the first hub down, the agent tries to connect to the second hub, and begin synchronization which includes restarting all situations.
Event data	Agents resample all polled situation conditions and reassert all that are still true. Situation history is preserved.	Agents resample all polled situation conditions and reassert all that are still true. Previous situations history is not replicated to mirror and thus lost. To persist historical event data, use the OMNIbus or Tivoli Enterprise Console.
Hub failback	Available through cluster manager administration/configuration	The secondary hub must be stopped so that primary hub can become master again.
Time for failover	The detection of a failed hub and restart is quick and can be configured through the cluster manager. The synchronization process until all situations are restarted and the whole environment is operational depends on the size of the environment, including the number of agents and distributed situations.	The detection of a failed hub is quick. There is no restart of the hub, but the connection of remote monitoring server and agents to the standby hub require at least one more heartbeat interval, because they try the primary before trying the secondary. The synchronization process until all situations are restarted and the whole environment is operational depends on the size of the environment, including the number of agents and distributed situations.
z/OS environments	The z/OS hub clustered solution has not yet been tested and therefore is not a supported configuration. Remote monitoring servers on z/OS are supported.	Hot Standby not supported on z/OS. Hot Standby has not been tested with remote monitoring servers on z/OS and therefore is not a supported configuration.
Data available on failover hub	All data is shared through disk or replication.	All EIB data, except for the following, is replicated through the mirror synchronization process: • Situation status history • Publishing of any UA metadata, versioning • CCT – Take Action DB • remote deployment Depot

Table 9. Resiliency characteristics of Tivoli Monitoring components and features (continued)

Component/ Feature	Characteristics on hub cluster failover	Characteristics on hub Hot Standby failover
Manageability of failover	Failover can be automatic or directed through cluster administration. You control which hub is currently the "master" and the current state of the cluster.	Failover can be directed by stopping the hub. Note that starting order controls which hub is the "master".

Using Hot Standby

Figure 7 depicts an environment with the Hot Standby feature configured.

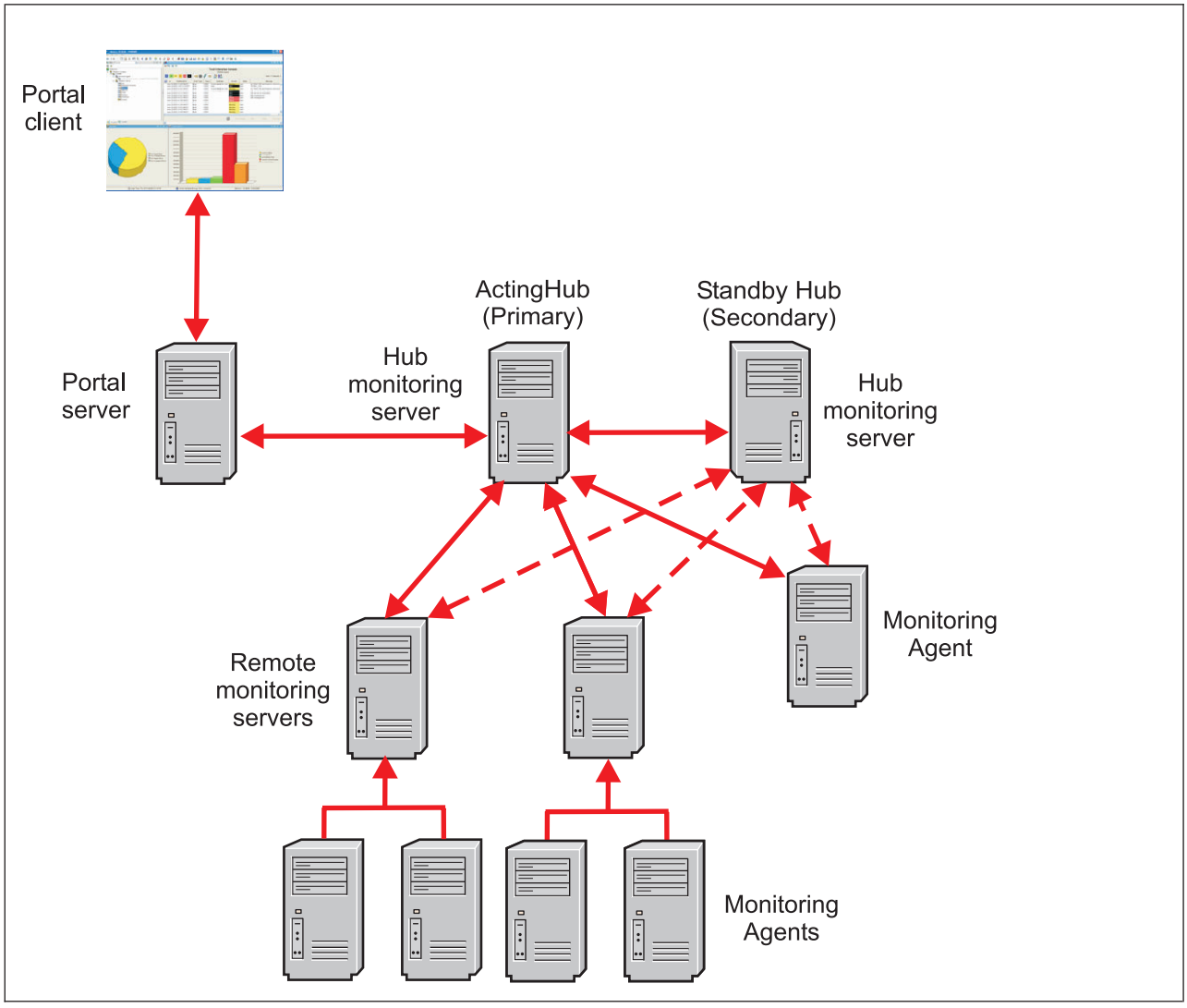


Figure 7. IBM Tivoli Monitoring configuration with hot standby

The following sections provide an overview of how each component in the IBM Tivoli Monitoring environment is configured to enable the Hot Standby feature.

Hub monitoring servers: In a Hot Standby environment, there are two hub monitoring servers. The configuration of each hub designates the other hub as the

Hot Standby hub. At any given time, one of the two hub monitoring servers is operating as the hub. This server is referred to as the *Acting Hub*. The other hub monitoring server is in standby mode and is referred to as the *Standby Hub*. (See Figure 7 on page 37.)

When the two hub monitoring servers are running, they continuously synchronize their Enterprise Information Base (EIB) data, enabling the Standby Hub to take over the role of the Acting Hub in case the Acting Hub becomes unavailable. The EIB contains definition objects such as situations and policies, information about managed systems, and information about the distribution or assignment of situations and policies to managed systems.

The two hub monitoring servers are symmetrical, but for reasons that will become clear later, one hub monitoring server is designated as the *Primary Hub* and the other is designated as the *Secondary Hub*. While it is not necessary, you can designate as the Primary Hub the server that you expect to be the Acting Hub most of the time.

Note that the terms *Acting* and *Standby* refer to an operational state, which can change over a period of time. The terms *Primary* and *Secondary* refer to configuration, which is relatively permanent.

Remote monitoring servers: All remote monitoring servers must be configured to operate in the Hot Standby environment. When you configure each remote monitoring server, you specify the Primary and Secondary hub monitoring servers to which the remote monitoring server reports.

It is important that you specify the same Primary and Secondary hub monitoring servers for each remote monitoring server. In Figure 7 on page 37, the connections from the remote monitoring servers to the Primary Hub are depicted with solid arrows. The connections to the Standby Hub are depicted with dashed arrows.

Monitoring agents: Monitoring agents that report directly to the hub monitoring server, as well as the Warehouse Proxy agent and the Summarization and Pruning agent, must be configured to operate in the Hot Standby environment. When you configure each of these agents, you specify the Primary and Secondary hub monitoring servers to which the agents report.

In Figure 7 on page 37, the connection between these monitoring agents and the Primary Hub is depicted with a solid arrow. The connection to the Standby Hub is depicted with a dashed arrow.

Portal server: The Tivoli Enterprise Portal Server cannot be configured to fail over to a Standby Hub. When the Standby Hub takes over as the Acting Hub, the portal server needs to be reconfigured to point to the Acting Hub. Portal clients do not need to be reconfigured. They automatically reconnect to the portal server when it restarts after it is reconfigured.

Failover scenario: The Hot Standby operation is best illustrated by describing a scenario. In this example, all monitoring components are started in order, a scenario that might take place only when the product is initially installed. After installation, components can be started and stopped independently.

Starting up the components: The following list describes the order of startup and what happens as each component is started.

1. The Primary Hub is started first.

a. When the Primary Hub starts, it adds a message to its operations log to indicate that it is configured for Hot Standby:

```
04/17/07  09:38:54 KQM0001  FTO started at  04/17/07  09:38:54.
```

b. The Primary Hub then attempts to connect to the Standby Hub (the Secondary Hub). Because the Standby Hub is not yet available, the Primary Hub assumes the role of the Acting Hub.

2. The Secondary Hub is started.

a. When the Secondary Hub starts, it adds a message to its operations log to indicate that it is enabled for Hot Standby:

```
04/17/07  09:47:04 KQM0001  FTO started at  04/17/07  09:47:04.
```

b. The Secondary Hub attempts to connect to the Primary Hub. The connection succeeds. Sensing that the Primary Hub started earlier (and is therefore the Acting Hub), the Secondary Hub assumes the role of the Standby Hub, indicated by the following messages:

```
04/17/07  09:47:18 KQM0003  FTO connected to IP.PIPE:#9.52.104.155
at 04/17/07 09:47:18.
04/17/07  09:47:33 KQM0009  FTO promoted HUB_PRIMARY as the acting HUB.
```

c. The Primary Hub also succeeds in connecting with the Secondary Hub, and issues the following messages:

```
04/17/07  09:45:50 KQM0003  FTO connected to IP.PIPE:#9.52.104.155
at 04/17/07 09:45:50.
04/17/07  09:45:58 KQM0009  FTO promoted HUB_PRIMARY as the acting HUB.
```

d. The Standby Hub queries the Acting Hub to see if there are any updates to the EIB data since it last communicated with the Acting Hub. It replicates all updates.

e. After the initial startup and connections, the two hubs monitor connections with each other periodically to ensure that the other hub is running and that there is no change in status.

f. The Standby Hub also monitors the Acting Hub periodically for further updates to the EIB, and replicates the updates in its own EIB. By default, this monitoring takes place every 5 seconds. As a result, the Standby Hub is ready to take over the role of the Acting Hub when required.

3. The remote monitoring servers and monitoring agents are started.

   When these components start, they attempt to connect to the Primary Hub in their configuration. In this scenario, the Primary Hub is also the current Acting Hub. Therefore, the connection attempt is successful, and these components start reporting to the Primary Hub.

4. The Tivoli Enterprise Portal Server connects to the Primary Hub.

   The portal server is configured to connect to the Primary Hub. One or more portal clients are connected to the portal server for monitoring purposes.

Failing over: The Acting Hub might become unavailable for a number of reasons. It might need to be shut down for scheduled maintenance, the computer on which it is running might need to be shut down or might have crashed, or it could be experiencing networking problems.

When the Standby Hub discovers that the Acting Hub is unavailable, it takes over the role of the Acting Hub and issues the following messages:

```
04/17/07  10:46:40 KQM0004  FTO detected lost parent connection
at 04/17/07 10:46:40.
04/17/07  10:46:40 KQM0009  FTO promoted HUB_SECONDARY as the acting HUB.
```

The Primary Hub is now the Standby Hub and the Secondary Hub is the Acting Hub, as depicted in Figure 8:

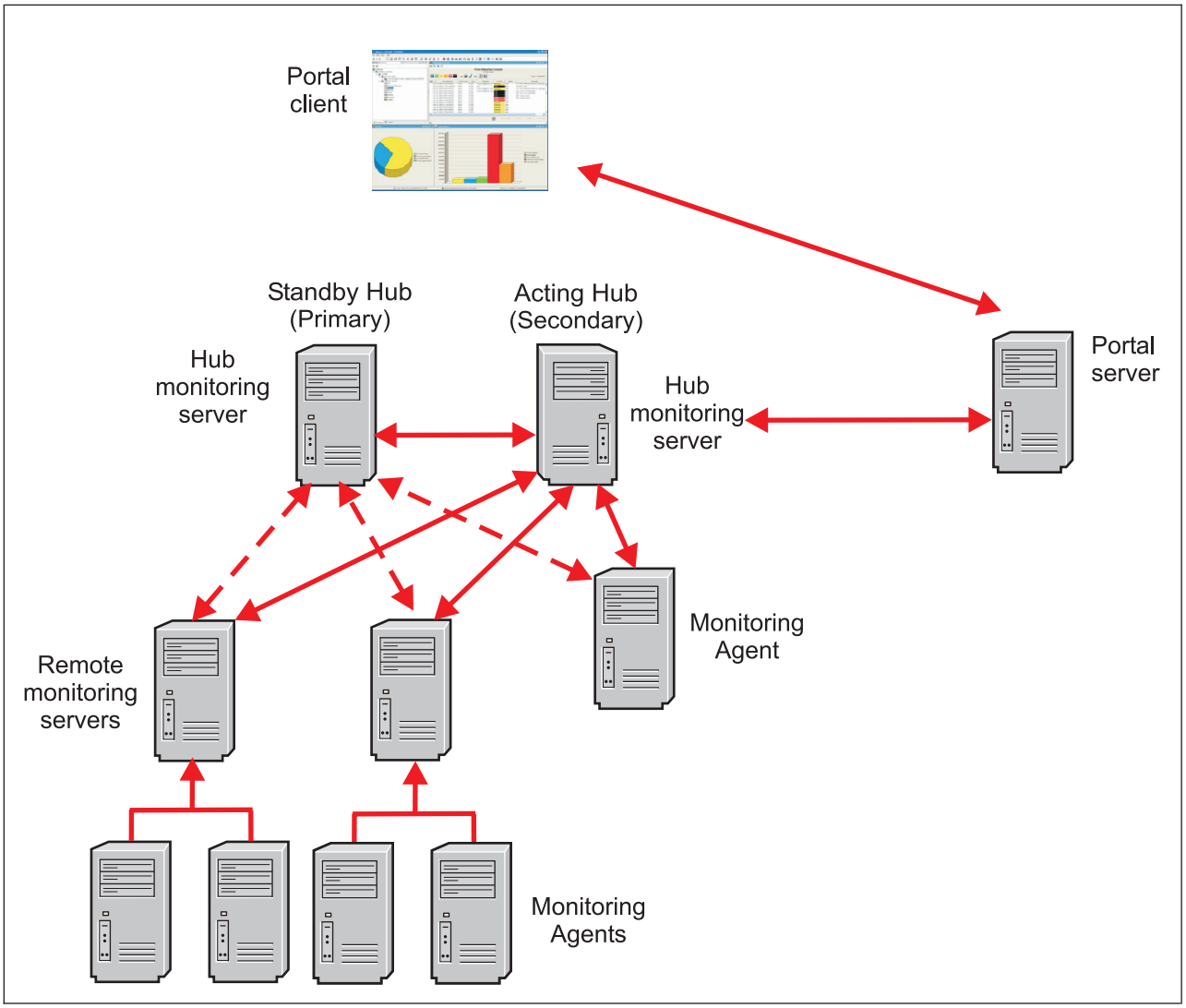


Figure 8. Configuration after failover

As the remote monitoring servers and agents connected to the previous Acting Hub discover that this hub is no longer available, they switch and reconnect to the new Acting Hub. Because these components are in various states of processing and communication with the hub monitoring server, the discovery and re-connection with the new hub is not synchronized.

The Tivoli Enterprise Portal Server must be reconfigured to point to the new Acting Hub and then restarted. All portal clients reconnect to the portal server after it is restarted.

The processing that takes place after re-connection is similar to the processing that takes place after re-connection in an environment without a Hot Standby server. The following processing takes place with regard to situations and policies:

1. Pure events that occurred before the failover are not visible. Subsequent pure events are reported when they occur.
2. Sampled situations are reevaluated, and are reported again if they are still true.

3. A Master Reset Event is sent to the Tivoli Enterprise Console when the failover occurs. Events that result from situations being reevaluated are resent to the Tivoli Enterprise Console if the monitoring server has been configured to send events to the Tivoli Enterprise Console.
4. Policies are restarted.

The new Acting Hub retains its role even after the other hub monitoring server becomes operational again. The other hub monitoring server now becomes the Standby Hub. When the new Standby Hub starts, it checks the EIB of the new Acting Hub for updates, and replicates the updates to its own EIB if necessary. The two hubs also start monitoring connections with each other to ensure that the other hub is running.

All remote monitoring servers and agents now report to the new Acting Hub. There is no mechanism available to switch them back to the Standby Hub while the Acting Hub is still running. The only way to switch them to the Standby Hub is to shut down the Acting Hub.

If a remote monitoring server or agent experiences a transient communication problem with the Acting Hub, and switches over to the Standby Hub, the Standby Hub instructs it to retry the connection with the Acting Hub, because the Standby Hub knows that the Acting Hub is still available.

The environment continues to operate with the configuration shown in "Using Hot Standby" on page 37 until there is a need to shut down the Acting Hub, or if the computer on which the Acting Hub is running becomes unavailable. Each time the Acting Hub becomes unavailable, the failover scenario described in this section is repeated.

Using clustering

This section provides an overview of Tivoli Monitoring high availability when using clustering technologies. It explains clustering concepts, describes the supported Tivoli Monitoring cluster configurations, provides an overview of the setup steps, and describes the expected behavior of the components running in a clustered environment.

For more information about using IBM Tivoli Monitoring in a clustered environment, search for "Clustering IBM Tivoli Monitoring" at the IBM Tivoli Open Process Automation Library (OPAL) Web site: http://catalog.lotus.com/wps/portal/topal/. Detailed instructions on how to set up Tivoli Monitoring components on different cluster managers are provided in separate papers, initially including: Microsoft® Cluster Server, Tivoli System Automation Multiplatform and HACMP (High-Availability Cluster Multi-Processing).

Review the following concepts to enhance your understanding of clustering technology:

- A *cluster* is a group of individual computer systems working together to provide increased application availability.
- A *node* is a computer system that is a member of a cluster.
- A *resource* is a physical or logical entity that is capable of being managed by a cluster, brought online, taken offline and moved between nodes.
- *Resource groups* are collections of resources that are managed as a single unit, and hosted on one node at any point in time.
- *Failover* is the process of taking resource groups offline on one node and bringing them back on another node. Resource dependencies are respected.

- *Failback* is the process of moving resources back to their original node after the failed node comes back online.

Although clusters can be used in configurations other than basic failover (for example, load sharing and balancing), the current Tivoli Monitoring design does not support multiple, concurrent instances of the monitoring components.

Clustering configurations: Consider the following three clustering configurations:

Note:

IBM DB2 was the database used in all of the configuration tests. Other Tivoli Monitoring-supported databases can also be clustered by following the specific database cluster setup procedures. All the clustering configurations include at least one agent directly reporting to the hub. For simplicity, this is not shown in the configuration diagrams that follow.

Configuration A

This configuration has a hub cluster, portal server cluster, and data warehouse cluster (including the Summarization and Pruning agent and the Warehouse Proxy), with multiple remote monitoring servers (RT1, RT2, RT3) and agents, and Tivoli Enterprise Console integration.

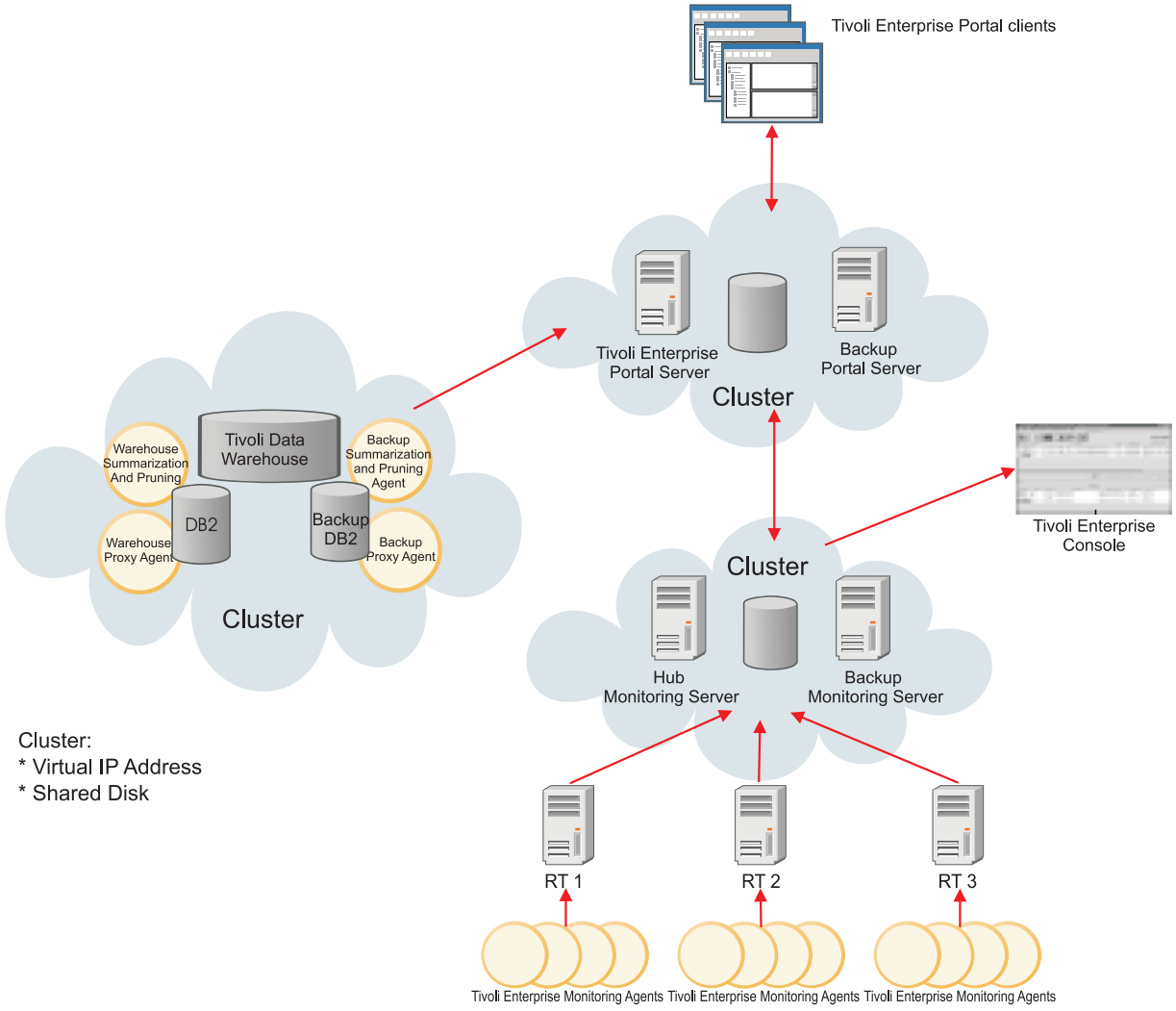


Figure 9. Separate component clusters

Configuration B

In this configuration, the Warehouse Proxy and Summarization and Pruning agents are running outside of the data warehouse cluster.

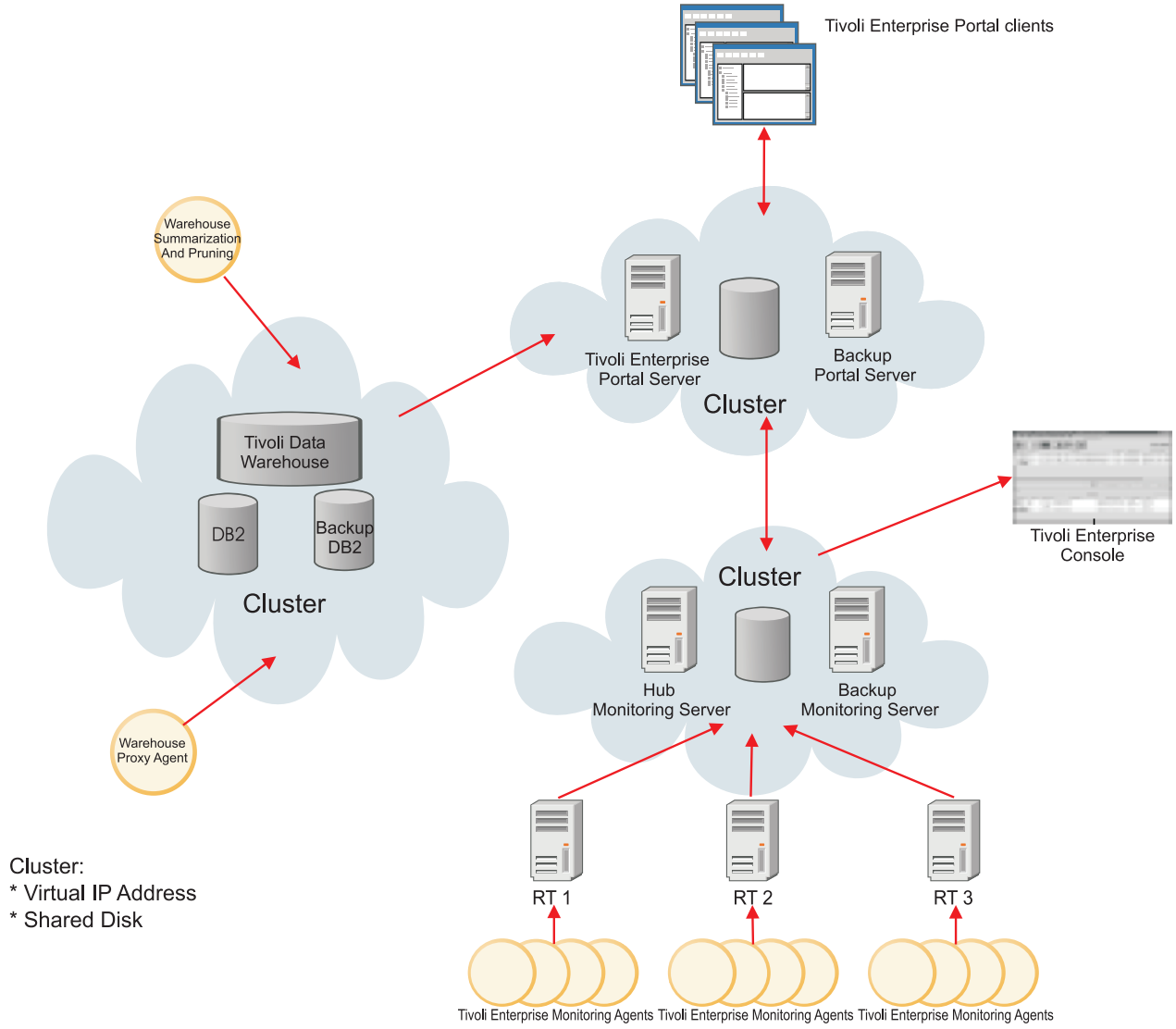


Figure 10. Separate component clusters, with the Warehouse Proxy and Summarization and Pruning agents outside the data warehouse cluster

Configuration C

In this configuration, all main components are clustered in just one cluster. Also included is one agent running on the clustered environment and directly reporting to the hub, which is not included in the picture for simplification.

This configuration represents a degenerated case of Configuration A. It is important to guarantee that the computers used for such an environment have enough power to handle all the components. The behavior of the clustered components is the same in this case, but the setup of Tivoli Monitoring on such an environment has some differences.

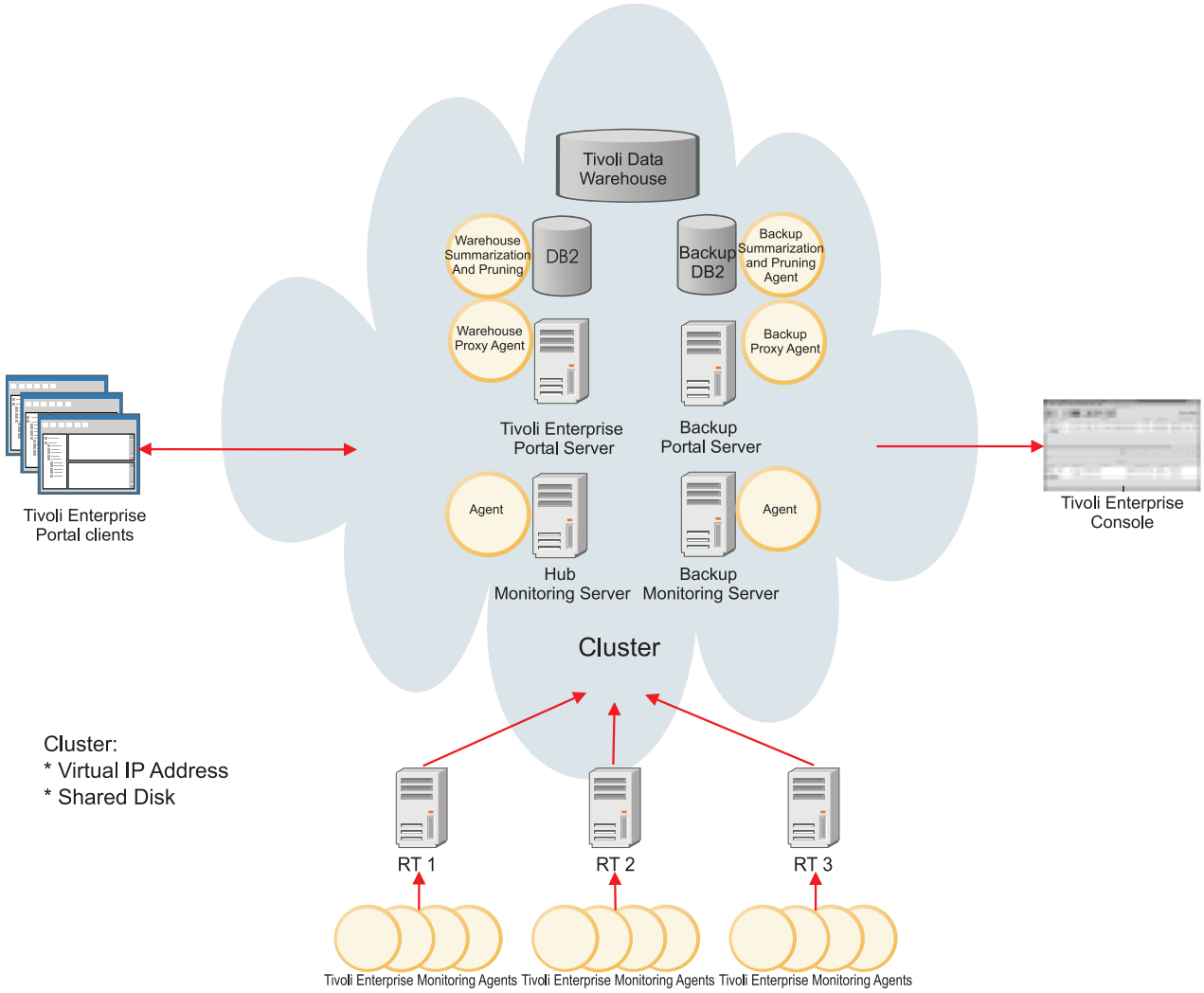


Figure 11. One cluster for the hub, portal server, and data warehouse

Setting up Tivoli Monitoring components in a clustered environment: This section describes the overall procedure for setting up Tivoli Monitoring components on clustered environments.

Tivoli Monitoring cluster setup: A basic cluster setup includes:

- Two computers to participate as nodes on the cluster
- Each computer has two network interface cards (NICs): one for the heartbeat function between them, the other for public access

The Tivoli Monitoring requirements for the cluster server are:

- A shared persistent storage for the Tivoli Monitoring installation directory as well as for any component-specific data
- A virtual IP Address to be assigned to the component running on the cluster

Table 10 on page 46 shows the high-level steps required to set up the main Tivoli Monitoring components running in a cluster.

Table 10. Basic steps to set up Tivoli Monitoring on a cluster

Step	Hub monitoring server	Portal Server	Data warehouse
1		Install the database software. Configure the database software for cluster.	Install the database software. Configure the database software for cluster.
2	Create the cluster. Define virtual IP and shared persistent storage for the resource group.	Create the cluster. Define virtual IP, shared persistent storage, and database for the resource group.	Create the cluster. Define virtual IP, shared persistent storage, and database for the resource group.
3	Install and set up the monitoring server on the first node of the cluster. Set up the monitoring server on the second node of cluster.	Install and set up the portal server on the first node of the cluster. Set up the monitoring server on the second node of cluster.	Optional: Install and set up the Summarization and Pruning agent and Warehouse Proxy on the first node of the cluster. Set up the Summarization and Pruning agent and Warehouse Proxy on the second node of the cluster.
4	Add the monitoring server as a resource to the resource group.	Add the portal server as a resource to the resource group.	Optional: Add the Summarization and Pruning agent and Warehouse Proxy as a resource to the resource group.

Some important characteristics of the Tivoli Monitoring setup on a cluster include:

- The shared persistent storage and virtual IP Address must be available before you can install Tivoli Monitoring, and the node where Tivoli Monitoring is being installed must own these resources.
- The Tivoli Monitoring component (such as the hub monitoring server) is installed only once on the first node of the cluster (on the shared directory) and then properly configured on the second node. In the Windows environment this means that the Tivoli Monitoring registry keys must be replicated to the second node.
- The Tivoli Monitoring component has to be bound to the virtual IP Address such that the other Tivoli Monitoring components of the infrastructure can reach it no matter which node it is running on. This is done by setting the network interface where the component listens.
- Only one instance of the component will be active at a time.
- When Tivoli Monitoring is running under the cluster, its services cannot be automatically started. Likewise, its services cannot be directly started or stopped through the command line or through the Manage Tivoli Enterprise Monitoring Services (or administrative GUI). Instead, the services must be controlled through the cluster manager.

Monitoring server setup: The monitoring server cluster resources include:

- Shared persistent storage

- Virtual IP Address
- Monitoring server service

The generic setup of the hub monitoring server on a cluster includes the following task:

1. Set up the basic cluster resource group with a shared persistent storage and virtual IP Address.
2. Install GSKIT, the Java runtime, and the monitoring server on the first node of the cluster or on the shared persistent storage. This depends on which platform you are running on, since IBM Tivoli Monitoring install on Windows allows the specification of a driver and location (so shared persistent storage can be specified) but the UNIX install does not.
3. Remove automatic startup of the monitoring server service (if applicable to this platform).
4. Bind the monitoring server to the virtual IP Address.
5. Set up GSKIT, the Java runtime, and the monitoring server on the second node of the cluster. Depending on the platform, this may involve copying registry keys or environment variables or both to the second node.
6. Add the monitoring server as a resource to the resource group.

Note that the specific setup of the monitoring server varies on different platforms and cluster managers.

Private and public interfaces when Tivoli Enterprise Monitoring Server is installed on an AIX server:

Note: This section applies to clustered environments if the Tivoli Enterprise Monitoring Server is installed on an AIX server.

By default, the location broker registers all available interfaces for a server. Thus, an internal IP address is configured on each node to be used for cluster internal communication between nodes. However, these internal (private) IP addresses should not be included on a list to be used by other servers or agents. If the Tivoli Enterprise Monitoring Server is installed on an AIX server with a public and a private interface, the Tivoli Enterprise Portal Server cannot connect to the Tivoli Enterprise Monitoring Server. There are two environment variables you can set to control which interfaces to publish. For IPV4 use KDEB_INTERFACELIST, for IPV6 use KDEB_INTERFACELIST_IPV6. In either address family, you can set those variables to set, restrict, or add to the interfaces in use. To avoid communication errors, remove the internal IP address registration, as explained in the following table.

Table 11. Control interface publishing

Interface control	Environment variable
To set specific interfaces for consideration:	KDEB_INTERFACELIST=ip4addr-1 ... ip4addr-n KDEB_INTERFACELIST_IPV6=ip6addr-1 ... ip6addr-n
To remove interfaces from consideration:	KDEB_INTERFACELIST...=-ip4addr-1 ... -ip4addr-n KDEB_INTERFACELIST_IPV6=ip6addr-1 ... ip6addr-n
To add interfaces for consideration:	KDEB_INTERFACELIST=+ ip4addr-1 ... ip4addr-n KDEB_INTERFACELIST_IPV6=+ ip6addr-1 ...ip6addr-n

Table 11. Control interface publishing (continued)

Interface control	Environment variable
where: **ip4addr** Specifies either a symbolic network name, or a raw form dotted decimal network address. **ip6addr** Specifies either a symbolic network name, or a raw form colon-separated hex digit network address. **Note:** The plus sign must stand alone.	

Portal server setup: The portal server cluster resources include the following:

- Shared persistent storage
- Virtual IP Address
- Database middleware (such as DB2)
- Portal server service

The generic setup of the portal server on a cluster includes the following tasks, performed in order:

1. Install the database middleware locally on both nodes.
2. Set up the database users and groups to be exactly the same on both nodes.
3. Remove automatic startup of the database middleware, such that it can run under the cluster control.
4. Set up the basic cluster resource group with shared persistent storage, virtual IP Address and the database middleware.
5. Create the portal server database on the first node of the cluster (shared persistent storage).
6. Catalog the portal server database on the second node of the cluster.
7. 7. Install GSKIT, Java runtime, portal server and the IBM Eclipse Help Server on the first node of the cluster (shared persistent storage). Note: The Eclipse Help Server is automatically installed when you install the portal server. 8.
8. Remove auto-start of the portal server service and Eclipse Help Server service (if applicable on this platform). 9.
9. Bind the portal server and Eclipse Help Server to the virtual IP address. 10.
10. Set up GSKit, Java runtime, portal server and Eclipse Help Server on the second node of the cluster (depending on the platform, this may involve copying registry keys or environment variables, or both, to the second node.).
11. Add the portal server and Eclipse Help Server as resources to the resource group. 12.
12. Add the Eclipse Help Server to the resource dependencies of the portal server.

Note that the setup of the portal server varies on different platforms and cluster managers.

Data warehouse setup: The data warehouse cluster resources include the following:

- Shared persistent storage
- Virtual IP Address
- Database middleware, such as DB2
- Warehouse Proxy and Summarization and Pruning agent processes (optional)

The generic setup of the data warehouse on a cluster involves the following tasks, performed in order:

1. Install the database middleware locally on both nodes.
2. Set up the database users and groups to be exactly the same on both nodes.
3. Remove automatic startup of the database middleware, such that it can run under the cluster control.
4. Set up the basic cluster resource group with shared persistent storage, virtual IP address, and the database middleware.
5. Create the data warehouse database on the first node of the cluster (shared persistent storage).
6. Catalog the data warehouse database on the second node of the cluster.

The following steps are optional and only necessary if the Summarization and Pruning agent and the Warehouse Proxy are included in the cluster:

1. Install the Summarization and Pruning agent and the Warehouse Proxy on the first node of the cluster (shared persistent storage).
2. Install GSKIT and Java runtime on both nodes of the cluster (or on the shared persistent storage, depending on the platform)
3. Turn off automatic startup of the Summarization and Pruning agent and Warehouse Proxy services (if applicable to this platform).
4. Bind the Summarization and Pruning agent and the Warehouse Proxy to the virtual IP Address.
5. Set up the Summarization and Pruning agent and Warehouse Proxy on the second node of the cluster (depending on the platform, this might involve copying the registry keys or environment variables or both to the second node).
6. Add the Summarization and Pruning agent and Warehouse Proxy as resources to the resource group.

The specific setup of the data warehouse on different platforms and cluster managers varies and is described on the specific cluster managers on this series.

What to expect from the Tivoli Management Services infrastructure in a clustered environment: In general, the failover or failback of a clustered component is treated by the other Tivoli Monitoring components as a restart of the clustered element.

Clustered hub: When the hub is clustered, its failover/failback is perceived by all the other Tivoli Monitoring components as a hub restart. This means that the other components automatically reconnect to the hub and some synchronization takes place.

As part of the remote monitoring server to hub synchronization after re-connection, all situations that are the responsibility of the remote monitoring server (distributed to the monitoring server itself or to one of its connected agents) are restarted. This restarting of situations represents the current behavior for all re-connection cases between remote monitoring servers and the hub, independent of clustered environments. See “Situations” on page 51 for more information.

For agents directly connected to the hub, there might be a periods in which situation thresholding activity on the connected agents is not occurring because the situations are stopped when a connection failure to the reporting hub is detected. As soon as the connection is reestablished, the synchronization process takes place and situations are restarted. (Note that historical metric collection is not stopped.)

The portal server, the Summarization and Pruning agent, and the Warehouse Proxy reconnect to the hub and perform any synchronization steps necessary.

The portal user's perception of the apparent hub restart depends on the size of the environment (including the number of agents and situations). Initially you are notified that the portal server has lost contact with the monitoring server, and views might be unavailable. When the portal server reconnects to the hub, the Enterprise default workspace displays, allowing access to the Navigator Physical view. However, some agents may have delays in returning online (due to the reconnection timers) and triggering polled situations again (as the situations are restarted by the agents).

While the hub failover or failback (including the startup of the new hub) may be quick (on the order of 1-3 minutes), the resynchronization of all elements to their normal state may be delayed in large-scale environments with thousands of agents. This behavior is not specific to a cluster environment, but valid any time the hub is restarted or when connections from the other Tivoli Monitoring components to the hub are lost and later re-established.

Clustered portal server: When the portal server is clustered, its failover or failback is perceived by its connected Tivoli Monitoring components as a portal server restart. The components that connect to the portal server include the portal consoles and the Summarization and Pruning agent (at the start of its summarization and pruning interval).

When a portal client loses connection to the portal server the user is notified and some views become unavailable. When the portal client re-establishes connection with the portal server, the home workspace displays and the Navigator refreshes.

If the Summarization and Pruning agent is connected to the portal server at the time of portal server failover, it loses the connection and attempts to reestablish contact on the next Summarization and Pruning agent interval.

Clustered data warehouse: When the data warehouse is clustered, its failover/failback is perceived by its connected Tivoli Monitoring components as a database restart. The components that connect to the data warehouse database include the Summarization and Pruning agent, the Warehouse Proxy and portal server (when retrieving long-term data collection for the portal workspace views).

When the Summarization and Pruning agent loses contact with the data warehouse database, it attempts to reestablish contact on the next Summarization and Pruning agent interval and then restart its work.

When the Warehouse Proxy loses contact with the data warehouse database, it attempts to reestablish the connection and restart its work.

When the portal server loses contact with the data warehouse, it reconnects on the next query request from a portal client.

Clustered Summarization and Pruning agent: When the data warehouse cluster resource group includes the clustered Summarization and Pruning agent, the agent fails together with the data warehouse database and must be restarted after the data warehouse. As the Summarization and Pruning agent uses transactions for its operations to the data warehouse database, it resumes its summarization and pruning work where it left off prior to failure.

Clustered Warehouse Proxy: When the Warehouse Proxy is part of the data warehouse cluster resource group, the proxy fails together with the data warehouse database and must be restarted after the data warehouse. The proxy then resumes the work of uploading the short-term data collection to the data warehouse.

Situations: Situations are potentially affected by failures on the hub, the remote monitoring server, and at the agent. During a hub cluster failover, situations are affected in the same way as a restart of the hub or when the hub gets disconnected from the other components.

When a remote monitoring server loses connection with the hub and then reestablishes contact, the server synchronizes after re-connection. This process involves restarting all the situations under that remote monitoring server's responsibility. Polled situations are triggered on the next polling interval, but pure events that were opened before the failure are lost. Use an event management product, such as OMNIbus or Tivoli Enterprise Console, as the focal point for storing and manipulating historical events from all event sources.

If you have agents directly connected to the hub, the situations distributed to them are stopped when connection is lost and the situations are restarted when the agent reconnects to the hub. This behavior also applies for agents that are connected to a remote monitoring server and lose connection to it.

Workflow policies: Workflow policies can be set to run at the hub. If the hub fails over while a workflow policy is running, the processing stops and then restarts at the beginning of the workflow policy (upon restart of the hub and triggering).

Short-term data collection: When a hub failover or failback occurs, any remote monitoring servers and agents reconnect to it, causing all situations to be restarted. Short-term data collection is performed at the agents through special internal situations called UADVISOR. These situations are also restarted and collect data only after the next full interval has passed, resulting in the loss of one collection interval of data.

Long-term data collection: The Warehouse Proxy and Summarization and Pruning agents connect to the hub. After a hub failover/failback occurrs, the proxy and agent reconnect to it without impacting their work on the data warehouse.

Note: Other behavior associated with long-term data collection components when they are clustered is described in the sections above.

Tivoli Event Integration Facility: When Tivoli Monitoring is configured to forward events to the Tivoli Enterprise Console event server or a Netcool/OMNIbus Objectserver, its behavior is to send a "MASTER_RESET" event to the event server every time the hub is restarted. This behavior also occurs after failover/failback for a clustered hub. The purpose of this event is to signal to the event server that the monitoring server restarted all its situations and that the event server will receive a new set of currently triggered situations. The default event synchronization rule for Tivoli Monitoring integration addresses that event by closing all the events that came from this hub monitoring server. Although this behavior guarantees that both Tivoli Monitoring and Tivoli Enterprise Console or Netcool/OMNIbus Objectserver have consistent triggered situations and events, the behavior may not be desirable in some environments. For example, this behavior closes pure events that are not reopened until the next pure event occurs. In such cases, you can filter out the

MASTER_RESET either at the hub (EIF configuration file) or at the event server by using correlation rules. In this case, the rules must handle duplicate events caused by the restarted situations.

Maintenance: The maintenance requirements of Tivoli Monitoring (patches, fix packs or release upgrades) when running in a cluster resembles those of running an unclustered Tivoli Monitoring environment. The cluster controls the starting and stopping of Tivoli Monitoring services. In order to return this control to the install procedure, you must stop the cluster while the maintenance is being performed. Also, due to current restrictions of the Tivoli Monitoring installation procedures, some settings that are completed during Tivoli Monitoring cluster setup might need to be repeated after the maintenance is completed and before the cluster is restarted.

Event integration scenarios

Using the Tivoli Enterprise Portal, you can define monitoring specifications, called *situations*, to detect the occurrence of specific conditions on managed systems. When conditions that match the specifications are detected by monitoring agents, events are reported to the monitoring servers. In environments where IBM Tivoli Enterprise Console or Netcool/OMNIbus are also being used for event management, hub Tivoli Enterprise Monitoring Servers can be configured to forward these situation events to either of these event servers for further correlation and management. Changes in the status of events made on the event server are reported back to the forwarding monitoring server so that events are synchronized on the two event management systems.

The scenarios in this section illustrate how event integration can be implemented with Tivoli Enterprise Console and Netcool/OMNIbus by forwarding situations events. In order to implement these scenarios, hub monitoring servers must be configured to forward events to at least one event server, and the event server must be configured to interpret the events and send updates to the originating monitoring server. A special event synchronization component, the Situation Update Forwarder must be installed on the event server. You can find complete instructions for implementing these scenarios in Chapter 17, “Setting up event forwarding to Tivoli Enterprise Console,” on page 361 and Chapter 18, “Setting up event forwarding to Netcool/OMNIbus,” on page 387.

You cannot forward situation events directly from a hub monitoring server running in z/OS to Netcool/OMNIbus or Tivoli Enterprise Console. However, you can configure monitoring agents running on z/OS to report directly to a hub monitoring server on zLinux or on a distributed system, or to report to a remote monitoring server running on z/OS that reports to a hub on zLinux or a distributed system.

If you prefer to use the Tivoli Enterprise Portal as your principal event management console, you can configure the Tivoli Enterprise Portal Server display events collected from these event servers. For more information, see the *IBM Tivoli Monitoring: Administrator's Guide*.

Event integration with Tivoli Enterprise Console

The scenarios in this section illustrate the various ways to forward situation events from one or more monitoring servers to one or more Tivoli Enterprise Console event servers:

- “One or more hub monitoring servers and a single event server” on page 53
- “A single hub monitoring server and multiple event servers” on page 54

- "Multiple hub monitoring servers and multiple event servers in a hub and spoke configuration" on page 54

Note: If you already have policies that contain emitter activities that send events to the Tivoli Enterprise Console, turning on Tivoli Event Integration event forwarding will result in duplicate events. You can deactivate the emitter activities within policies so you do not have to modify all your policies when you activate Tivoli Event Integration Facility forwarding by using **Disable Workflow Policy/Tivoli Emitter Agent Event Forwarding** when you configure the monitoring server.

Using policies gives you more control over which events are sent and may not want to lose this granularity. Moreover, it is likely the policies that are invoking the Tivoli Enterprise Console emitter are doing little else. If you deactivate these activities, there is no point in running the policy. You may prefer to delete policies that are longer required, instead of disabling them.

One or more hub monitoring servers and a single event server: You can configure one or more monitoring servers to forward situation events to an event server. Figure 12 shows multiple hub monitoring servers that are configured to forward situation events to the same event server. The event server sends situation updates based on Tivoli Enterprise Console® rules and operator actions back to the hub monitoring server that is associated with that situation.

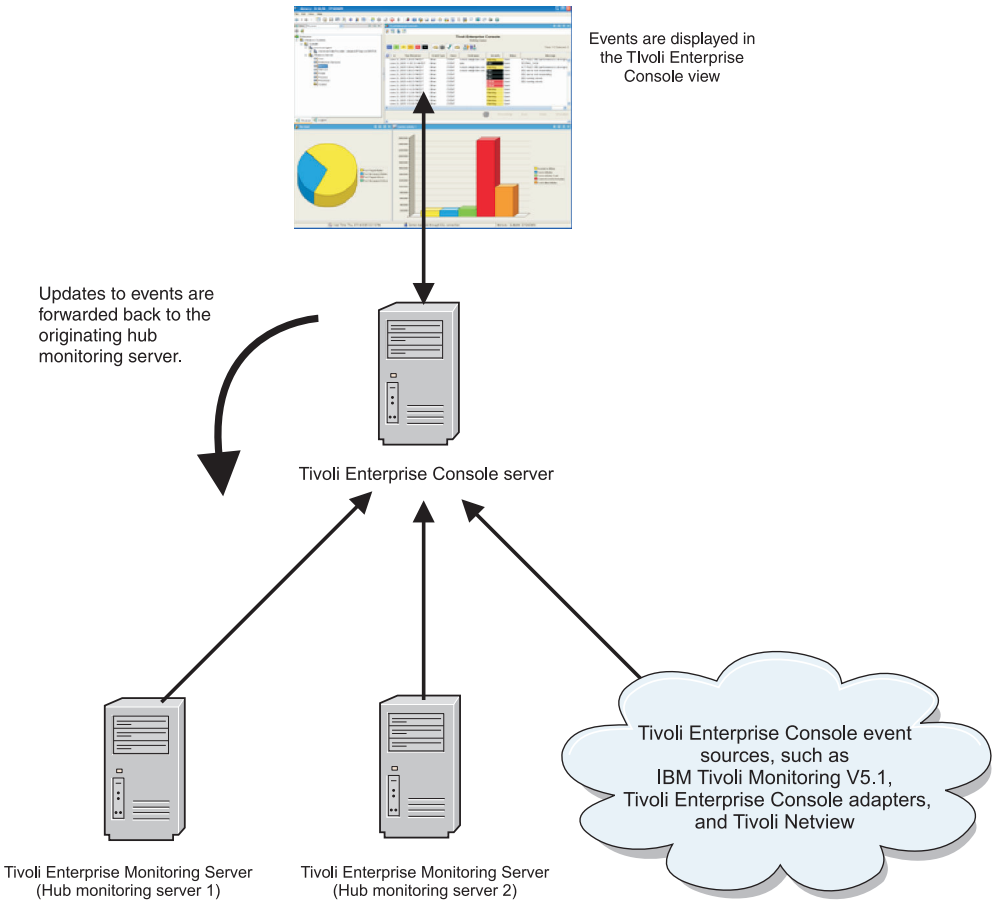


Figure 12. One or more hub monitoring servers connecting to a single event server

A single hub monitoring server and multiple event servers: Figure 13 shows a single hub monitoring server that is configured to forward situation events to multiple event servers. The event servers send situation updates based on Tivoli Enterprise Console rules and operator actions back to the hub monitoring server.

For this configuration, you must install the Tivoli Enterprise Console event synchronization component on each event server, and you must specify each situation event and the event server or servers (see the *IBM Tivoli Monitoring Administrator's Guide*).

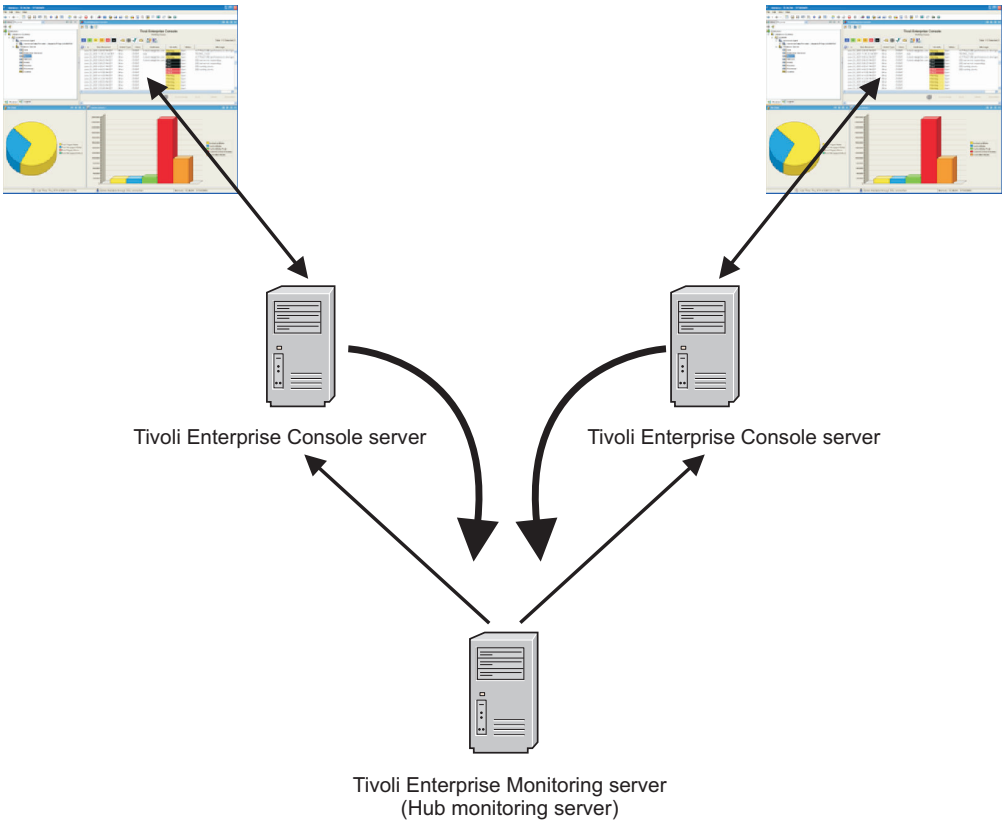


Figure 13. Single hub monitoring server and multiple event servers

Multiple hub monitoring servers and multiple event servers in a hub and spoke configuration: Figure 14 on page 55 shows multiple hub monitoring servers that are configured to forward situation events to an event server that is connected to a hub event server. The hub event server sends situation updates based on Tivoli Enterprise Console rules and operator actions back to the hub monitoring server that is associated with that situation.

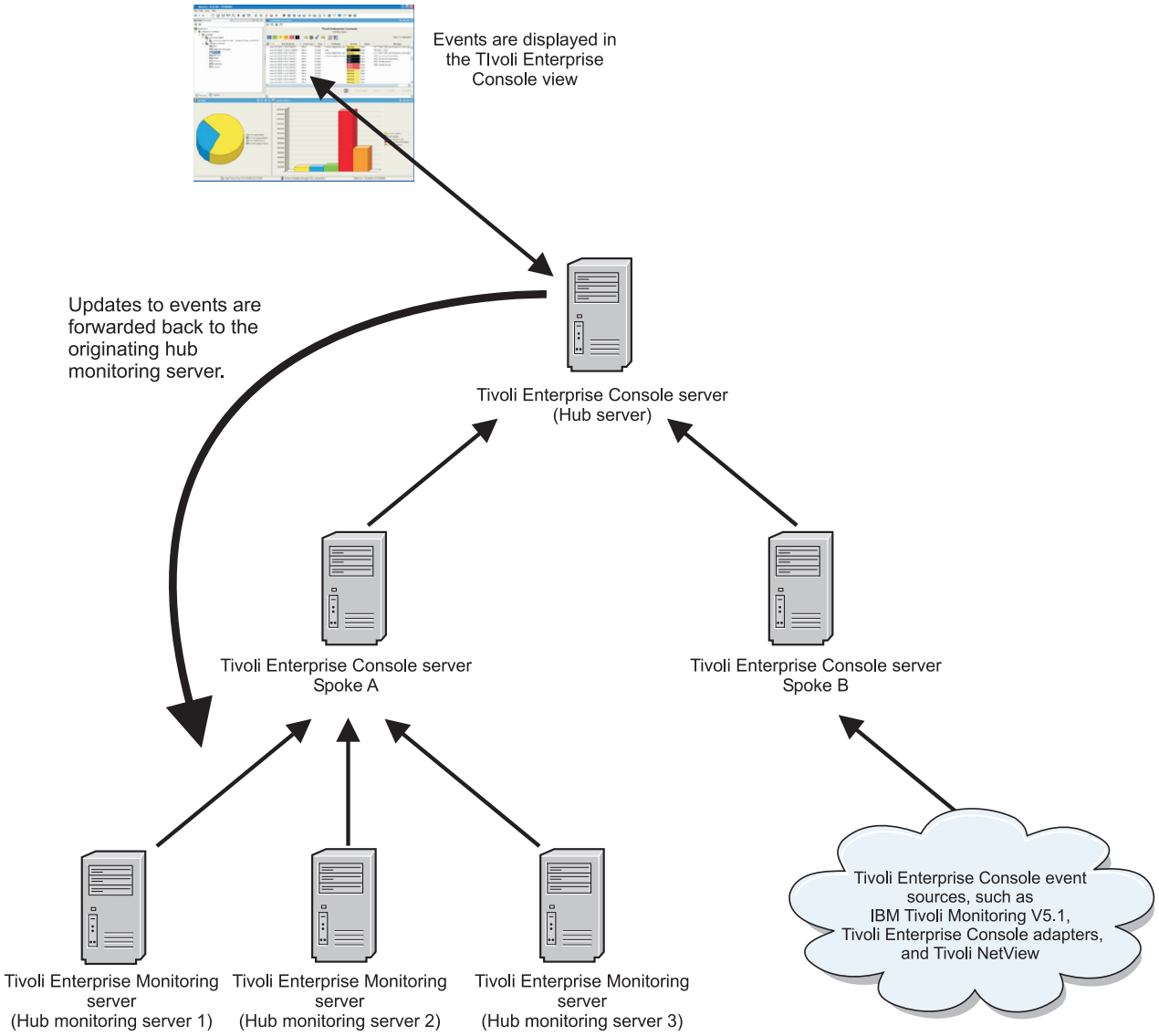


Figure 14. Multiple hub monitoring servers and multiple event servers in a hub and spoke configuration

Note: This graphic is intended to be an example of one possible scaled configuration for the IBM Tivoli Monitoring and Tivoli Enterprise Console integration. The procedures in this chapter do not provide all of the information needed to set up this sort of configuration.

For this configuration, you must install the Tivoli Enterprise Console event synchronization component on the hub event server. You must also load the omegamon.baroc and Sentry.baroc files on the spoke event servers, as described in "Modifying an existing rule base" on page 376. In addition, you must load each .baroc file for any monitoring agent generating situations that are forwarded to spoke event servers, as described in "Installing monitoring agent .baroc files on the event server" on page 377.

Event integration with Netcool/OMNIbus

The scenarios in this section illustrate various ways to forward situation events from one or more monitoring servers to one or more Netcool/OMNIbus

Objectservers (the event server). For complete instructions for implementing these scenarios, see Chapter 18, “Setting up event forwarding to Netcool/OMNIbus,” on page 387.

Monitoring servers use the Tivoli Event Integration Facility (EIF) interface to forward situation events to OMNIbus. The events are received by the Netcool/OMNIbus Probe for Tivoli EIF, which maps them to OMNIbus events and then inserts them into the OMNIbus server. Updates to those events are also sent to OMNIbus. When an OMNIbus user acknowledges, closes, or reopens a forwarded event, OMNIbus sends those changes to back to the monitoring server that forwarded them.

One or more hub monitoring servers and a single event server: You can configure one or more monitoring servers to forward situation events to an event server.Figure 15 shows multiple hub monitoring servers that are configured to forward situation events to the same event server. The event server sends situation updates back to the hub monitoring server that is associated with that situation. Event forwarding must be enabled on each monitoring server, and the EIF probe associated with the Objectserver must be defined as the default EIF receiver.

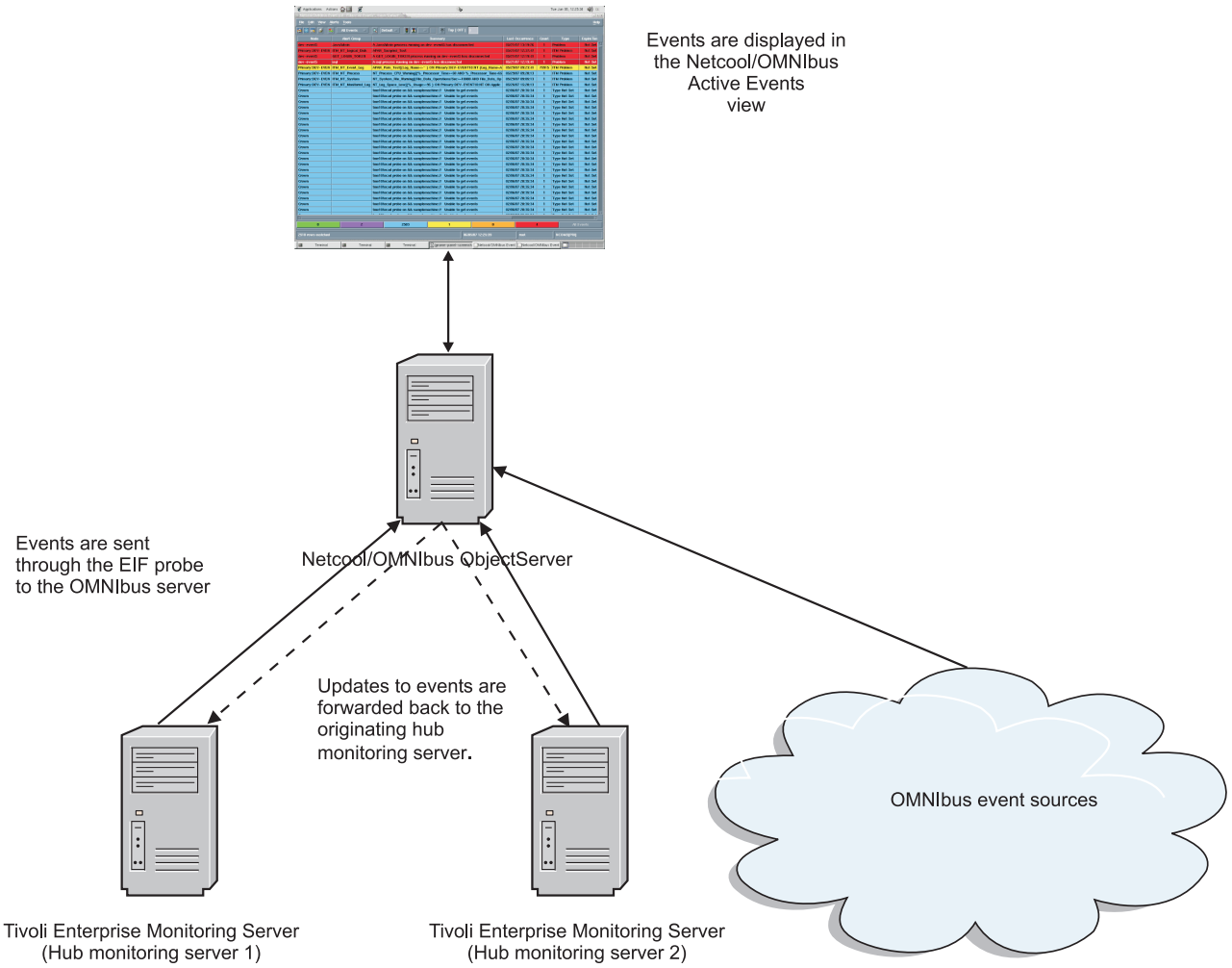


Figure 15. One or more hub monitoring servers connecting to a single event server

A single hub monitoring server and multiple event servers: You can configure one monitoring server to forward situations to different event servers. "A single hub monitoring server and multiple event servers" shows a single hub monitoring server that is configured to forward situation events to multiple event servers. The event servers send situation updates back to the monitoring server from which they were forwarded.

Each event server to which events are forwarded must have an EIF probe associated with it and the event synchronization component installed on it. You must specify for each situation the event server to which the situation event is forwarded. (By default, all situation events are forwarded and all of them are forwarded to the default EIF receiver, which is the probe defined to the monitoring server when event forwarding is enabled.) You must also define additional EIF receivers to the monitoring server. See the *IBM Tivoli Monitoring: Administrator's Guide* for information on defining multiple EIF receivers and customizing event forwarding.



Figure 16. Single hub monitoring server and multiple event servers

Chapter 3. Preparing for installation

The following sections provide information to help you prepare to install your IBM Tivoli Monitoring environment.

Overview of the installation process

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

Table 12. Installation and configuration steps

Step	Where to find detailed information
Assess your monitoring needs to determine the best deployment of IBM Tivoli Monitoring components.	"Assessing the existing environment" on page 14
Ensure you have the required hardware and software.	"Hardware and software requirements" on page 70
Gather any information required for successful installation (such as DB2 user information and security specifications).	"Specific information to have ready" Appendix A, "Installation worksheets," on page 409
Install the Tivoli Enterprise Monitoring Server.	"Installing and configuring the hub Tivoli Enterprise Monitoring Server" on page 114
Install the Tivoli Enterprise Portal Server.	"Installing the Tivoli Enterprise Portal Server" on page 129
Install the management agent software.	"Installing monitoring agents" on page 148
Install support for IBM Tivoli Enterprise Console.	Chapter 17, "Setting up event forwarding to Tivoli Enterprise Console," on page 361
Install the portal desktop client on any system where you want to use it.	"Installing the Tivoli Enterprise Portal desktop client" on page 156
Start the portal client to verify that you can view the monitoring data.	"Starting the Tivoli Enterprise Portal client" on page 188

If you are upgrading from IBM Tivoli Monitoring V6.1 or OMEGAMON Platform 350 or 360 and CandleNet Portal® 195, see Chapter 4, "Upgrading from a previous installation," on page 87 before installing any IBM Tivoli Monitoring components.

If you are upgrading from Tivoli Distributed Monitoring to IBM Tivoli Monitoring, see the *IBM Tivoli Monitoring: Upgrading from Tivoli Distributed Monitoring* guide.

If you are upgrading from IBM Tivoli Monitoring V5.x to V6.2, see *IBM Tivoli Monitoring: Upgrading from V5.1.2*.

If you plan to use firewalls in your environment, see Appendix C, "Firewalls," on page 427 for an overview of the IBM Tivoli Monitoring implementation of firewalls.

Specific information to have ready

During installation, you must supply the following information:

© Copyright IBM Corp. 2005, 2007

- Name of the monitoring server you are installing or to which the agent will connect
- Host name for the computer where you are installing the product (a monitoring server or one instance of an agent)
- Whether the monitoring server being installed or being connected to is configured as a hub or remote monitoring server
- Hub monitoring server host name
- Port number

Use the worksheets in Appendix A, "Installation worksheets," on page 409 to collect this information for each component that you want to install.

Information to gather for event forwarding

You need the following additional information to successfully install and configure event forwarding and synchronization between a hub Tivoli Enterprise Monitoring Server and either IBM Tivoli Enterprise Console or Netcool/OMNIbus:

- Host names, user IDs, and passwords for the monitoring servers that you want to receive events from
- The amount of free space in your temporary directory. The installation requires 200 MB of temporary space.
- Simple Object Access Protocol (SOAP or Web Services) information to send events to a monitoring server (the URL, the rate to send requests to the server).

  By default, all monitoring servers are configured as SOAP servers. If you did not change this configuration to make it unique for your environment, you can accept the default values during the installation.

  If you did change this configuration, use the SOAP information unique to your configuration.
- For TEC, the host of the event server or servers to which events are being forwarded and the port on which it is listening. For Netcool/OMNIbus, the host of the EIF probe and the port on which it is listening.
- For TEC, 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:

  1. For a Windows event server, any existing rule base that you use must indicate a relative drive letter (such as C:\) as part of its associated path. To verify that your existing rule base contains a relative drive letter, run the following command from a bash environment on your event server:

     ```
     wrb -lsrb -path
     ```

     If the returned path includes something like *hostname*:*Rulebase_directory*, with no drive letter (such as C:\), copy the `ESync2000Win32.exe` file from the \TEC subdirectory of the IBM Tivoli Monitoring installation image to the drive where the rule base exists and run the installation from that file.
  2. If you are using a Windows event server, if you have any rule base with an associated path that does not contain a relative drive letter and that has the Sentry2_0_Base class imported, copy the `ESync2000Win32.exe` file from the \TEC subdirectory of the IBM Tivoli Monitoring installation image to the drive where the rule base exists and run the installation from that file.

     To verify if you have any rule bases that have an associated path containing no relative drive letter, run the **wrb -lsrb -path** command as described in the previous note.

To determine if your rule bases have the Sentry2_0_Base class imported, run the following command against all of your rule bases:

```
wrb -lsrbclass rule_base
```

where *rule_base* is the name of the rule base.

Naming your monitoring server

You must decide how the monitoring servers are to be named. In general, create names that are short but meaningful within your environment. Use the following guidelines:

- Each name must be unique. One name cannot match another monitoring server name for its entire length. (For example, ″ibm″ and ″ibmremote″ are unique and permitted.)
- 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.
- Monitoring server naming is case-sensitive on all platforms.

Required order of installation or upgrade of IBM Tivoli Monitoring component products

If any of the following products will be installed on the same computer as monitoring agents, they must be installed before the agent is installed:

- Hub Tivoli Enterprise Monitoring Server
- Remote monitoring server (if necessary)
- Tivoli Enterprise Management Agent Framework
- Tivoli Enterprise Portal Server
- Tivoli Enterprise Portal desktop client

In addition, these products must be installed on at least one computer before the agent can be properly configured.

Windows installation considerations

The following sections provide information about issues unique to Windows installations.

User authority

To install IBM Tivoli Monitoring on a Windows computer, you must have Administrator privileges on that computer. You must also run the IBM Tivoli Monitoring components as a user with Administrator privileges.

Installation using a Citrix client

If you are using a Citrix client to access the IBM Tivoli Monitoring installation program for Windows through Microsoft Windows Terminal Services, you must manually change Terminal Services to install mode before running the installation. To change Terminal Services to install mode, run the **change user /install** command before starting the installation. After installation, run the **change user /execute** command to return Terminal Services to normal mode.

Linux or UNIX installation considerations

The following sections provide information about issues unique to Linux and UNIX installations:

- "Changes in the behavior of the autostart scripts"
- "Create an IBM Tivoli account for installing and maintaining the installation directory" on page 64
- "Host name for TCP/IP network services" on page 64
- "Use of fully qualified path names" on page 64
- "Multiple network interface cards" on page 64
- "Installing into an NFS environment" on page 64
- "Installing into Solaris zones" on page 65
- "Increasing virtual memory" on page 66
- "File descriptor (maxfiles) limit" on page 66

Changes in the behavior of the autostart scripts

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

- In Fix Pack 003, the installation process produced an autostart script with only one entry using a generic `CandleAgent start all` command and users modified this file as needed.
- In Fix Pack 004, the installation process generated individual entries for each application in a particular installation, but the values captured in the file could not be overridden.
- In Fix Pack 005, the multiple entries remain and an override capability has been added.

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

```
su - <USER> -c "ITM_Install_Home/bin/itmcmd agent start <product_code>"
```

Or

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

Where:

USER Is the ID that the application will be started as. By default, *USER* is the owner of the bin directory for the application. For the UNIX Log Alert agent, *USER* is the owner of the *ITM_Install_Home*/*PLAT*/ul/bin directory.

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

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

product_code Is the two-character code for this application. Refer to Appendix D, "IBM Tivoli product codes," on page 437 for a list of the codes for the common components and the base agents. See the documentation for the product for other product codes.

instance Is the instance name required to start this application.

PLAT Is the platform directory where the application is installed.

See "Changes in the behavior of the autostart scripts" on page 62 for more information

Components are started in the order listed in the autostart script. This order is based on the dependencies between components, rather than any logical sequence. If you need to change the order, use the `kcirunas.cfg` file.

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

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

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

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

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

1. Remove the comment indicator (the exclamation point, !) so that the product code item looks like <product_code>.
2. Copy a product code section.
3. Customize the product code section and activate it, rather than create new sections from scratch.

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

Notes:

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

Create an IBM Tivoli account for installing and maintaining the installation directory

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

Note: This does not apply to installing the portal server on Linux. You must use either the root user or the DB2 administrator to install and configure the portal server. You can then use the IBM Tivoli account to run the portal server.

- You can use any valid name.

  You can install the IBM Tivoli Monitoring software as the root user, but you do not have to. If you do not install as a root user, you must follow the steps outlined in "Changing the file permissions for agents" on page 155 after you install any monitoring agents.
- Use the same user to install all components.
- If you are using NFS or a local file system, establish your installation directory according to the guidelines used in your environment.
- Only the Korn shell is supported for the execution of the installation and runtime scripts. Consider using the Korn shell as the default environment for your IBM Tivoli login account.

Host name for TCP/IP network services

TCP/IP network services such as NIS, DNS, and the /etc/hosts file must 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.

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 (do not use 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.

Multiple network interface cards

When more than one network interface card (NIC) exists in the computer on which the monitoring server is installed, you need to identify which NIC to use when specifying the monitoring server name and host name. Additionally, the host name of the system might not match the interface name, even when only one NIC exists. In either of these cases, to establish connectivity between the monitoring server and agents, you must specify an additional variable when configuring the monitoring server or agents. This variable is listed under the **Optional Primary Network Name** option in the configuration windows or during the installation.

If the host of the Tivoli Enterprise Portal Server has more than one NIC, you need to configure an additional interface for each one.

Installing into an NFS environment

IBM supports installing IBM Tivoli Monitoring in NFS environments. Using NFS, you can concentrate your software and data in a specific location, minimizing maintenance, administrative overhead, and disk space.

Although using NFS to support multiple hosts simplifies the maintenance of installed IBM Tivoli products, its use can impact performance. If you are installing into an NFS environment, consider the administrative savings to the possible impact on the performance of your network.

Consider the number of hosts that share a single installation directory, as well as the effects of network congestion and file system performance on the overall response time of your IBM Tivoli products.

NFS also has some trade-offs in how you manage your environment. While you can have your entire IBM Tivoli Monitoring in one place, there might be additional configuration required to define the use of specific products or processes in your installation directory. Will every product on every host system execute using the same configuration; or will you tailor the configuration to the particular environment?

Installing into Solaris zones

There are limitations that must be taken into consideration when installing into zones that share resources.

Big local zones share no resources with other zones, so there are no limitations on installing into a Big Local zone. For local zones that share resources, there are the following limitations:

- Anything installed outside of $CandleHome must:
  - Be installed in the global zone, OR
  - Grant local zone write access to the global zone directory tree
- Any devices used by an agent to obtain statistics must be linked to the Local zone.

The following are the types of zones and the installation possibilities.

Global Zone:

The main administration zone. Both local and remote installation is possible. GSKit installs into the standard location for Solaris, and the links are created in the standard location for Solaris.

Big Local Zone:

A local zone with no shared file system resources. Local and remote installation is possible. GSKit installs into the standard location for Solaris, and the links are created in the standard location for Solaris. These locations are local to this zone and not shared with any other zone.

Small Local Zone:

A local zone with some shared file system resources. Local and remote installation is possible if /opt is not a shared resource. GSKit installs into the standard location for Solaris, but the links are created in the new default location of $CANDLEHOME/gsklinks. These locations are local to this zone and not shared with any other zone.

Default Small Local Zone:

A local zone with the default set of shared file system resources. This is a Small Local Zone with /sbin /lib /usr and /export directories shared with global zone. These directories are read-only file systems in local zone. Local and remote installation is possible. GSKit installs into the standard location for Solaris, but the links are created in the new default location of $CANDLEHOME/gsklinks. These locations are local to this zone and not shared with any other zone.

Small Local Zone with /opt directory shared:

Local and remote installation is not possible. Tivoli Monitoring installation always requires read-write access to the /opt directory. This is not only a GSKit issue. Even if CANDLEHOME is specified as the non-default directory, read-write access to /opt/IBM/ITM/tmaitm6/links is still needed.

Note: In all supported Small Local Zone configurations, the Tivoli monitoring interactive command line installation prompts you for the parent directory where the links will be created. For example, if you enter /tmp for the directory, the links will be created in the /tmp/usr/lib and /tmp/usr/bin directories. The default directory for this prompt is $CANDLEHOME/gsklinks. During remote installation, the default directory is always used.

It is very difficult to predict all the possible "share resources" policies for small local zones and the possible side effects. It is the responsibility of the system administrator to create these policies without causing unintentional side effects between different zones and software installed.

Architecture and product codes

On UNIX and Linux operating systems, some IBM Tivoli Monitoring files are placed in directories whose paths include a code for the platform architecture. You can find the codes for the supported architectures in the registry directory. **archdsc.tbl** contains the architecture codes and descriptions. You can find the product codes and descriptions for supported components and products in the same directory, in **proddsc.tbl**.

Increasing virtual memory

On AIX, the Tivoli Enterprise Portal Server process (KfwServices) is linked with the default memory model, which allows for data and stack of only 256 MB. In large environments, this can cause the portal server to crash at startup. In smaller environments, this may not cause a problem at startup, but may at some later point as more virtual storage is required. The problem can be predicted if the **topas** command shows KfwServices with PgSp value of 180-250 MB. If a smaller environment is close to that value, it may occur when large queries are being handled. If the **topas** output shows that KfwServices is nearing these values, the memory model should be changed in smaller environments as well as large ones.

See "Increasing virtual memory on AIX for large environments" on page 235 for instructions for changing the memory model.

File descriptor (maxfiles) limit

The monitoring server can use a large number of file descriptors, especially in a large environment. On UNIX and Linux systems, the maximum number of file descriptors available to a process is controlled by user limit parameters. To display the user limits, run the following command:

```
ulimit -a
```

The ″nofiles″ parameter is the number of file descriptors available to a process. For the monitoring server process (kdsmain), the ″nofiles″ parameter should be set larger than the maximum number of agents that will be connecting to the monitoring server. If the monitoring server is unable to get file descriptors when needed, unexpected behavior can occur, including program failures. Consider increasing the value to 8000 file descriptors or more.

There are other user limit parameters that control how much data, stack and memory are available to a process. For large environments, consider increasing these memory-related user limit parameters for the monitoring server (kdsmain) process. Configuring the user limit parameters usually requires root access, and involves changing system startup files which are operating system specific. Consult the operating system manuals for information on how to configure the user limit parameters.

Understanding security options

User IDs and passwords sent between Tivoli Management Services components are encrypted by default. All other communication between components can be secured by configuring components to use secure protocols. See "Securing communications between components."

Access to the Tivoli Enterprise Portal is controlled by user accounts (IDs) defined to the Tivoli Enterprise Portal Server. In addition, you can configure the hub monitoring server to validate, or *authenticate*, both user IDs and passwords using either the local system registry or a central LDAP authentication and authorization system. See "Authorizing users to log in to the Tivoli Enterprise Portal" on page 68.

If user validation is *not* enabled on the hub monitoring server, anyone can make requests to the SOAP server. If user validation *is* enabled on the hub, however, the SOAP server honors only requests that supply a valid user ID and password. If type of access is specified for specific users, then only requests from those users for which access is specified are honored. See "Securing the SOAP server" on page 70

Note: The IBM Tivoli Monitoring Service Console enables you to read logs and turn on traces for remote product diagnostics and configuration. The Service Console performs user authentication using the native operating system security facility. This means that if you use the Service Console on z/OS, your user ID and password are checked by the z/OS security facility (such as RACF/SAF). If you use the Service console on Windows, you must pass the Windows workstation user ID and password prompt. A password is always required to access the service console. Even if a user ID is allowed to log in to the operating system without a password, access to the Service Console will be denied. If necessary, you must create a password for the user ID that is being used to log in to the Service Console. For more information about the Service Console, see *IBM Tivoli Monitoring: Problem Determination Guide*.

Securing communications between components

To secure communication between agents, monitoring servers, and the Tivoli Enterprise Portal, use SPIPE as the protocol when you configure communications between the Tivoli Enterprise Portal Server and the hub Tivoli Enterprise Monitoring Server, between hub and remote monitoring servers, and between agents and monitoring servers.

Two additional protocols are used to secure communication between clients and the portal server:

- Secure Hypertext Transport Protocol (HTTPS) to retrieve files and Interoperable Object Reference (IOR). The integrated browser in the client provides HTTPS support on the client side; for the server, consider using a third party web server that supports HTTPS, such as the IBM HTTP Server. See "Configuring an external Web server to work with Tivoli Enterprise Portal" on page 243 for more information.
- Internet Inter-ORB Protocol (IIOP) to secure the communications between the portal server and client. This uses Secure Socket Layer (SSL) provided by VisiBroker. This secure communication uses public key cryptography. See "Using SSL between the portal server and the client" on page 239 for more information.

Global Security Tool Kit

IBM Tivoli Monitoring includes the Global Security Tool Kit (GSKit) for SSL processing as used in SPIPE and HTTPS. GSKit is installed by default on all distributed components, and its utilities are used to create and manage the encryption of data between components through the use of digital certificates.

On z/OS, GSKit is known as the Integrated Cryptographic Service Facility, or ICSF. If ICSF is not installed on the z/OS system, the monitoring server uses an alternative, less secure encryption scheme. Since both components must be using the same scheme, if the hub system does not use ICSF, you must configure the Tivoli Enterprise Portal to use the less secure scheme (EGG1) as well. For more information, see *IBM Tivoli Monitoring: Configuring IBM Tivoli Enterprise Monitoring Server on z/OS*.

A default certificate and key are provided with GSKit at installation. A stash file provides the database password for unattended operation. You can also use the key management facilities in GSKit to generate your own certificates. For more information regarding GSKit and iKeyMan, including information about creating and using security certificates, see the GSKit product documentation located at http://www-1.ibm.com/support/docview.wss?uid=pub1sc32136300.

Authorizing users to log in to the Tivoli Enterprise Portal

Access to the Tivoli Enterprise Portal is controlled by user accounts defined to the portal server. In addition to defining the user IDs that are authorized to log on to the Tivoli Enterprise Portal, these accounts define the permissions that determine which Tivoli Enterprise Portal features a user is authorized to see and use, a list of monitored applications the user is authorized to see, and a list of Navigator views (and the highest level within a view) the user can access. An initial sysadmin user ID with full administrator authority is provided so you can log in to the Tivoli Enterprise Portal and add more user accounts. For information on creating user accounts setting user permissions, see *IBM Tivoli Monitoring: Administrator's Guide*.

If user security is enabled on the hub Tivoli Enterprise Monitoring Server (**Security: Validate User**), a password as well as a user ID is required to log in to the Tivoli Enterprise Portal. Password authentication is controlled by the host of the hub monitoring server. If the hub is configured to authenticate users, when a user logs in to the Tivoli Enterprise Portal, the portal server asks the hub monitoring server to validate the account and sends the encrypted user ID and password. The hub monitoring server validates the account by sending a request to the operating system. For authentication to be performed at the hub, then, Tivoli Enterprise Portal user IDs and associated passwords must be defined on the hub computer. How you configure password authentication depends upon the

operating system where the hub monitoring server is installed (see Table 13).

Table 13. User security configuration method

Operating system of the hub monitoring server	Method of Tivoli Enterprise Portal password authentication
Windows	User accounts
Linux and UNIX	Password files
z/OS	RACF, CA-ACF2, CA-TOP SECRET, or Network Access Method

Note: The terms "authenticate" and "validate" when used for user ID and password purposes are the same. Existing Tivoli Enterprise Monitoring Server code uses the term “validate” for the same purpose as “authenticate” in LDAP and other contexts.

Wait to enable user authentication at the hub monitoring server until you have completed and tested at least a basic installation of Tivoli Management Services components and IBM Tivoli Monitoring base agents. Before you enable user authentication on the hub, at a minimum, add the sysadmin user ID to the network domain user accounts or to the operating system on the host where the hub monitoring server is installed. On Windows, the installation program creates a sysadmin user account and asks you to specify a password for that ID. On other systems, an administrator must create the user account, if it does not already exist.

User authentication using LDAP

When you enable security on the hub monitoring server, you have the option of enabling validation using LDAP instead of the local registry for user authentication.

Note: LDAP is not supported for hub monitoring servers on z/OS.

Before you configure LDAP authentication, the LDAP administrator must create a filter mapping Tivoli Enterprise Portal user IDs to LDAP names. If you intend to use SSL for communications with the LDAP server, a CMS key store and key store stash must be created, using GSKit, and public key certificates imported into either the CMS key store, the LDAP keystore, or both.

A public key certificate is a digital document that associates a user ID with a public key. Digital certificates establish, or certify, the identity of a public key holder. They are issued by a trusted third party, or certificate authority (CA). They contain the key holder’s name, a serial number, a copy of the certificate holder’s public key, and other information such as expiration date of the certificate, and are signed by the CA that issued the certificate.

LDAP user authentication works with the following types of certificates:

- LDAP server certificate from a CA
- Tivoli Enterprise Monitoring Server certificate from CA

If the LDAP at your site requires certificates from a CA, one or both of the following two certificates must be imported into the CMS key store:

- Trusted Root certificate
- LDAP server certificate

The LDAP administrator can tell you which certificates are required.

Some sites also require that monitoring server certificates be used by the LDAP server. The LDAP administrator can tell you if a monitoring server certificate is necessary. If so, one or both of the following two certificates must be imported into the LDAP server and CMS key stores:

- Trusted Root certificate
- Tivoli Enterprise Monitoring Server certificate

See "Creating a new key database" on page 241, "Creating a new public-private key pair and certificate request" on page 241 and "Receiving the CA-signed certificate" on page 242 for more information.

Securing the SOAP server

You can control access to the SOAP server in two ways:

- You can control *who* is permitted to make requests by enabling user authentication on the hub monitoring server.

  If the **Security: Validate User** option is *not* enabled, the SOAP server honors all requests regardless of the sender. If the **Security: Validate User** option on the hub monitoring server is enabled, the SOAP server honors requests only from users defined to the operating system or security authorization facility of the host of the monitoring server.
- You can control *what type of requests* users are permitted to make by configuring the SOAP server.

  If you specify a specific type of access for any users, the SOAP server honors requests only from those users, regardless of whether Security: Validate User is enabled.

For information on configuring the security on the SOAP server, see Chapter 11, "Configuring IBM Tivoli Monitoring Web Services (SOAP Server)," on page 255

Hardware and software requirements

The following sections provide specific information about the memory, software, and hardware requirements for installing IBM Tivoli Monitoring.

Note: This section does not show agent-specific requirements (such as supported application levels or any hardware requirements unique to a certain agent). For this information, see the user's guide (for agents on distributed system) or configuration guide (for agents on mainframe systems) for the agent that you are installing.

Supported operating systems

The following tables show which operating systems are supported for the different IBM Tivoli Monitoring components: monitoring server, portal server, portal client, monitoring agent, Warehouse Proxy, and Warehouse Proxy Summarization and Pruning agent.

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

Note: In the following tables, an X indicates a supported component on the platform. The X is replaced by a bit level specification if the bit level supported for the component differs from that of the platform.

Table 14 shows the support for monitoring components on Windows computers.

Table 14. Supported Windows operating systems

Operating system	Monitoring server	Portal server	Portal client[1]	OS monitoring agent[2]	Warehouse Proxy	Warehouse Summarization and Pruning agent
Windows 2000 Server	X	X	X	X	X	X
Windows 2000 Advanced Server	X	X	X	X	X	X
Windows XP (32 bit)[3]			X	X	X	X
Windows 2003 Server SE (32 bit) with R2 SP2	X	X	X	X	X	X
Windows 2003 Server EE (32 bit) with R2 SP2	X	X	X	X	X	X
Windows Server 2003 Data Center (32 bit) with R2 SP2				X		
Windows 2003 SE (64 bit) with R2 SP2	X	X	X	X	X	X
Windows 2003 EE (64 bit) with R2 SP2	X	X	X	X	X	X
Windows Server 2003 Data Center (64 bit) with R2 SP2				X		
Windows 2003 Server on Itanium2 (IA64) with R2 SP2				X		
Windows Vista Enterprise, Business, and Ultimate (32 bit)[3]			X			
Windows Vista Enterprise, Business, and Ultimate (64 bit)[3]			X			

Notes:

1. The Tivoli Enterprise Portal desktop client is supported on marked platforms. However, the browser client can be accessed only from Windows computers running Internet Explorer 6 or 7.
2. The **OS monitoring agent** column indicates the platforms on which an operating system monitoring agent is supported. This column does not indicate that any agent runs on any operating system. For example, to monitor a Linux computer, you must use a Linux monitoring agent, not a Windows monitoring agent.

   For information about the operating systems supported for non-OS agents, see the documentation for the specific agents you are using in your environment.
3. For the Windows XP and Windows Vista operating systems, the Microsoft® End User License Agreement (EULA) does not license these operating systems to function as a server. Tivoli products that function as a server on these operating systems are supported for demonstration purposes only.

Table 15 shows the support for monitoring components on UNIX (non-Linux), i5/OS®, and z/OS computers.

Table 15. Supported UNIX, i5/OS, and z/OS operating systems

Operating system	Monitoring server	Portal server	Portal client	OS monitoring agent[1, 2]	Warehouse Proxy[3]	Warehouse Summarization and Pruning agent
AIX® V5.2 (32 bit)[4]	X			X		X
AIX V5.2 (64 bit)[4]	(32 bit)			X		(32 bit)

Table 15. Supported UNIX, i5/OS, and z/OS operating systems (continued)

Operating system	Monitoring server	Portal server	Portal client	OS monitoring agent[1, 2]	Warehouse Proxy[3]	Warehouse Summarization and Pruning agent
AIX V5.3 (32 bit)[4]	X	X		X	X	X
AIX V5.3 (64 bit)[4]	(32 bit)	(32 bit)		X	X	(32 bit)
Solaris Operating Environment V8 (SPARC) (32/64 bit)[5]				X		
Solaris V9 (SPARC) (32/64bit)[6]	(32 bit)			X		(32 bit)
Solaris V10 (SPARC) (32/64 bit)	(32 bit)			X		(32 bit)
Solaris V10 (x86-64) (64 bit)	(32 bit)			X		
Solaris Zones[7]	(32 bit)			X		(32 bit)
HP-UX 11i v1 (B.11.11) (32/64) on PA-RISC[11]				X		
HP-UX 11i v2 (B.11.23) (64 bit) on PA-RISC				X		
HP-UX 11i v3 (B.11.31) (64 bit) on PA-RISC				X		
HP-UX 11i v2 (B.11.23) on Integrity (IA64)[10]	X			X	X	X
HP-UX 11i v3(B.11.31) on Integrity (IA64)[10]	X			X	X	X
i5/OS 5.3 (64 bit)				X		
i5/OS 5.4 (64 bit)				X		
z/OS 1.6 (31/64 bit)[8,9]	(31 bit)			X		
z/OS 1.7 (31/64 bit)[8,9]	(31 bit)			X		
z/OS 1.8 (31/64 bit)[8,9]	(31 bit)			X		
z/OS 1.9 [8,9]	(31 bit)			X		

Table 15. Supported UNIX, i5/OS, and z/OS operating systems (continued)

Operating system	Monitoring server	Portal server	Portal client	OS monitoring agent[1, 2]	Warehouse Proxy[3]	Warehouse Summarization and Pruning agent

Notes:

1. The **OS monitoring agent** column indicates the platforms on which an operating system monitoring agent is supported. This column does not indicate that any agent runs on any operating system. For example, to monitor a Linux computer, you must use a Linux monitoring agent, not a Windows monitoring agent.

   For information about the operating systems supported for non-OS agents, see the documentation for the specific agents you are using in your environment.
2. If you are installing the OMEGAMON XE for Messaging agent on a 64-bit operating system, you must install the 32-bit version of the agent framework.
3. Configuration of the Warehouse Proxy agent requires an X Window System (also known as the X11 GUI) on the computer where you are configuring it. Alternatively, you can run the following command to utilize an X terminal emulation program (such as Cygwin) that is running on another computer:

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

   where *my_windows_pc_IP_addr* is the IP address of a computer that is running an X terminal emulation program.
4. Supported AIX systems must be at the required maintenance level for IBM Java 1.5. Refer to the following Web site for the Java 5 AIX maintenance level matrix: http://www-128.ibm.com/developerworks/java/jdk/aix/service.html . Component xlC.aix50.rte must be at 8.0.0.4. See the following Web site for installation instructions: http://www-1.ibm.com/support/docview.wss?uid=swg1IY84212. Version 8 of the AIX XL C/C++ runtime must be installed. To determine the current level, run the following AIX command:

   ```
   lslpp -l | grep -i xlc
   ```

   For the Tivoli Enterprise Portal server, AIX 5.3 must be at TL5.
5. Solaris V8 32-bit requires patches 108434-17 and 109147-07. Solaris V8 64-bit requires 108435-17 and 108434-17. Both 32-bit and 64-bit versions require 111721-04.
6. Solaris V9 32-bit requires patch 111711-11. Solaris V9 64-bit requires 111712-11 and 111711-11. Both 32-bit and 64-bit versions require 111722-04.
7. There are some limitations on installing into Solaris 10 when zones are configured. See "Installing into Solaris zones" on page 65.
8. For information about installing the monitoring server on z/OS, refer to the program directory that comes with that product.
9. The OS monitoring agent for z/OS computers is part of the IBM Tivoli OMEGAMON for z/OS product.
10. You cannot upgrade either the OS or Log Alert agents that you currently have running on an HP-UX 11i v2 (B.11.23) on an Integrity (IA64) computer in PA-RISC mode prior to Fix Pack 4. Fix Packs prior to Fix Pack 4 did not run in native 64-bit mode by default. You must first uninstall the agent if the version is previous to the Fix Pack 4 version.
11. The 32-bit kernel still requires a 64-bit processor. Ensure that any HP-UX managed system is based on PA-RISC2 architecture. From the native kernel mode (for example, 64-bit if the system is 64-bit based), run the following command:

    ```
    file /stand/vmunix
    ```

    This returns the native architecture type. For example:

    ```
    /stand/vmunix:  PA-RISC1.1 executable -not stripped
    ```

    Verify that that architecture as at least PA-RISC2.

Table 16 on page 74 shows the monitoring components supported on Linux operating systems.

Table 16. Supported Linux operating systems

Operating system	Monitoring server	Portal server	Portal client[1]	OS monitoring agent[2, 5]	Warehouse Proxy[3]	Warehouse Summarization and Pruning agent
Asianux 2.0 for Intel® (32 bit)	X	X	X	X	X	X
Asianux 2.0 IA64				X		
Asianux 2.0 on x86-64				X		
Red Flag 4.1 for Intel (32 bit)	X	X	X	X	X	X
RedHat Enterprise Linux 2.1 Intel (32 bit)				X		
RedHat Enterprise Linux 3 on Intel (32 bit)				X		
RedHat Enterprise Linux 3 on zSeries® (31 bit)				X		
RedHat Enterprise Linux 3 on zSeries® (64 bit)				X		
RedHat Enterprise Linux 4 Intel (32 bit)	X	X	X	X	X	X
RedHat Enterprise Linux 4 on x86-64 (64 bit)	(32 bit)			X		
RedHat Enterprise Linux 4 on Itanium® (64 bit)				X		
RedHat Enterprise Linux 4 on iSeries™ and pSeries				X		
RedHat Enterprise Linux 4 on z/Series (31-bit)	X	X		X	X	X
RedHat Enterprise Linux 4 on zSeries® (64 bit)	(31 bit)	(31 bit) [4]		X	(31 bit)	(31 bit)
RedHat Enterprise Linux 5 Intel (32 bit)[6]	X	X	X	X	X	X
RedHat Enterprise Linux 5 on x86-64[6]	(32 bit)			X		
RedHat Enterprise Linux 5 on Itanium 64-bit[6]				X		
RedHat Enterprise Linux 5 on iSeries and pSeries[6]				X		
RedHat Enterprise Linux 5 on z/Series (31 bit)[6]	X	X		X	X	X
RedHat Enterprise Linux 5 on zSeries (64 bit)[6]	(31 bit)	(31 bit)[4]		X	(31 bit)	(31 bit)
SUSE Linux Enterprise Server 8 Intel (32 bit)				X		
SUSE Linux Enterprise Server 8 for z/Series (31 bit)				X		
SUSE Linux Enterprise Server 8 for z/Series (64-bit)				X		
SUSE Linux Enterprise Server 9 Intel (32 bit)	X	X	X	X	X	X

Table 16. Supported Linux operating systems (continued)

Operating system	Monitoring server	Portal server	Portal client[1]	OS monitoring agent[2, 5]	Warehouse Proxy[3]	Warehouse Summarization and Pruning agent
SUSE Linux Enterprise Server 9 on x86-64 (64 bit)				X		
SUSE Linux Enterprise Server 9 on Itanium (64 bit)				X		
SUSE Linux Enterprise Server 9 for iSeries and pSeries®				X		
SUSE Linux Enterprise Server 9 for z/Series (31 bit)	X	X		X	X	X
SUSE Linux Enterprise Server 9 for z/Series (64 bit)	(31 bit)	(31 bit)[4]		X	(31 bit)	(31 bit)
SUSE Linux Enterprise Server 10 Intel (32 bit)	X	X	X	X	X	X
SUSE Linux Enterprise Server 10 on x86-64 (64 bit)				X		
SUSE Linux Enterprise Server 10 on Itanium (64 bit)[4]				X		
SUSE Linux Enterprise Server 10 for iSeries and pSeries (64 bit)				X		
SUSE Linux Enterprise Server 10 for z/Series (64 bit)[4]	(31 bit)	(31 bit)[4]		X	(31 bit)	(31 bit)

Table 16. Supported Linux operating systems (continued)

Operating system	Monitoring server	Portal server	Portal client[1]	OS monitoring agent[2, 5]	Warehouse Proxy[3]	Warehouse Summarization and Pruning agent

Notes:

1. The Tivoli Enterprise Portal desktop client is supported on marked platforms. However, the browser client can be accessed only from Windows computers running Internet Explorer 6 or 7.
2. The **OS monitoring agent** column indicates the platforms on which an agent is supported. This column does not indicate that any agent runs on any operating system. For example, to monitor a Linux computer, you must use a Linux monitoring agent, not a Windows monitoring agent. An "X" symbol in the column indicates that an operating system agent is available for the specific operating system that is named in the row where the "X" is located.
3. Configuration of the Warehouse Proxy agent requires an X Window System (also known as the X11 GUI) on the computer where you are configuring it. Alternatively, you can run the following command to utilize an X terminal emulation program (such as Cygwin) that is running on another computer:

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

   where *my_windows_pc_IP_addr* is the IP address of a computer that is running an X terminal emulation program.
4. You must install the Tivoli Enterprise Portal Server and its IBM DB2 database in a 31-bit mode session. Each time you start the Tivoli Enterprise Portal Server, you must be in a 31-bit mode session. To enter a 31-bit mode session, type `s390 sh` at the command line. The s390 command is included in the s390-32 rpm package and the 31-bit libraries.

   SUSE Linux Enterprise Server 9 must be at SP3 or higher. SUSE 10 must be at pdksh-5.2.14 or higher.
5. The Linux OS Monitoring Agent requires the installation of the latest versions of the following libraries:

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

   These libraries are available on the Linux operating system installation media and Service Packs. Each library could have multiple packages, and each should be installed.
6. Red Hat Enterprise Linux 5 now enables SELinux by default, which interferes with the normal operations of IBM Tivoli Monitoring. To ensure the proper operations of V6.2, the SELinux setting must be changed from ″enforcing″ mode to either ″permissive″ or ″disabled″ mode. When the ″permissive″ mode is chosen, the system log will contain entries regarding which Tivoli Monitoring binaries have triggered the SELinux security condition. However, under the ″permissive″ mode, these entries are for auditing purpose only, and will operate normally.

The following table lists the operating system patches required for the IBM Global Security Toolkit (GSKit), which is used to provide security between monitoring components. GSKit is installed automatically when you install Tivoli Management Services components.

Table 17. Operating system requirements for IBM GSKit

Operating system	Patch required
Solaris V8	108434-14, 111327-05, 108991, 108993-31, 108528-29, 113648-03, 116602-01, 111317-05, 111023-03, 115827-01
Solaris V9	111711-08
Solaris V10	none
HP-UX V11i	PHSS_26946, PHSS_33033
AIX V5.x	xlC.aix50.rte.6.0.0.3 or later
Windows Server 2003	none
RedHat Enteprise Linux 2.1 Intel	pdksh-5.2.14-13.i386.rpm
RedHat Enterprise Linux 4 Intel	compat-gcc-32-c++-3.2.3-46.1.i386.rpm compat-gcc-32-3.2.3-46.1.i386.rpm compat-libstdc++-33-3.2.3-46.1.i386.rpm
SUSE Linux Enterprise Server 8 Intel	none
SUSE Linux Enterprise Server 9 Intel	none

Supported databases for Tivoli Enterprise Portal Server and Tivoli Data Warehouse

The following tables show the supported databases for the portal server and the Tivoli Data Warehouse.

Table 18 shows the supported databases for the portal server. Note that the database and the portal server must be installed on the same computer.

Note: IBM provides a restricted-use version of DB2 UDB Enterprise Edition V9.1 for use with the portal server and the Tivoli Data Warehouse. Each instance of the database must be registered. See "Registering the DB2 product license key using the db2licm command" on page 79 for instructions.

Table 18. Supported databases for the portal server

Portal server operating system	Portal server database ("TEPS")[1, 2, 3]	
	IBM DB2 UDB[4]	MS SQL
AIX	V8.1 with Fix Pack 10 or higher fix packs V8.2 with Fix Pack 3 or higher fix packs V9.1 and fix packs[7, 8]	
Linux[5]	V8.1, with Fix Pack 10 or higher fix packs V8.2 with Fix Pack 3 or higher fix packs V9.1 and fix packs[7]	

Table 18. Supported databases for the portal server (continued)

Portal server operating system	Portal server database ("TEPS")[1, 2, 3]	
	IBM DB2 UDB[4]	**MS SQL**
Windows	V8.1, with Fix Pack 10 or higher fix packs V8.2 with Fix Pack 3 or higher fix packs V9.1 and fix packs	MS SQL 2000 SP3[6]

Notes:

1. "TEPS" is the default database name for the database used by the portal server.
2. Support is for 32-bit and 64-bit databases.
3. Your portal server database must be located on the computer where the portal server is installed.
4. If, in your environment, you are using products whose licenses require you to collect software use information and report it to IBM using IBM Tivoli License Manager, you must ensure that use of this instance of IBM DB2 is not included in the report. To do this, create a Tivoli License Manager license, selecting a license type that does not involve reporting to IBM, and associate this instance of the product with it.
5. On Linux, the portal server database must be installed with the operating system language set to UTF-8.
6. IBM Tivoli Monitoring supports MS SQL Server 2000 only if the data is limited to codepoints inside the Basic Multilingual Plane (range U+0000 to U+FFFF). This restriction does not apply to IBM DB2.
7. Requires an installation workaround that is described in APAR IY95415.
8. If you are using 64-bit DB2 9.1 on zSeries Linux, you must modify the /<*install_dir*>/config/cq.ini file by changing the $DB2DIR$/lib value in LD_LIBRARY_PATH and SHLIB_PATH to $DB2DIR$/lib32 or adding $DB2DIR$/lib32 before $DB2DIR$/lib.

Table 19 shows the supported databases for the Tivoli Data Warehouse.

Table 19. Supported databases for the Tivoli Data Warehouse

Tivoli Data Warehouse database ("WAREHOUS")[1, 2]		
IBM DB2	**MS SQL[3]**	**Oracle[4]**
IBM DB2 UDB V8.1, Fix Pack 10 and higher fix packs, V8.2, Fix Pack 3 and higher fix packs, and V9.1 and fix packs on the following operating systems:[4] • AIX V5.3 • HP-UX 11iv3 • Solaris 10 • Windows 2003 Server • SUSE Linux Enterprise Server 9 for Intel and zSeries • SUSE Linux Enterprise Server 10 for Intel and zSeries[6] • RedHat Enterprise Linux 4 for Intel and zSeries • RedHat Enterprise Linux 5 for Intel and zSeries[6]	MS SQL 2000 **EE**[5] MS SQL 2005	Oracle V9.2, 10g Release 1, and 10g Release 2 on the following operating systems: • AIX V5.3 • HP-UX 11iv3 • Solaris 10 • Windows 2003 Server • SUSE Linux Enterprise Server 9 for Intel • SUSE Linux Enterprise Server 10 for Intel • RedHat Enterprise Linux 4 for Intel • RedHat Enterprise Linux 5 on Intel and zSeries

Table 19. Supported databases for the Tivoli Data Warehouse (continued)

Tivoli Data Warehouse database ("WAREHOUS")[1, 2]		
IBM DB2	**MS SQL[3]**	**Oracle[4]**

Notes:

1. "WAREHOUS" is the default database name for the database used by Tivoli Data Warehouse. Support is for 32-bit or 64-bit databases. Your Tivoli Data Warehouse database can be located on the same computer as your portal server or on a remote computer.
2. If, in your environment, you are using products whose licenses require you to collect software use information and report it to IBM using IBM Tivoli License Manager, you must ensure that use of this instance of IBM DB2 is not included in the report. To do this, create a Tivoli License Manager license, selecting a license type that does not involve reporting to IBM, and associate this instance of the product with it.
3. See the Oracle company support Web site (www.oracle.com) for information about installing and configuring Oracle on Solaris V10.
4. Do not use DB2 V9.1 Fixpack 2 for the Tivoli Data Warehouse. Use of DB2 V9.1 FP2 can cause the Warehouse Proxy Agent and the Summarization and Pruning Agent not to function properly. Use an earlier version, such as DB2 V9.1 Fix Pack 1, or upgrade to a level which contains the fix for APAR JR26744, such as DB2 V9.1 Fix Pack 3.
5. IBM Tivoli Monitoring supports MS SQL Server 2000 only if the data is limited to code points inside the Basic Multilingual Plane (range U+0000 to U+FFFF). This restriction does not apply to IBM DB2.
6. Limitations with respect to the korn shell of newer Linux operating systems require a workaround for monitoring agents on SUSE Linux Enterprise Server 10 and RedHat Enterprise Linux 5. Upgrades fail for IBM Tivoli Monitoring components on the following Linux operating systems: SUSE Linux Enterprise 10 (SLES 10) and RedHat Enterprise Linux 5 (RHEL 5). This problem is related to the implementation of the korn shell in those releases. You can replace the default korn shell with the korn shell used in the previous release, SLES 9 and RHEL 4 respectively. The previous shell is distributed in the **pdksh** package. You must perform a forced installation of the package, using the **force** option and the **nodeps** (no dependency) option. The following is an example command that installs the package on SLES10:

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

   Note that if you wrote scripts in the korn shell for a SLES 10 or RHEL 5 operating system, moving to the older korn shell might affect those scripts.

Registering the DB2 product license key using the db2licm command

The DB2 product uses the license key information contained in the nodelock file. The nodelock file is created or updated by running the **db2licm** command and specifying the license file for the DB2 product. Creating or updating the nodelock file is referred to as registering the DB2 product license key. You must register the DB2 product license key by running the **db2licm** command on each computer where DB2 is installed. If you want the product or feature license key added automatically during the installation, you need to copy the license key to the `/db2/license` directory of the installation image before launching the DB2 Setup wizard.

The Tivoli Monitoring V6.2 license file is named `db2ese_o.lic.txt`, and is located in the root of your Tivoli Monitoring V6.2 installation media for a mounted DVD or CD (for example `D:\db2ese_o.lic.txt` or `/mnt/cdrom/db2ese_o.lic.txt`), or the directory you downloaded the software to (for example, `/files/downloaded_ITM_6.2/db2ese_o.lic.txt` or `e:\files\downloaded_ITM_6.2\db2ese_o.lic.txt`).

To register the license key, follow the instructions at the following location on the DB2 Information Center, substituting the location of the Tivoli Monitoring license

for the location in the example command: http://publib.boulder.ibm.com/infocenter/db2luw/v9/topic/com.ibm.db2.udb.uprun.doc/doc/t0006749.htm.

Required hardware for distributed systems

The following sections describe the processor, disk, memory, and other hardware requirements for the IBM Tivoli Monitoring infrastructure components on distributed systems. A *distributed system* is defined here as any hardware that is not zSeries.

Following is a list of the IBM Tivoli Monitoring components covered in this section:

- Hub monitoring server
- Remote monitoring server
- Portal server
- Portal client
- Tivoli Data Warehouse
- Warehouse Proxy agent
- Summarization and Pruning agent

Processor requirements

For best performance, processor speeds should be at least 1 GHz for RISC architectures and 2 GHz for Intel architectures. Choosing faster processors should result in improved response time, greater throughput and lower CPU utilization.

Except for the Tivoli Data Warehouse, single processor systems are suitable when an IBM Tivoli Monitoring infrastructure component is installed on a separate computer from the other components. The infrastructure components (monitoring server, portal server, portal client) run as multithreaded processes and are able to run threads concurrently across multiple processors if they are available. CPU utilization for most components is bursty, and steady state CPU utilization is expected to be low in most cases. For components supporting large environments, using multiprocessor systems can improve throughput.

You should also consider using multiprocessor systems in the following scenarios:

- You want to run the Tivoli Enterprise Portal client on a computer that is also running one of the server components.
- You have a monitoring environment of 1000 or more monitored agents, and you want to install multiple server components on the same computer. For example:
  - Portal server and hub monitoring server
  - Monitoring server (hub or remote) and Warehouse Proxy agent
  - Warehouse Proxy and Summarization and Pruning agents
- You have a small environment and you want to include all of the server components (monitoring server, portal server, Warehouse Proxy agent, and Summarization and Pruning agent) on a single computer.
- Except in very small environments, use a multiprocessor system for the Tivoli Data Warehouse database server. You can run the Warehouse Proxy agent and the Summarization and Pruning agent on the Warehouse database server to eliminate network transfer from the database processing path:
  - If you install the Warehouse Proxy agent on the Warehouse database server, consider using a two-way or four-way processor.
  - If you install the Summarization and Pruning agent on the Warehouse database server (with or without the Warehouse Proxy agent), consider using

a four-way processor. For large environments where more CPU resources might be needed, you can run the Summarization and Pruning agent on a computer separate from the Warehouse database server. In this case, ensure that a high-speed network connection exists (100 Mbps or faster) between the Summarization and Pruning agent and the database server.

Memory and disk requirements

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

Table 20. Estimated memory and disk storage for IBM Tivoli Monitoring components on distributed systems

Component	Process memory requirements[1]		Disk storage requirements[4]
	Small environment[2]	Large environment[3]	
Hub monitoring server	70 MB	400 MB	650 MB[5]
Remote monitoring server	100 MB	400 MB	600 MB[5]
Portal server	100 MB[6]	600 MB[6]	800 MB
Portal client (browser or desktop)	150 MB	300 MB	150 MB
Tivoli Data Warehouse	2 - 4 GB depending on database configuration parameters	4 - 8 GB depending on database configuration parameters	See "Estimating the required size of your database" on page 19.
Warehouse Proxy agent	100 MB	200 MB	150 MB
Summarization and Pruning agent	100 MB	200 MB	150 MB

Notes:

1. The memory and disk sizings shown in this table are the amounts required for the individual component beyond the needs of the operating system and any concurrently running applications.
2. A small environment is considered to be a monitoring environment with 500 to 1000 agents, with 100 to 200 monitored agents per remote monitoring server.
3. A large environment is considered to be a monitoring environment with 3000 or more monitored agents, with 500 to 1500 monitored agents per remote monitoring server.
4. The disk storage estimates apply to any size monitoring environment and are considered high estimates. The size of log files affect the amount of storage required.
5. The storage requirements for the hub and remote monitoring servers do not include storage for the agent depot, which can require an additional 1 GB or more.
6. The memory requirement for the portal server does not include database processes for the portal server database, which require up to 400 MB of additional memory, depending on configuration settings.

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

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

Additional requirements

- The best network connection possible is needed between the hub monitoring server and portal server and also between the Tivoli Data Warehouse, Warehouse Proxy agent, and Summarization and Pruning agent.
- A video card supporting 64,000 colors and 1024 x 768 resolution is required for the portal client.

Required hardware for System z

The Tivoli Enterprise Monitoring Server can be installed on either a z/OS or Linux operating system running on System z hardware. The Tivoli Enterprise Portal Server is supported on Linux for zSeries, but not z/OS. The supported product versions for z/OS and Linux for zSeries are listed in Table 15 on page 71.

The following paragraphs summarize the hardware requirements for IBM Tivoli Monitoring components that run on zSeries:

- Tivoli Enterprise Monitoring Server on z/OS

  The Tivoli Enterprise Monitoring Server can run on any zSeries hardware that supports z/OS V1.6 or later. A detailed description of hardware requirements for a monitoring server on z/OS 1.6 or later, including storage requirements, is documented in the *Program Directory for IBM Tivoli Monitoring Services* (GI11-4105).

- Tivoli Enterprise Monitoring Server or Tivoli Enterprise Portal Server on Linux for zSeries

  Any zSeries hardware provides adequate processing capability for a monitoring server or portal server running on Linux for zSeries. For memory and disk requirements, use the figures shown in Table 20 on page 81.

Required software

The following table lists the software required for IBM Tivoli Monitoring.

Table 21. Required software for IBM Tivoli Monitoring

Product	Supported version	Component where the software is required				
		Monitoring server	Portal server	Portal desktop client	Portal browser client	Monitoring agent
IBM Runtime Environment for Java™	JRE V1.5	X	X	X[1]	X	
For Linux computers: a Korn shell interpreter	pdksh-5.2.14	X	X	X		
For RedHat Enterprise Linux 4.0 computers: libXp.so.6 (available in xorg-x11-deprecated-libs)						X
AIX only: xlC Runtime Environment (required for GSkit). Component xlC.aix50.rte must be at 8.0.0.4.		X				
AIX only: Version 8 of the XL C/C++ runtime						X

Table 21. Required software for IBM Tivoli Monitoring (continued)

Product	Supported version	Component where the software is required				
		Monitoring server	**Portal server**	**Portal desktop client**	**Portal browser client**	**Monitoring agent**
Microsoft Internet Explorer	V6.0 or V7.0 with all critical Microsoft updates applied	X			X	
Database[1]	A supported RDBMS is required for the Tivoli Enterprise Portal Server and the Tivoli Data Warehouse. Supported database platforms for the portal server are listed in Table 18 on page 77. Supported database platforms for the Tivoli Data Warehouse are listed in Table 19 on page 78. Each database requires a driver. For detailed information, see Chapter 12, "Tivoli Data Warehouse solutions," on page 265 and subsequent chapters about the Tivoli Data Warehouse.					
IBM Tivoli Enterprise Console	Version 3.9 with Fix Pack 06					
For TCP/IP communication: • Windows 2000 Professional or Server with Service Pack 3 or above • Microsoft Winsock v1.1 or later • Microsoft TCP/IP protocol stack		X	X	X	X	
For SNA communication: • Windows 2000 Professional or Server with Service Pack 3 or above • Microsoft SNA Server V3.0 or later • IBM Communications Server V5.0 or 5.2	Microsoft SNA Server V4.0 requires Service Pack 1. IBM Communications Server V5.0 requires fixes JR10466 and JR10368.	X				

1. If the JRE is not installed on the computer on which the browser is launched, you are prompted to download and install it. The Windows user account must have local administrator authority to download and install the JRE.

Required software for event integration with Netcool/OMNIbus

The following products must be installed and configured before you install event synchronization and configure event forwarding for Netcool/OMNIbus:

- Netcool/OMNIbus V7.x
- Netcool/OMNIbus V7.x probe for Tivoli EIF

- IBM Tivoli Monitoring V6.2

Part 2. Installation and initial configuration of base components and agents

The chapters in this section provide instructions for installing and configuring base components and agents. If you are installing Tivoli Monitoring for the first time, review the chapters in the preceding section before you use the chapters in this section.

Chapter 4, "Upgrading from a previous installation," on page 87, provides instructions for upgrading an existing installation of OMEGAMON Platform 350/360 or IBM Tivoli Monitoring version 6.1 to version 6.2.

Chapter 5, "Installing IBM Tivoli Monitoring on one computer," on page 105, contains instructions for installing the base components on a single Windows computer. This scenario is useful for creating a test or teaching environment or for monitoring a small environment.

Chapter 6, "Installing IBM Tivoli Monitoring," on page 113, contains instructions for installing each of the base components on Windows, UNIX and Linux (command and GUI installations) computers and for completing the initial configuration of those components. It also contain procedures for installing and configuring the base agents and for installing support for those agents on the Tivoli Enterprise Portal and the Tivoli Enterprise Monitoring Server.

Chapter 7, "Deploying monitoring agents across your environment," on page 195, provides instructions for deploying distributed monitoring agents from a monitoring server.

© Copyright IBM Corp. 2005, 2007

Chapter 4. Upgrading from a previous installation

This chapter provides information to help you upgrade from a previous installation.

- "Upgrade scenarios" helps you identify the scenario to use as a guide when you upgrade and where to find information about it.
- "Planning your upgrade" on page 88 identifies the platforms no longer supported, describes two methods for determining what components need to be upgraded, provides instructions for backing up your existing environment, and specifies the required order for upgrading components.
- "Upgrading from IBM Tivoli Monitoring V6.1" on page 96 provides an overview of the process of upgrading from V6.1 to V6.2 of IBM Tivoli Monitoring.
- "Upgrading from OMEGAMON Platform V350 and V360" on page 97 provides an overview of the process of upgrading from OMEGAMON Platform 350 or 360 to IBM Tivoli Monitoring V6.2.

Upgrade scenarios

Use one of the following scenarios as a guide when you upgrade from a previous installation:

Upgrading from Tivoli Distributed Monitoring: The new IBM Tivoli Monitoring is not dependent on the Tivoli Management Framework. An upgrade toolkit is provided to facilitate your move from a Tivoli Distributed Monitoring environment to the new IBM Tivoli Monitoring. For information, see *IBM Tivoli Monitoring: Upgrading from Tivoli Distributed Monitoring*.

Upgrading from IBM Tivoli Monitoring V5.1.2: An upgrade toolkit is provided to facilitate your move from IBM Tivoli Monitoring V5.1.2 to IBM Tivoli Monitoring V6.2. For information about using the toolkit and some best practices guidelines, see *IBM Tivoli Monitoring: Upgrading from V5.1.2*.

IBM Tivoli Monitoring V5.x interoperability: Using the IBM Tivoli Monitoring 5.x Endpoint agent, you can view data from IBM Tivoli Monitoring 5.x resource models in the Tivoli Enterprise Portal and warehouse granular data in the Tivoli Data Warehouse. You can use this visualization to replace the Web Health Console used in IBM Tivoli Monitoring V5.1. For information about using this visualization, see the *IBM Tivoli Monitoring: Upgrading from V5.1.2*.

Upgrading from IBM Tivoli Monitoring V6.1: In order to upgrade from a previous installation of IBM Tivoli Monitoring V6.1, use the planning, upgrading, and post-installation configuration instructions provided in this chapter (see "Planning your upgrade" on page 88 and "Upgrading from IBM Tivoli Monitoring V6.1" on page 96).

Upgrading from OMEGAMON Platform V350 and V360: Migration tools are provided to facilitate the upgrade process to IBM Tivoli Monitoring. You can upgrade custom situations, policies, and queries, and the historical data in your data warehouse.

Many of the existing OMEGAMON Platform V350 and V360 agents have equivalent IBM Tivoli Monitoring agents. For any that do not yet have an IBM

© Copyright IBM Corp. 2005, 2007

Tivoli Monitoring counterpart, you can continue to monitor those agents in your new IBM Tivoli Monitoring environment. Use the planning and upgrade instructions in this chapter (see "Planning your upgrade" and "Upgrading from OMEGAMON Platform V350 and V360" on page 97).

Planning your upgrade

The following sections provide planning information for upgrading to IBM Tivoli Monitoring V6.2:

- "Platforms no longer supported for IBM Tivoli Monitoring V6.2"
- "Prerequisites for IBM Tivoli Monitoring V6.2" on page 89
- "IBM Tivoli Monitoring V6.2 coexistence and interoperability" on page 89
- "Determining what components to upgrade" on page 90
- "Required order of upgrade" on page 91
- "Migrated information when upgrading from a previous version" on page 91
- "Backing up IBM Tivoli Monitoring" on page 92

Note: In previous versions there was no validation on hub and remote monitoring server protocols and stand-by configuration, so it is possible that your configuration has incorrect entries. Consider reconfiguring all monitoring servers, both hub and remote. During this reconfiguration you will be warned about incorrect entries. Reconfiguration may be particularly useful if you are experiencing long startup and stopping times for monitoring servers. You can reconfigure a hub monitoring server as a remote, but reconfiguring a remote monitoring server from a remote to a hub is currently not supported. In this case you must reinstall the monitoring server.

Platforms no longer supported for IBM Tivoli Monitoring V6.2

The following platforms are no longer supported for IBM Tivoli Monitoring V6.2:

- Windows 2000 Professional
- AIX V5.1
- i5/OS 5.2
- z/OS 1.4
- z/OS 1.5
- RedHat Enterprise Linux 3 x86 Warehouse Proxy agent and Summarization and Pruning agent
- RedHat Enterprise Linux 3 zSeries Warehouse Proxy agent and Summarization and Pruning agent
- Solaris V8 - SPARC Tivoli Enterprise Monitoring Server and Summarization and Pruning agent
- RedHat Enterprise Linux 2.1 x86 Summarization and Pruning agent
- SUSE Linux Enterprise 8 x86 Tivoli Enterprise Monitoring Server, Warehouse Proxy agent and Summarization and Pruning agent
- SUSE Linux Enterprise 8 zSeries Warehouse Proxy agent and Summarization and Pruning agent

For a complete description of the supported platforms for IBM Tivoli Monitoring V6.2, see "Hardware and software requirements" on page 70.

Prerequisites for IBM Tivoli Monitoring V6.2

Some of the prerequisites for IBM Tivoli Monitoring have changed for version 6.2. Review the V6.2 hardware and software requirements for each component and platform and apply all necessary upgrades and fix packs before you begin your upgrade. See "Hardware and software requirements" on page 70 for more information.

IBM Tivoli Monitoring V6.2 coexistence and interoperability

The following statements specify the level of interoperability for IBM Tivoli Monitoring V6.2 in support of existing agents and staged upgrade scenarios.

Tivoli Enterprise Monitoring Server:

- V6.1 remote monitoring servers can connect to V6.2 hub monitoring servers.
- V6.2 remote monitoring servers can connect to V6.1 hub monitoring servers.

  Note: Agents created with the Agent Builder require that the entire path from the agent, through the remote monitoring server it connects to, to the hub monitoring server, to the portal server, and the data warehouse must be upgraded to V6.2 Agents released after IBM Tivoli Monitoring V6.2 may also require V6.2 path. Check your agent documentation.
- V6.2 interoperability with OMEGAMON Platform V350/360 remains the same as for IBM Tivoli Monitoring V6.1.

Tivoli Enterprise Portal Server:

- Tivoli Enterprise Portal Server can interoperate with older hubs back to V350.
- A Tivoli Enterprise Portal Server upgrade in place is supported from CandleNet Portal Server V196 or IBM Tivoli Monitoring V6.1 portal server to IBM Tivoli Monitoring V6.2 portal server on the same platform.
- A Tivoli Enterprise Portal Server upgrade to a new platform is accomplished with database export and import.

  For information about migrating the database, see the description of the migrate-export and migrate-import scripts in the *IBM Tivoli Monitoring: Administrator's Guide*
- IBM Tivoli Monitoring V6.2 supports importing an IBM Tivoli Monitoring V6.1 database and then upgrading it by running buildpresentation.bat (for Windows platforms) or InstallPresentation.sh (for UNIX/Linux platforms).

Tivoli Data Warehouse:

- All Warehouse Proxy and Summarization and Pruning agents must be at the same level to avoid inconsistencies in presentation.
- Warehouse Proxy and Summarization and Pruning V6.1 or V6.2 agents can interoperate with either V6.1 or V6.2 monitoring servers.
- Tivoli Enterprise Portal Server V6.2 requires V6.2 Warehouse Proxy and Summarization and Pruning agents.

Agents:

Back level agents can connect through up-level monitoring servers.

An agent upgrade elevates the user credentials of agents that have been set at deploy-time to run with reduced (non-root) credentials. Use one of the following steps to stop the agent and restart it with the appropriate user credentials:

- After stopping the agent, log in (or 'su') to the desired user, and then run the itmcmd command to start the agent in that user's context.
- Edit the startup file and add the following line to change the default user context for starting agents:

  ```
  /usr/bin/su - <dbinstancename>-c "<itmhome>/bin/itmcmd agent -h <itmhome>
       -o <dbinstancename> start product_code
  ```

  where *product_code* is the two-character product code for the agent (for example, ud for DB2).

Tivoli Event Synchronization component:

IBM Tivoli Monitoring and Tivoli Event Synchronization version 1.x installed on a Tivoli Enterprise Console event server does not operate with a V6.2 hub monitoring server. If you have already installed a previous version of Tivoli Event Synchronization, you must upgrade to version 2.0.0.0. (see "Upgrading to Tivoli Event Synchronization component version 2.0.0.0" on page 381). The upgrade is required for the event server to correctly parse events coming from the V6.2 hub monitoring server.

Determining what components to upgrade

You can determine what components to upgrade by using either of two methods. Use the Enterprise level of the Managed Systems Status list to display the version of any connected agent, as well as its status (online/offline). Identifying an agent's status is especially important as you plan remote deployments. An alternative method, available at the Enterprise level of the Navigator, is to use the Tivoli Management Services Infrastructure view. This topology view visually expresses the relationships and linking of monitoring agents and other components to the hub monitoring server. Use hover-help (help flyovers) in the Tivoli Enterprise Portal topology view to determine the current version of your installed monitoring agents and other components.

1. Access the Tivoli Enterprise Portal through the desktop client or the browser client:
   - **Desktop client:**
     a. In the Windows **Start** menu, select **Programs → IBM Tivoli Monitoring → Tivoli Enterprise Portal**. The login message is displayed.
     b. Type the name (**sysadmin**) and password of the account that you created during installation.
     c. Click **OK**.
   - **Browser client:**
     a. Start the Microsoft Internet Explorer browser.
     b. Type the following URL for the Tivoli Enterprise Portal into the Address field of the browser:

        ```
        http://systemname:1920///cnp/client
        ```

        where the *systemname* is the host name of the computer where the Tivoli Enterprise Portal is installed.
     c. Click **Yes** in response to any security prompts.
     d. In the login prompt, type the user name and password of the **sysadmin** account that you created during installation.
     e. Click **OK**.
     f. Click **Yes** to accept Java Security certificates for this browser session.

2. Click the Navigator, the view that is located by default in the upper-left corner of the portal. The first display that you see in the Navigator view is Enterprise Status workspace.
3. Select the **Enterprise** node at the top of the navigation tree, if it is not already selected.
4. Right-click the node and select **Workspace > Self-Monitoring Topology** to display the default topology view.
5. Click on the **TMS Infrastructure - Base view**. This view contains the topology display.
6. Click on the Maximize icon in the upper-right corner of the portal. The topology view occupies the entire display area of the workspace.

Required order of upgrade

Upgrade the products that comprise your configuration in the following order:

- If you use event synchronization, upgrade the event synchronization component first (see "Upgrading to Tivoli Event Synchronization component version 2.0.0.0" on page 381).
- If you are collecting warehouse data from any of the agents listed below, warehouse database migration steps must be performed before upgrade. Refer to"Upgrading the warehouse" on page 95 and the User's Guide for each agent for details:
  - Windows OS
  - Unix OS
  - Monitoring for Databases: DB2 agent
  - Monitoring for Databases: Sybase agent
  - Monitoring for Databases: mySAP
  - Monitoring for Databases: Oracle
- Hub Tivoli Enterprise Monitoring Server
- Remote monitoring server (if necessary)
- Tivoli Enterprise Management Agent Framework
- Tivoli Enterprise Portal Server
- Tivoli Enterprise Portal desktop client

Note: Agents created with the Agent Builder require that the entire path from the agent, through the remote monitoring server it connects to, to the hub monitoring server, to the portal server, and the data warehouse be upgraded to V6.2 Agents released after IBM Tivoli Monitoring V6.2 may also require V6.2 path. Check your agent documentation.

Migrated information when upgrading from a previous version

When installing over a previous release (into the same installation directory) the following information is migrated into the new version:

- Windows:
  - Port number and communication protocol settings
  - Situations
- UNIX: situations

Backing up IBM Tivoli Monitoring

Before upgrading, make a backup copy of your current IBM Tivoli Monitoring installation in case you need to revert to it. You should always contact IBM Software Support before attempting to use the files generated by the following procedures to restore the IBM Tivoli Monitoring environment. The support staff can help ensure success of the restoration. Otherwise, errors made during the modification of the Windows registry could lead to a corrupted operating system or other problems.

The following procedures describe valid methods for creating a backup. However, an enterprise typically has a standard process for preserving a backup image of all computer systems, including the IBM Tivoli Monitoring environment. In most cases, the standard process for your enterprise is preferable to the processes described in this section. Use the instructions in this section only when a standard backup process is not available.

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

- "Backing up a UNIX or Linux installation"
- "Backing up a Windows installation" on page 93

Backing up a UNIX or Linux installation

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

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

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

   ```
   ./itmcmd execute cq "runscript.sh migrate-export.sh"
   ```
4. Use the tar command to compress the contents of *ITM_Install_dir* (the directory where IBM Tivoli Monitoring is installed), using a command that is similar to the following:

   ```
   tar -cvf /tmp/ITM_Install_dir.backup.tar ITM_Install_dir
   ```
5. Add the following files to the tar file created in step 4 above:
   - On AIX:

     ```
     /etc/rc.itm*
     tar -uvf /tmp/ITM_Install_dir.backup.tar /etc/rc.itm*
     ```
   - On HP-UX:

     ```
     /sbin/init.d/ITMAgents*
     tar -uvf /tmp/ITMinstall_dir.backup.tar /etc/init.d/ITMAgents*
     ```
   - On other UNIX or Linux systems:

     ```
     /etc/initd/ITMAgents*
     tar -uvf /tmp/ITM_Install_dir.backup.tar /etc/init.d/ITMAgents*
     ```
6. Use the appropriate database commands to back up the Tivoli Data Warehouse databases.

For more information, see "Backing up your portal server and Tivoli Data Warehouse databases" on page 94.

You are now ready to proceed with the upgrade.

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

Backing up a Windows installation

Follow these steps to back up a Windows installation. In Step 4 of this procedure, you record the current configuration settings. In Step 9 on page 94, you apply these settings again.

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

1. Close any browser or desktop clients for the Tivoli Enterprise Portal.
2. Launch the **Manage Tivoli Monitoring Services** (`KinConfg.exe`) utility.
3. On the computer where you are backing up an installation, stop the Tivoli Enterprise Portal Server, the Tivoli Enterprise Monitoring Server, the Eclipse Help Server, and all the monitoring agents running on the system.
4. Perform the following steps to record the current configuration settings for IBM Tivoli Monitoring. (For example, you can make a record on a sheet of paper or in a buffer file.)
   a. Right-click in the row of the component that you want to configure.
   b. Select **Reconfigure**.

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

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

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

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

      When you are finished, all components except the Tivoli Enterprise Portal desktop show **No** in **Configured** column of the **Manage Tivoli Monitoring Services** window.

6. Use a compression command to compress the contents of the directory where IBM Tivoli Monitoring is installed.
7. Use the appropriate database commands to back up the Tivoli Enterprise Portal Server and Tivoli Data Warehouse databases.

   For more information, see "Backing up your portal server and Tivoli Data Warehouse databases."
8. Export the entire Windows registry to a backup file as follows:
   a. Select **Run** in the Windows **Start** menu.
   b. Type **regedit** in the **Open** field.
   c. Click **OK**. The Registry Editor is displayed.
   d. Ensure that the **MyComputer** node at the top of the registry is selected, so that all values in the registry are exported.
   e. Select **Export** in the **File** menu.
   f. Save the copy of the registry to the following path and filename:
      `C:\WinRegistryBeforeInstall.reg`

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

      "Unconfigured" components show **No** in the **Configured** column of the **Manage Tivoli Monitoring Services** window.
   b. Select **Advanced >> Configure Advanced** in the popup menu.
   c. In the series of dialog boxes that is displayed, enter the original parameter settings that you recorded in Step 4 on page 93.
   d. Click **OK** in each configuration window and accept other prompts to save your changes.

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

You are ready to proceed with the upgrade on this computer.

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

Backing up your portal server and Tivoli Data Warehouse databases

When backing up your IBM Tivoli Monitoring environment, you must also back up your portal server database and Tivoli Data Warehouse database. The following sections contains procedures for backup up DB2 databases, which are provided as examples. If you use SQL Server for your portal server database, or Oracle for your Tivoli Data Warehouse database, use the corresponding commands.

- "Backing up your portal server database"
- "Backing up your Tivoli Data Warehouse database" on page 95

Backing up your portal server database

Use the following command to backup your portal server database.

```
db2 backup database yourtepsdatabase to /yourbackuplocation
```

If an existing connection prevents you from backing up the database, use the following commands.

1. `db2 connect to yourtepsdatabase`
2. `db2 quiesce database immediate force connections`
3. `db2 connect reset`
4. `db2 backup database yourtepsdatabase to /yourbackuplocation`
5. `db2 connect to yourtepsdatabase`
6. `db2 unquiesce database`
7. `db2 connect reset`

Backing up your Tivoli Data Warehouse database

Use the following command to back up your Tivoli Data Warehouse database.

```
db2 backup database yourwarehousedatabase to /yourbackuplocation
```

If an existing connection prevents you from backing up the database, use the following commands.

1. `db2 connect to yourwarehousedatabase`
2. `db2 quiesce database immediate force connections`
3. `db2 connect reset`
4. `db2 backup database yourwarehousedatabase to /yourbackuplocation`
5. `db2 connect to yourwarehousedatabase`
6. `db2 unquiesce database`
7. `db2 connect reset`

Upgrading the warehouse

Some of the monitoring agents have made changes to the warehouse tables. There are three types of changes, two of these types of changes require performing upgrade procedures before running the 6.2 Warehouse Proxy and Summarization and Pruning agents. The procedure for the other change can be performed before or after you upgrade IBM Tivoli Monitoring.

Case 1 changes affect the table structure, and Case 3 changes affect the table location. Both Case 1 and Case 3 changes must be completed before running the 6.2 Warehouse Proxy and Summarization and Pruning agents. These changes and procedures are documented comprehensively in the following user's guide appendix for each monitoring agent that is affected: "Upgrade: upgrading for warehouse summarization."

- Case 1 changes add a new column to a raw table, and assign a default value to the column. If the 6.2 Warehouse Proxy agent is started before these scripts are run, a NULL default value is assigned, and that default value cannot be changed. The following monitoring agents have Case 1 changes:
  - Monitoring for Databases: DB2 Agent
  - Monitoring for Applications: mySAP Agent
  - Monitoring: UNIX OS Agent
  - Monitoring: Windows OS Agent
- Case 2 changes affect how agent data is summarized because of changes in primary key definitions. The Case 2 changes can be done before or after you upgrade IBM Tivoli Monitoring.The following monitoring agents have Case 2 changes:

  - Monitoring for Applications: mySAP Agent
  - Monitoring for Databases: Sybase Server Agent
  - Monitoring: Windows OS Agent
- Case 3 changes are only applicable if you are using DB2 as your warehouse database. These changes move a summary table from the 4K table space to the 8K table space. If the 6.2 Summarization and Pruning agent is started before these scripts are run, you receive DB2 errors, because the row size of the upgraded table is longer than what can fit into the 4K table space. The following monitoring agents have Case 3 changes:
  - IBM Tivoli Monitoring for Databases: DB2 Agent
  - IBM Tivoli Monitoring for Databases: Oracle Agent
  - IBM Tivoli Monitoring: UNIX OS Agent

To ensure that you can make the table upgrades required by Case 1 and Case 3 before installing the 6.2 monitoring agents, do the following:

- Stop the Warehouse Proxy and the Summarization and Pruning agents prior to upgrading to IBM Tivoli Monitoring V6.2.
- Change the default startup of these monitoring agents so they do not start automatically during a restart of IBM Tivoli Monitoring. This prevents these monitoring agents from starting automatically during the upgrade process.
- Perform the IBM Tivoli Monitoring upgrades.
- Make the warehouse updates for the monitoring agents with Case 1 and Case 3 changes as described in the user's guide for the affected agent.
- Enable the default startup of the Warehouse Proxy and the Summarization and Pruning agents, and start these agents.

Several monitoring agents made changes to the warehouse collection and summarization characteristics for some agent attribute groups. These changes correct and improve the way warehouse data is summarized, producing more meaningful historical reports. For an explanation of these changes and the implications to your warehouse collection and reporting, see the ″Upgrading for warehouse summarization″ appendix of the user's guide for your specific monitoring agent.

Upgrading from IBM Tivoli Monitoring V6.1

The following sections provide information for upgrading from IBM Tivoli Monitoring V6.1 to IBM Tivoli Monitoring V6.2:

- "Overview of the upgrade process"
- "Required Java JRE" on page 97

Overview of the upgrade process

Upgrading from IBM Tivoli Monitoring V6.1 to IBM Tivoli Monitoring V6.2 involves the following steps:

Table 22. Upgrading from IBM Tivoli Monitoring V6.1 to IBM Tivoli Monitoring V6.2

Task		Where to find information
Before upgrading your monitoring environment	Review the upgrade planning information to identify what you can and cannot upgrade, as well as the required upgrade order.	"Planning your upgrade" on page 88
	Stop all components that you are upgrading and change their startup from **Automatic** to **Manual**.	"Starting and stopping components" on page 210
	Restart the computer on which you are installing IBM Tivoli Monitoring.	
Upgrading your monitoring environment	Run the IBM Tivoli Monitoring installation program on all components that you want to upgrade. Use your existing installation directory as your IBM Tivoli Monitoring directory.	Chapter 6, "Installing IBM Tivoli Monitoring," on page 113
After upgrading your monitoring environment	On platforms other than Windows, you must reconfigure the Tivoli Enterprise Monitoring Server and the Tivoli Enterprise Portal Server. **Note:** On Windows platforms, the installer manages the reconfiguration process.	Chapter 8, "Configuring IBM Tivoli Monitoring components," on page 207
	Support for base agents is upgraded automatically, but you must add application support for any other monitoring agents you are upgrading.	"Configuring application support for non-Base monitoring agents" on page 164

Notes:

1. The installation instructions sometimes reference the default path for the installation of IBM Tivoli Monitoring. If you did not install the product in the default path, you must specify the correct path whenever the upgrade procedures require a path specification.
2. After you upgrade a UNIX monitoring server, you must run the **itmcmd config -S** command to configure the upgraded monitoring server and the **itmcmd support** command to update application support files.
3. You can use the **tacmd updateAgent** command to install an agent update on a specified managed system. For reference information about this command and related commands, see the *IBM Tivoli Monitoring: Command Reference*.
4. You must recycle (stop and restart) the portal server to use upgraded workspaces for your monitoring agents.

Required Java JRE

IBM Tivoli Monitoring V6.2 requires Java 1.5. However, running IBM Tivoli Monitoring V6.1 agents and IBM Tivoli Monitoring V6.2 agents on same computer requires Java 1.4.2 and 1.5 on that computer.

Upgrading from OMEGAMON Platform V350 and V360

The following sections provide information for upgrading from OMEGAMON Platform 350 or 360 and CandleNet Portal 195 to IBM Tivoli Monitoring 6.2.

Note: You cannot upgrade directly to IBM Tivoli Monitoring from a version of OMEGAMON Platform prior to 350 or 360. If you are using an older version of OMEGAMON Platform, you must first upgrade to OMEGAMON Platform 350 or 360 before upgrading to IBM Tivoli Monitoring.

If you are upgrading from Tivoli Distributed Monitoring, see the *IBM Tivoli Monitoring: Upgrading from Tivoli Distributed Monitoring* guide.

- "Overview of the upgrade process"
- "Considerations" on page 99
- "Migrating data from an existing Warehouse Proxy database" on page 101
- "Using existing OMEGAMON and other monitoring agents with IBM Tivoli Monitoring" on page 103

Overview of the upgrade process

Upgrading from Candle® OMEGAMON Platform 350 or 360 involves the following steps:

Table 23. Upgrading from OMEGAMON Platform 350 or 360

Task		Where to find information
Before installing IBM Tivoli Monitoring	Review the new terminology. Although the same components exist in IBM Tivoli Monitoring, many have new names.	"Terminology changes" on page 99
	Review the upgrade planning information to identify what you can and cannot upgrade.	"Considerations" on page 99
	Stop all components that you are upgrading and change their startup from **Automatic** to **Manual**.	"Starting and stopping components" on page 210
	Restart the computer on which you are installing IBM Tivoli Monitoring.	
Upgrading your monitoring environment	Run the IBM Tivoli Monitoring installation program on all components that you want to upgrade. Use your existing installation directory as your IBM Tivoli Monitoring directory.	Chapter 6, "Installing IBM Tivoli Monitoring," on page 113
After installing IBM Tivoli Monitoring	Run the Warehouse Proxy migration tool to migrate your existing Warehouse Proxy database.	"Migrating data from an existing Warehouse Proxy database" on page 101
	For any *existing* OMEGAMON monitoring agents that you want to use with the IBM Tivoli Monitoring monitoring server, change their configuration to point to the new monitoring server.	"Using existing OMEGAMON and other monitoring agents with IBM Tivoli Monitoring" on page 103

Notes:

1. After you upgrade a UNIX monitoring server, you must run the **itmcmd config -S** command to configure the upgraded monitoring server and the **itmcmd support** command to update application support files.
2. You must recycle (stop and restart) the portal server to use upgraded workspaces for your monitoring agents.
3. You cannot use the agent deployment function in IBM Tivoli Monitoring to upgrade OMEGAMON agents.

Considerations

Consider the following issues when upgrading from OMEGAMON Platform 350 or 360 and CandleNet Portal 195 to IBM Tivoli Monitoring 6.2.

Terminology changes

The following terms have changed with the move from Candle OMEGAMON to IBM Tivoli Monitoring:

Table 24. OMEGAMON to IBM Tivoli Monitoring terminology

OMEGAMON term	**IBM Tivoli Monitoring term**
Candle Management Server® (CMS)	Tivoli Enterprise Monitoring Server
CandleNet Portal (CNP)	Tivoli Enterprise Portal
CandleNet Portal Server (CNPS)	Tivoli Enterprise Portal Server
OMEGAMON Monitoring Agent® (OMA)	Tivoli Enterprise Monitoring Agent (monitoring agent)
OMEGAMON Platform	Tivoli Management Services
Manage Candle Services	Manage Tivoli Monitoring Services
Event	Situation event
Seeding	Adding application support
OMEGAMON Web Services	Tivoli Monitoring Web Services
Candle Customer Support	IBM Software Support

When to run the upgrade

Run the upgrade to IBM Tivoli Monitoring immediately after you have rebooted the computer on which you are running the upgrade. IBM Tivoli Monitoring does not install if the computer has any locked files.

If your OMEGAMON components are currently set to start automatically, change the startup to **Manual** in Manage Tivoli Monitoring Services before you restart the components.

Installation directory for upgraded components

When you upgrade an existing OMEGAMON component to the IBM Tivoli Monitoring level, the installation process installs all new files in your existing installation directory (instead of the new default installation directory for IBM Tivoli Monitoring: C:\IBM\ITM on Windows and /opt/IBM/ITM on Linux and UNIX). Your existing files are overwritten.

If you have applied fixes or patches to the OMEGAMON product component, those fixes and patches that were available when IBM Tivoli Monitoring was released are included in the upgraded version.

Configuration settings for upgraded agents

When OMEGAMON Platform V350 or 360 agents are upgraded to IBM Tivoli Monitoring, agent-specific configuration settings regarding the connection to the monitoring server are not maintained. The IBM Tivoli Monitoring installation uses the default settings for all agents (not the one change that you made for one agent). To ensure that your upgraded agents can immediately connect to a monitoring server, determine whether the default settings for all agents point to the new monitoring server prior to upgrading. To change the default settings for all agents, right-click an agent in Manage Candle Services and click **Set defaults for all agents**.

Candle Management Workstation coexistence

If you currently use Candle Management Workstation in your OMEGAMON monitoring environment, you are migrated to IBM Tivoli Monitoring automatically when you migrate the rest of your environment. However, the installed Candle Management Workstation continues to function after the migration, although it is not officially part of IBM Tivoli Monitoring and no new function has been added.

If you use the OMEGAMON XE for CICS® 3.1.0 product, you must continue to use Candle Management Workstation to configure workloads for Service Level Analysis. After you have configured the workloads, you can use the Tivoli Enterprise Portal for all other tasks.

If you do not currently have Candle Management Workstation (for example, if you are installing OMEGAMON XE for CICS 3.1.0 into an IBM Tivoli Monitoring environment), you must install the Candle Management Workstation that is shipped with the OMEGAMON XE for CICS 3.1.0 product. Install Candle Management Workstation on a different computer than the Tivoli Enterprise Portal. Otherwise, the Candle Management Workstation attempts to uninstall the Tivoli Enterprise Portal.

Additional unsupported OMEGAMON functions

The following functions are no longer supported as part of IBM Tivoli Monitoring:

Table 25. Unsupported OMEGAMON functions

Function	IBM Tivoli Monitoring equivalent function
CandleClone	Agent deployment, as described in Chapter 7, "Deploying monitoring agents across your environment," on page 195
CandleRemote	
Event emitters	Event forwarding using the Tivoli Enterprise Console event synchronization, as described in Chapter 17, "Setting up event forwarding to Tivoli Enterprise Console," on page 361
Event adapters	
GUI installation wizard on UNIX	Use the command line installation option, as described in Chapter 6, "Installing IBM Tivoli Monitoring," on page 113
Silent installation on UNIX using the multi-platform installation program	Silent installation using custom response files, as described in "Performing a silent installation on a Linux or UNIX computer" on page 423.

CandleNet Portal database

If you use a DB2 database for the CandleNet Portal, the database is converted to UTF-8 format during the upgrade. This might take several minutes, depending on the size of your database. If you used the default database password when you created the CandleNet Portal database (cnps), you are prompted for a new password to comply with the more stringent security provisions in IBM Tivoli Monitoring.

Required Java JRE

The CandleNet Portal requires the Sun Java JRE; however Tivoli Enterprise Portal requires the IBM Java JRE 1.5. You do not need to install this JRE prior to the upgrade: it is installed automatically when you choose to install an IBM Tivoli Monitoring component that requires it.

Migrating data from an existing Warehouse Proxy database

You can migrate your existing data in an OMEGAMON Platform 360 data warehouse to the IBM Tivoli Monitoring Tivoli Data Warehouse using a migration tool provided with IBM Tivoli Monitoring.

Before you migrate to the new data warehouse, you need to create a new ODBC data source for the V6.2 of the Warehouse Proxy agent and connect that data source to a new database. The migration tool moves your data from the existing database to the new database. For information about creating a new data source and database, see Chapter 13, "Tivoli Data Warehouse solution using DB2," on page 273 or Chapter 14, "Tivoli Data Warehouse solution using Microsoft SQL Server," on page 299.

The warehouse migration tool is installed when you install the Warehouse Summarization and Pruning Agent. The following files are installed in the *itm_installdir*/tmaitm6 directory:

- khdmig.jar
- KHDENV_MIG
- migratewarehouse.bat

Note: Warehouse migration is supported only on Windows computers.

The tool also uses several files installed by the Warehouse Summarization and Pruning agent.

The following sections provide information on using the warehouse migration tool.

Before you run the tool

Perform the following tasks before you run the migration tool:

- Back up your existing database.
- If your existing database is a Microsoft SQL database, install a Microsoft SQL JDBC driver on the computer where that database is installed. You can download the JDBC driver from the Microsoft Web site for Microsoft SQL.
- Install the IBM Java JRE, version 1.4.2.
- If you have collected data for multiple types of agents in the past and you want to migrate the data for all of those agents, you must install support for the new V6.2 agents on the Tivoli Enterprise Portal Server.
- Start the Tivoli Enterprise Portal Server.
- Stop the Warehouse Summarization and Pruning and the Warehouse Proxy agents.
- Do not start data collection with the Warehouse Summarization and Pruning agent prior to running this migration tool. If you do, the information that you migrate will not be pruned or summarized. If this is the case, delete the content of the WAREHOUSEMARKER table to enable pruning of both migrated and new data.

Configuring the migration tool

Before running the migration tool, use the following steps to configure the tool for your environment:

1. Update the migratewarehouse.bat file to set the correct CLASSPATH for your JDBC driver.

The file contains the following default installation directories for the 3 supported drivers. Update the location based on where your JDBC driver is installed.

- Microsoft SQL Server:

  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.jar
- DB2: C:\Program Files\IBM\SQLLIB\java\db2java.zip
- Oracle: C:\oracle\ora92\jdbc\lib\classes12.zip

2. Update the following variables in the KHDENV_MIG file:

Table 26. KHDENV_MIG file variables for warehouse migration

Type of information	Variable	Description
Commit rate	KHD_MAX_ROWS_PER_TRANSACTIONS	The number of rows committed at each insertion of data.
Bad rows to skip	KHD_MAX_ROWS_SKIPPED_PER_TABLE	The number of rows per table the tool skips to migrate if the data that needs to be inserted is incorrect. When this number is reached, the tool stops the migration of the table.
Tivoli Enterprise Portal connection information	KHD_CNP_SERVER_HOST	The name of the Tivoli Enterprise Portal Server.
	KHD_CNP_SERVER_PORT	The port number of the Tivoli Enterprise Portal Server.
Source database connection information	KHD_SOURCE_JDBC_DRIVER	The JDBC driver used to connect to the source database.
	KHD_SOURCE_URL	The URL to use to connect to the source database.
	KHD_SOURCE_DATABASE_SCHEMA	The owner or schema in the Candle tables in the source database.
	KHD_SOURCE_DATABASE_USER	The user that connects to the source database.
	KHD_SOURCE_DATABASE_PASSWORD	The password for the user to connect to the source database.
Target database connection information	KHD_TARGET_JDBC_DRIVER	The JDBC driver used to connect to the target database.
	KHD_TARGET_URL	The URL to use to connect to the target database.
	KHD_TARGET_DATABASE_SCHEMA	The owner or schema in the tables in the target database.
	KHD_TARGET_DATABASE_USER	The user that connects to the target database.
	KHD_TARGET_DATABASE_PASSWORD	The password for the user to connect to the target database.

For JDBC driver information, use the syntax appropriate to your driver vendor:

DB2 URL: jdbc:db2:<*database*>

Driver: COM.ibm.db2.jdbc.app.DB2Driver

MS SQL Server

URL: jdbc:microsoft:sqlserver://<*server*>:<*port*>;DatabaseName=<*database*>

Driver: com.microsoft.jdbc.sqlserver.SQLServerDriver

Default port: 1433

Oracle URL: jdbc:oracle:thin:@<*server*>:<*port*>:<*database*>

Driver: oracle.jdbc.driver.OracleDriver

Default port: 1521

Running the warehouse migration tool

After you update the files, as described in the previous section, run the migratewarehouse.bat file.

Status tables

Part of the migration of data to the new warehouse requires shortening the table and column names if the target database is not a Microsoft SQL database. When a name is shortened, an entry is created inside the WAREHOUSEID table in your new database. You can view this table to check which table names or column names have been modified.

For each package of rows committed, an entry is also made in the new WAREHOUSEMIGLOG table.

If the migration tool fails during the migration, you can look at the WAREHOUSEMIGLOG table to identify those tables that migrated successfully. If you want to restart the migration without migrating these tables again, delete the tables from the source database. You must also delete all the data that has been partially exported in the last tables. Use the **writetime** column in this table to determine which data is old and which new.

Using existing OMEGAMON and other monitoring agents with IBM Tivoli Monitoring

Existing installed OMEGAMON Platform 350 and 360 agents and new IBM Tivoli Composite Application Management and AF/Operator agents can be supported using the Tivoli Enterprise Monitoring Server; however, the following restrictions apply:

- New features in IBM Tivoli Monitoring (such as remote deployment) are *not* supported on OMEGAMON Platform 350 and 360 agents.
- Agents must use one of the following protocols to communicate with the monitoring server:
  - IP.UDP (formerly TCP/IP)
  - IP.PIPE
  - SNA

  The IP.SPIPE protocol is not supported for OMEGAMON agents.
- You cannot install an OMEGAMON agent on the same computer as a Tivoli Enterprise Portal Server. If you want to monitor something on the same computer as the portal server, install an IBM Tivoli Monitoring agent, if one is available.
- IBM Tivoli OMEGAMON XE for Messaging V6.0 requires that the hub Tivoli Enterprise Monitoring Server, the Tivoli Enterprise Portal Server, and the Tivoli Enterprise Portal client be at the IBM Tivoli Monitoring V6.2 level.

After you upgrade the infrastructure components to IBM Tivoli Monitoring V6.2, install application support files for this monitoring agent on the monitoring server, the portal server, and the portal desktop client. To install and enable application support, follow the instructions in the *IBM Tivoli OMEGAMON XE for Messaging Version 6.0 Installation Guide*.

- To enable the Tivoli Data Warehouse to collect data from OMEGAMON Platform 350 and 360 agents (through the Warehouse Proxy), copy the product attribute file to the *itm_installdir*/TMAITM6/ATTRLIB directory on the Warehouse Proxy agent (where *itm_installdir* is the IBM Tivoli Monitoring installation directory).

For full interoperability between OMEGAMON Platform 350 and 360 and AF/Operator agents and IBM Tivoli Monitoring, you need to install the application support files for these agents on the monitoring server, portal server, and portal desktop client. See the "Agent interoperability" document in the IBM Tivoli Monitoring information center for information about downloading and installing these support files.

Chapter 5. Installing IBM Tivoli Monitoring on one computer

This chapter describes how to deploy a small IBM Tivoli Monitoring environment on a single Windows computer. Installation on one computer might be useful for a test environment, a teaching environment, or for monitoring a small server environment.

The single-computer installation supports between 100 and 200 monitoring agents and can perform minimal historical data collection. See "Small monitoring environment" on page 27 for further discussion of the capabilities of a small monitoring environment.

The single-computer installation includes the following components:

The hub Tivoli Enterprise Monitoring Server (hub monitoring server)
The Tivoli Enterprise Portal Server (portal server)
The Tivoli Enterprise Portal Client (portal client)
The Tivoli Enterprise Portal Server database (portal server database)
The Tivoli Data Warehouse database (warehouse database)
The Warehouse Proxy agent
The Summarization and Pruning agent

The single-computer installation does not include the IBM Tivoli Enterprise Console.

Prerequisites for the single computer installation

The software prerequisites for the single-computer installation described in this chapter are as follows:

- A supported Windows operating system
- One of the following RDBMS servers for the portal server:
  - IBM DB2 UDB
  - Microsoft SQL Server 2000

For the Tivoli Data Warehouse, you can also use Microsoft SQL Server 2005. IBM DB2 UDB V9.1 is included with IBM Tivoli Monitoring. This version should be used for new installations to minimize the need to upgrade DB2 in the future.

While it is possible to install Tivoli Monitoring on a single Linux or UNIX computer, additional manual configuration is required. When you install Tivoli Monitoring on a Windows computer with IBM DB2 or Microsoft SQL Server, much of the configuration required to set up the Tivoli Data Warehouse is automated. (An extra configuration step is required after installation if you use Microsoft SQL Server 2005 for the Tivoli Data Warehouse database.)

In a single-computer installation, the RDBMS server is used for both of the databases required by Tivoli Monitoring:

- The *Tivoli Enterprise Portal Server database* (or *portal server database*) stores user data and information required for graphical presentation on the user interface. The portal server database is created automatically during configuration of the portal server. It is always located on the same computer as the portal server.

© Copyright IBM Corp. 2005, 2007

- The *Tivoli Data Warehouse database* (also called the *warehouse database* or *data warehouse*) stores historical data for presentation in historical data views. In a single-computer installation, the warehouse database is created on the same RDBMS server used for the portal server database. In larger environments, it is best to create the warehouse database on a different computer from the portal server.

Installation procedure

Complete the following steps to install IBM Tivoli monitoring on one Windows computer with IBM DB2 or Microsoft SQL Server already installed:

1. Launch the installation wizard by double-clicking the setup.exe file in the WINDOWS subdirectory of 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. On the Install Prerequisites window, read the information about the required levels of IBM Global Security Toolkit (GSKit) and IBM Java.

   The check box for each prerequisite is cleared if the correct level of the software is already installed. Otherwise, the check box is selected to indicated that the software is to be installed.
4. Click **Next**. The prerequisite software is installed if necessary.
5. Click **Accept** to accept the license agreement.
6. Choose the directory where you want to install the product. The default directory is C:\IBM\ITM. Click **Next**.
7. Click **Next** to accept the default encryption key and then click **OK** on the popup window to confirm the encryption key.
8. On the Select Features window, select the check boxes for the components you want to install. Select all components for a complete installation on one computer.
9. Click **Next**.

   The Agent Deployment window is displayed. This window lists monitoring agents that you can deploy to remote computers. For this installation, do not select any agents for remote deployment.
10. Click **Next**.
11. A window is displayed for you to select a program folder for the Windows Start menu. Select a program folder and click **Next**. The default program folder name is IBM Tivoli Monitoring.
12. If the TEPS Desktop and Browser Signon ID and Password window is displayed, enter and confirm the password to be used for logging on to the Tivoli Enterprise Portal. The default logon user ID, `sysadmin`, cannot be changed on this window.

    This password is required only when Security: Validate User has been enabled on the hub monitoring server. This window is not displayed if the sysadmin user ID has already been defined in the operating system.
13. Review the installation summary details. The summary identifies the components you are installing. Click **Next** to begin the installation.

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

14. Click **Next** to start configuring all selected components. (Leave all check boxes selected for this installation.)
15. Configure communications for the Tivoli Enterprise Portal Server:
    a. Click **Next** to confirm that you are installing the portal server on this computer. (The host name of this computer is displayed by default.)
    b. If more than one RDBMS product is installed on this computer, a window is displayed for you to choose the RDBMS product you want to use. Choose **IBM DB2** or **SQL Server** and click **Next**.
    c. A window is displayed for you to configure the connection between the portal server and the *portal server database* (TEPS database).

       The installation program uses the information on this window to automatically perform the following tasks:

       - Create the portal server database.
       - Create a database user for the portal server to use to access the database.
       - Configure the ODBC connection between the portal server and the database.

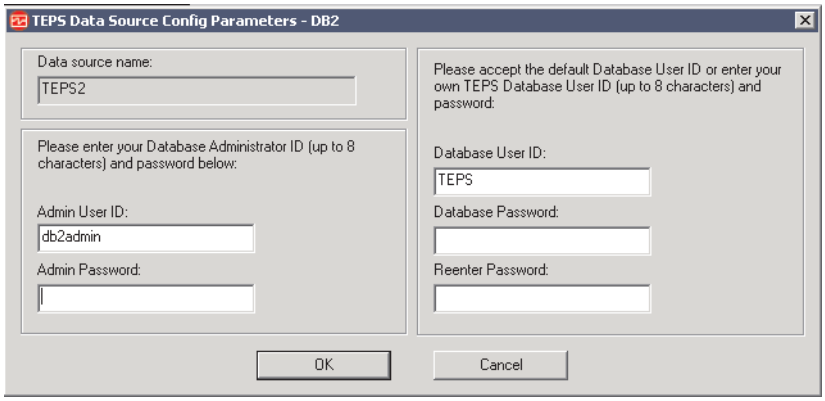


Figure 17. Configuration window for the portal server database using DB2

Figure 17 shows the configuration window for a portal server database using DB2. The configuration window for a Microsoft SQL Server database is similar. The fields on the configuration window are described in the following table:

Table 27. Configuration information for the portal server database

Field	DB2 default	MS SQL default	Description
Admin User ID	db2admin	sa	The database administrator ID.
Admin Password	(no default)	(no default)	The password for the database administrator ID.
Database User ID	TEPS	cnps	The login name of the database user that the portal server will use to access the database.
Database Password	(no default)	(no default)	The password for the database login user. If your environment requires complex passwords (passwords that require both alpha and numeric characters), specify a password that complies with these requirements.

Table 27. Configuration information for the portal server database (continued)

Field	DB2 default	MS SQL default	Description
Reenter password	(no default)	(no default)	Confirm the password by entering it again.

d. Optionally change the default values for the administrator ID and database user ID. Enter passwords for the administrator and database user. Click **OK**.

e. Click **OK** on the message that tells you that the portal server configuration was successful.

f. Click **Next** to accept the default Tivoli Data Warehouse user ID and password. (You can change these values in a later step.)

g. In the TEP Server Configuration window, click **OK** to accept the default communications protocol, **IP.PIPE**. IP.PIPE is the protocol that the portal server will use to communicate with the Tivoli Enterprise Monitoring Server.

   A second TEP Server Configuration window is displayed. The **IP.PIPE** area of this window displays the host name of this computer and the default port number, 1918.

h. Click **OK** to accept the default host name and port number.

i. Click **Yes** on the message asking if you want to reconfigure the warehouse connection information for the portal server.

j. Select **DB2** or **SQL Server** from the list of RDBMS platforms and click **OK**.

   A window is displayed for you to configure the connection between the portal server and the *Tivoli Data Warehouse database*. (The Tivoli Data Warehouse database is referred to in the title of this window as the data source for the Warehouse Proxy. The Warehouse Proxy agent sends information collected from monitoring agents to the Tivoli Data Warehouse.)

   The installation program uses the information on this window to automatically perform the following tasks:

   - Create the Tivoli Data Warehouse database.
   - Create a database user (called the *warehouse user*) for the portal server, Warehouse Proxy agent, and Summarization and Pruning agent to use to access the warehouse database.
   - Configure the ODBC connection between the portal server and the warehouse database.

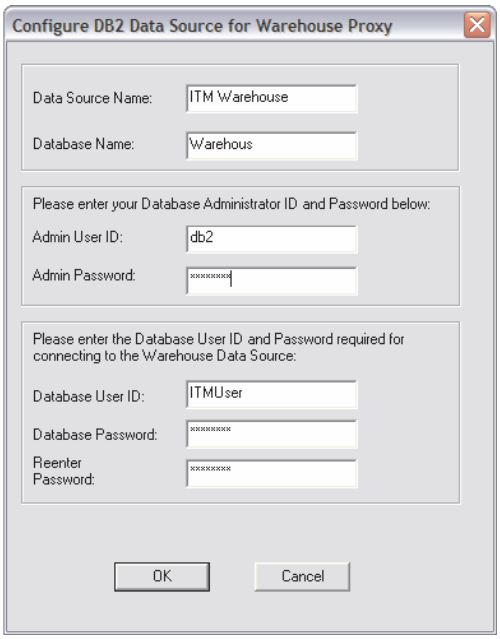


Figure 18. Configuration window for the Tivoli Data Warehouse database using DB2

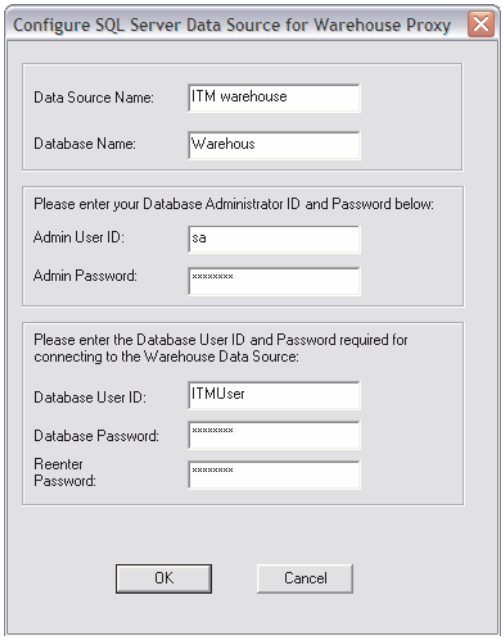


Figure 19. Configuration window for the Tivoli Data Warehouse database using Microsoft SQL Server

The fields on this window are described in the following table:

Table 28. Configuration information for the Tivoli Data Warehouse database

Field	DB2 default	MS SQL default	Description
Data Source Name	ITM Warehouse	ITM Warehouse	The name of the data source.
Database Name	WAREHOUS	WAREHOUS	The name of the database.
Admin User ID	db2admin	sa	The database administrator ID.
Admin Password	(no default)	(no default)	The password for the database administrator ID.
Database User ID	ITMUser	ITMUser	The login name of the database user that the portal server, Warehouse Proxy agent, and Summarization and Pruning agent will use to access the Tivoli Data Warehouse database.
Database Password	itmpswd1	itmpswd1	The password for the database login user. If your environment requires complex passwords (passwords that require both alpha and numeric characters), specify a password that complies with these requirements.
Reenter password	itmpswd1	itmpswd1	Confirm the password by entering it again.

k. Optionally change the default values on this window. Enter the password of the database administrator. Click **OK**.

l. Click **OK** on the message that tells you that the portal server configuration was successful.

16. Configure communications for the hub Tivoli Enterprise Monitoring Server:
    a. Click **OK** to accept the defaults on the Tivoli Enterprise Monitoring Server Configuration window:
       - The type of server you are configuring is **Hub**.
       - The default name of the hub monitoring server is HUB_*host_name*, for example, HUB_ITMSERV16.
       - The default communications protocol is **IP.PIPE**. IP.PIPE is the protocol that the monitoring server will use to communicate with the portal server.

         Note: If your site uses the IP.PIPE protocol for communications, be aware of the following limitations:
         - There can be at most 16 IP.PIPE processes per host.
         - IP.PIPE uses one, and only one, physical port per process. Port numbers are allocated using a well-known port allocation algorithm. The first process for a host is assigned port 1918, which is the default.
         - KDC_PORTS is not supported for IP.PIPE.

         If you need to have more than 16 processes per host, use IP.UDP (User Datagram Protocol) for connections.
       - Do *not* change the **Security: Validate User** check box. The default setting enables the hub monitoring server to validate users who log on to the Tivoli Enterprise Portal. For more information, see "Configuring user authentication" on page 211.

       The Hub TEMS Configuration window is displayed. The **IP.PIPE** area of this window displays the host name of this computer and the default port number, 1918.
    b. Click **OK** to accept the default host name and port number.
17. Add application support to the hub Tivoli Enterprise Monitoring server. Application support files contain specific information, such as predefined situations, for the monitoring agents included on the IBM Tivoli Monitoring installation media.
    a. Click **OK** on the popup window to indicate that the hub monitoring server is installed on this computer.
    b. Click **OK** to add all available application support to the monitoring server. (By default, all application support packages are selected.)
    c. Click **Next** on the message telling you that the application support has been added.
18. Configure the default communication between any IBM Tivoli Monitoring component and the hub Tivoli Enterprise Monitoring Server:
    a. On the configuration window, click **OK** to accept the default communications protocol, **IP.PIPE**.

       A second configuration window is displayed. The **IP.PIPE** area of this window displays the host name of this computer and the default port number, 1918.
    b. Click **OK** to accept the default host name and port number.
19. Click **Finish** to complete the installation.

When the installation is complete, the Manage Tivoli Enterprise Monitoring Services window is displayed. This window is used for starting, stopping, and configuring installed components. This window can be displayed at any time from

the Windows Start menu by clicking **Start → Programs → IBM Tivoli Monitoring → Manage Tivoli Monitoring Services**.

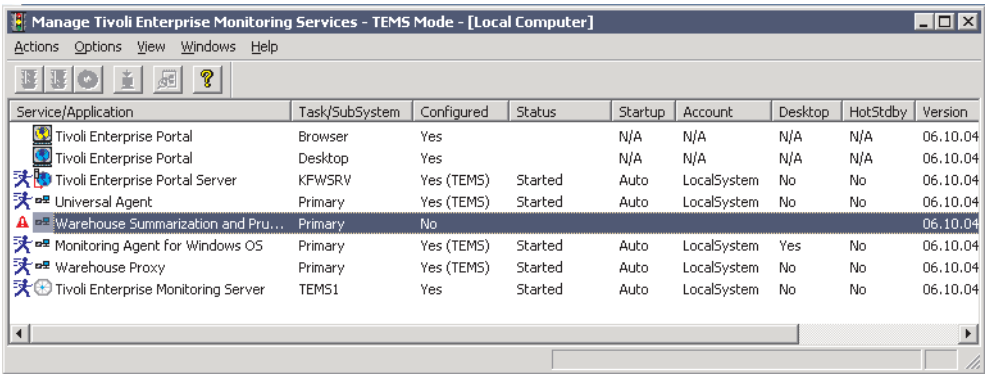


Figure 20. Tivoli Enterprise Monitoring Services window

The symbol next to a component indicates its current state:

A blue running figure indicates the component is started.

A green check mark indicates that the component is configured and can be started.

A red exclamation mark indicates that the component needs to be configured before it can be started.

Post-installation procedures

Complete the following tasks after you finish the installation procedure:

- Start the Eclipse Help Server and the Tivoli Enterprise Portal Server, if not started. Right-click the component in the Manage Tivoli Enterprise Monitoring Services window and select **Start**.

  To log on to the Tivoli Enterprise Portal using the desktop client, double-click the Tivoli Enterprise Portal icon on your Windows desktop. Use the sysadmin password that you specified in Step 12 on page 106. (For more information about logging on to the Tivoli Enterprise Portal, see "Starting the Tivoli Enterprise Portal client" on page 188.)

- Configure the Summarization and Pruning agent.

  The installation procedure automatically starts and configures all the monitoring agents that you installed except for the Summarization and Pruning agent. The Summarization and Pruning agent is not configured and started during installation to give you an opportunity to configure history collection in advance for all installed monitoring agents, a task that must be performed prior to starting the Summarization and Pruning agent for the first time.

  To configure and start the Summarization and Pruning agent, refer to the following procedures:

  - "Configuring the Summarization and Pruning agent (JDBC connection)" on page 337
  - "Starting the Summarization and Pruning agent" on page 347

- If you are using Microsoft SQL Server 2005 for the Tivoli Data Warehouse database, perform the following additional steps:

  - Create a schema with the same name (and owner) as the database user ID for accessing the Tivoli Data Warehouse. (The default user ID is `ITMUser`.) Change the default schema from `dbo` to this database user ID.

You specified the database user ID on the Configure SQL Data Source for Warehouse Proxy window during installation. See Step 15j of the installation procedure.

– Ensure that the database is set up to support inbound network TCP/IP connections.

Chapter 6. Installing IBM Tivoli Monitoring

You install the Tivoli Monitoring distributed components and base agents using *IBM Tivoli Monitoring V6.2.0 Base* DVD or DVD image. The installation and initial configuration of your environment consists of the steps described in Table 29 on page 114.

Before you begin, take note of the following information concerning the installation procedures in this chapter:

- The installation procedures provide information for installing a single component (such as the monitoring server) on one computer. If you want to install multiple components (such as the monitoring server and the portal server) on the same computer and you want to install them simultaneously, the actual steps might vary. Refer to the individual sections for required configuration information during your installation.
- The installer now validates configuration values for hub, remote, and standby monitoring servers. During configuration, the installer may prompt you to verify values that it considers suspect.
- The installation procedures in this chapter contain instructions for new installations. Follow the same procedures for upgrading or updating your installation. However, when you upgrade or update an installation, configuration windows for components that are already configured might not be displayed. Skip the steps that do not apply. The instructions sometimes references the default path for the installation of IBM Tivoli Monitoring. If you did not install the product in the default path, you must specify the correct path whenever the upgrade procedures require a path specification.

  An *upgrade* is an installation that replaces a previous release or fix pack level of the product or component with a later release or fix pack level. An *update* is a modification to an existing installation at the same release or fix pack level.
- See Appendix A, "Installation worksheets," on page 409 for a set of worksheets that you can use to gather the information required for installation.
- The following sections contain Windows, Linux, and UNIX procedures for installing the various components. Use the procedure that best applies to your environment layout. For example, you can install a monitoring server on UNIX, a portal server on Linux, and a portal desktop client on Windows. To install a monitoring server or monitoring agents on a z/OS system, refer to the appropriate z/OS documentation as described in Table 29 on page 114.
- If your site uses the IP.PIPE protocol for communications, be aware of the following limitations:
  - There can be at most 16 IP.PIPE processes per host.
  - IP.PIPE uses one, and only one, physical port per process. Port numbers are allocated using a well-known port allocation algorithm. The first process for a host is assigned port 1918, which is the default.
  - KDC_PORTS is not supported for IP.PIPE.

  If you need to have more than 16 processes per host, use IP.UDP (User Datagram Protocol) for connections between IBM Tivoli Monitoring components.

© Copyright IBM Corp. 2005, 2007

Table 29. IBM Tivoli Monitoring high-level installation steps

Step	Where to find information
Install the hub Tivoli Enterprise Monitoring Server.	• To install a hub monitoring server on a Windows, Linux, or UNIX system, see "Installing and configuring the hub Tivoli Enterprise Monitoring Server." • To install a hub monitoring server on a z/OS system, refer to the IBM Tivoli Monitoring publication entitled *Configuring Tivoli Enterprise Monitoring Server on z/OS*.
Install any remote monitoring servers.	• To install a remote monitoring server on a Windows, Linux, or UNIX system, see "Installing and configuring the remote monitoring servers" on page 123. • To install a remote monitoring server on a z/OS system, refer to the IBM Tivoli Monitoring publication entitled *Configuring Tivoli Enterprise Monitoring Server on z/OS*.
Install the Tivoli Enterprise Portal Server.	"Installing the Tivoli Enterprise Portal Server" on page 129
Install monitoring agents.	• To install monitoring agents on Windows, Linux, or UNIX systems, see "Installing monitoring agents" on page 148. • To install monitoring agents on a z/OS system, refer to the configuration guides for your z/OS agent product. If you plan to use the remote deployment function in IBM Tivoli Monitoring to install distributed monitoring agents across your environment, see Chapter 7, "Deploying monitoring agents across your environment," on page 195 for the required steps. (You cannot use the remote deployment function to install z/OS monitoring agents.)
Install the portal desktop client (optional). If you want to use only the browser client, you do not need to install the desktop client.	"Installing the Tivoli Enterprise Portal desktop client" on page 156
Install required application support on the monitoring server, portal server, and portal desktop client.	"Installing and enabling application support" on page 159
Install the language packs for all languages other than English.	"Installing language packs" on page 183
Specify what browser to use to display the online help	"Specifying the browser used for online help" on page 185
Start the Tivoli Enterprise Portal to verify your installation.	"Starting the Tivoli Enterprise Portal client" on page 188
Use Web Start to download the run the desktop client	"Using Web Start to download and run the desktop client" on page 189

Installing and configuring the hub Tivoli Enterprise Monitoring Server

The following sections provide detailed information for installing and initially configuring the hub monitoring server:

- "Windows: Installing the hub monitoring server" on page 115
- "Linux or UNIX: Installing the hub monitoring server" on page 119

Note: IBM Tivoli Monitoring does not support multiple monitoring servers (hub or remote) on the same computer.

Windows: Installing the hub monitoring server

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 in the \WINDOWS subdirectory of IBM Tivoli Monitoring V6.2.0 Base DVD.

   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.

   Note: If you have another IBM Tivoli Monitoring component already installed on this computer, select **Modify** on the Welcome window to indicate that you are updating an existing installation. Click **OK** on the message telling you about preselected items. Then skip to Step 8.

3. On the Install Prerequisites window, read the information about the required levels of IBM Global Security Toolkit (GSKit) and IBM Java.

   The check box for each prerequisite is cleared if the correct level of the software is already installed. Otherwise, the check box is selected to indicated that the software is to be installed.

4. Click **Next**. The prerequisite software is installed if necessary.
5. Click **Accept** to accept the license agreement.
6. Choose the directory where you want to install the product. The default directory is C:\IBM\ITM. Click **Next**.
7. Type a 32-character encryption key. You can use the default key.

   Notes:

   a. Do not use any of the following characters in your key:
      - =
      - ’
      - |

   b. 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.

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

8. On the Select Features window, select the check box for **Tivoli Enterprise Monitoring Server**.

   When you select the **Tivoli Enterprise Monitoring Server** check box, all of the check boxes in the attached subtree are automatically selected. The support check boxes in the subtree are for installing application support files for monitoring agents to the monitoring server. You can leave all of the support check boxes selected so you do not need to reconfigure application support as new agent types are added to your environment, but adding support for many agents can extend the installation time considerably. If you do not intend to install a particular type of agent, you uncheck the selection box. For detailed information about application support, see “Installing and enabling application support” on page 159.

   Notes:

   a. If you have purchased monitoring agents that run on z/OS, but have not purchased IBM Tivoli Monitoring as a separate product, expand the **Tivoli Enterprise Monitoring Server** node. Clear the check boxes in the subtree

for the base agents except for the Warehouse Proxy and Summarization and Pruning Agents. (The *base* monitoring agents are included with the base IBM Tivoli Monitoring installation package: see "Installing monitoring agents" on page 148.)

b. If you are updating an existing installation (you selected **Modify** on the Welcome window), all check boxes on the Select Features window reflect your choices during the initial installation. Clearing a check box has the effect of *uninstalling* the component. Clear a check box only if you want to remove a component.

9. Click **Next** to display the Agent Deployment window.

   The Agent Deployment window lists monitoring agents on this installation image that you can add to the agent depot. The agent depot contains agents that you can deploy to remote computers. For information about how to deploy agents in the agent depot to remote computers, see Chapter 7, "Deploying monitoring agents across your environment," on page 195.

   Note: By default, the agent depot is located in the <*itm_installdir*>/CMS/depot directory on Windows. If you want to use a different directory, create the directory (if it does not exist) and specify the directory using the DEPOTHOME key in the KBBENV file.

   Select the agents, if any, that you want to add to the agent depot. (You can add agents to the agent depot at a later time by updating your installation.) Click **Next**.

10. If no IBM Tivoli Monitoring component has been previously installed on this computer, a window is displayed for you to select a program folder for the Windows Start menu. Select a program folder and click **Next**. The default program folder name is IBM Tivoli Monitoring.

11. If the TEPS Desktop and Browser Signon ID and Password window is displayed, enter and confirm the password to be used for logging on to the Tivoli Enterprise Portal. The default logon user ID, `sysadmin`, cannot be changed on this window.

    This password is required only when **Security: Validate Users** is enabled on the hub monitoring server. This window is not displayed if the sysadmin user ID has already been defined in the operating system.

12. Review the installation summary details. The summary identifies the components you are installing. Click **Next** to begin the installation.

    After the components are installed, a configuration window (called the Setup Type window) is displayed.

13. Clear the check boxes for any components that have already been installed and configured (at the current release level) on this computer, unless you want to modify the configuration. Click **Next** to start configuring all selected components.

14. Configure the Tivoli Enterprise Monitoring Server:

    a. Select the type of monitoring server you are configuring: **Hub** or **Remote**. For this procedure, select **Hub**.

    b. Verify that the name of this monitoring server is correct in the **TEMS Name** field. If it is not, change it.

       The default name is HUB_*host_name*, for example, HUB_itmserv16. *This name must be unique in the enterprise*.

    c. Identify the communications protocol for the monitoring server. You have four choices: IP.UDP, IP.PIPE, IP.SPIPE, or SNA. You can specify up to three

methods for communication. If the method you identify as Protocol 1 fails, Protocol 2 is used as a backup. If Protocol 2 fails, Protocol 3 is used as a backup.

Do not select any of the other options on this window (for example **Address Translation**, **Tivoli Event Integration Facility** or the option to configure **Hot Standby**). You can configure these options after installation is complete.

Important: Uncheck the box for **Security: Validate Users**. Use the procedures in "Configuring user authentication" on page 211 to configure security after installation is complete. If you decide to leave security enabled, and you want to use LDAP to authenticate users instead of the hub security system, use the information in "Configuring user authentication" on page 211 to complete the configuration.

d. Click **OK**.

e. Complete the following fields for the communications protocol for the monitoring server.

Table 30. Communications protocol settings for the hub monitoring server

Field	Description
IP.UDP Settings	
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. The default port is 1918.
IP.PIPE Settings	
Hostname 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 number is 1918.
IP.SPIPE Settings	
Hostname or IP Address	The host name or IP address for the hub monitoring server.
Port number	The listening port for the hub monitoring server. The default value is 3660.
SNA Settings	
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.

f. 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.

g. Click **OK** to continue.

15. If you selected **Tivoli Event Integration Facility**, provide the host name and port number for the TEC event server or Netcool/OMNIbus EIF probe to which you want to forward events and click **OK**.
16. Enable application support on the monitoring server.

    In Step 8 on page 115, you selected the base monitoring agents for which you wanted to install application support files on the monitoring server. In this step, you activate the application support through a process known as *seeding* the monitoring server.

    a. Specify the location of the monitoring server to which to add application support. You have two choices:
       - **On this computer**
       - **On a different computer**

       Click **OK**.

    b. Click **OK** on the Select the application support to add to the TEMS window.

       This window lists the monitoring agents that you selected in Step 8 on page 115. Click **OK** to begin seeding the monitoring server (using the SQL files listed on this window). This process can take up to 20 minutes.

    c. Click **Next** on the message that provides results for the process of adding application support. A return code of 0 (rc: 0) indicates that the process succeeded.

       Note: If the Application Support Addition Complete window is not displayed after 20 minutes, look in the IBM\ITM\CNPS\Logs\ seedk*pc*.log files (where *pc* is the two-character product code for each monitoring agent) for diagnostic messages that help you determine the cause of the problem. For a list of product codes, see Appendix D, "IBM Tivoli product codes," on page 437.

17. Configure the communication between any IBM Tivoli Monitoring component and the hub monitoring server:

    a. Specify the default values for IBM Tivoli Monitoring components to use when they communicate with the monitoring server.

       1) If agents must cross a firewall to access the monitoring server, select **Connection must pass through firewall**.
       2) 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 up to three methods for communication. If the method you identify as Protocol 1 fails, Protocol 2 is used as a backup. If Protocol 2 fails, Protocol 3 is used as a backup.

       Click **OK**.

    b. Complete the communication protocol fields for the monitoring server. See Table 30 on page 117 for definitions of these fields. Click **OK**.

18. Click **Finish** to complete the installation.
19. Click **Finish** on the Maintenance Complete window if you are updating an existing installation.

The Manage Tivoli Monitoring Services utility is opened. (This might take a few minutes.) You can start, stop, and configure IBM Tivoli Monitoring components with this utility.

Linux or UNIX: Installing the hub monitoring server

Use the following steps to install and configure the hub monitoring server on a Linux or UNIX computer.

Note: GSKit must be installed from a user ID with root or administrator authority. If you are running the installer program interactively as non-root, the installer will prompt you for the root password. If you do not supply the root password when prompted or supply an invalid password, then GSKit must be installed manually from a user ID with root or administrator authority when the installation has completed. If you perform the installation using a silent installation as non-root, the prompt for the root password is bypassed, and GSKit must be installed manually from a user ID with root or administrator authority after the silent installation has completed.

Table 31. Steps for installing a hub monitoring server on a Linux or UNIX computer

Steps	Where to find information
Install the hub monitoring server.	"Installing the monitoring server"
Configure the hub monitoring server.	"Configuring the hub monitoring server" on page 120
Add application support to the hub monitoring server.	"Adding application support to the hub monitoring server" on page 122

Note: IBM Tivoli Monitoring does not support multiple monitoring servers (hub or remote) on the same computer.

Installing the monitoring server

Use the following steps to install the monitoring server on a Linux or UNIX computer:

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.
3. If the directory you specified does not exist, you are asked whether to create it. Type 1 to create this directory.
4. The following prompt is displayed:

   ```
   Select one of the following:
   1) Install products to the local host.
   2) Install products to depot for remote deployment (requires TEMS).
   3) Install TEMS support for remote seeding
   4) Exit install.
   Please enter a valid number:
   ```

   Type 1 to start the installation and press Enter.

   The end user license agreement is displayed. Press Enter to read through the agreement.
5. Type 1 to accept the agreement and press Enter.
6. Type a 32-character encryption key and press Enter. If you want to use the default key, press Enter without typing any characters.

Notes:

a. Do not use any of the following characters in your key:
   - =
   - ’
   - |

b. 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.

A numbered list of available operating systems is displayed.

7. Type the number for the operating system on which you are installing the monitoring server. The default value is your current operating system. Press Enter.
8. Type 1 to confirm the operating system and press Enter.

   A numbered list of available components is displayed.
9. Type the number that corresponds to the Tivoli Enterprise Monitoring Server option. Press Enter.

   A list of the components to install is displayed.
10. Type 1 to confirm the installation.

    The installation begins.
11. When prompted, type a name for your monitoring server. For example: HUB_*hostname*. Do not use the fully qualified host name. Press Enter.
12. After all of the components are installed, you are asked whether you want to install components for a different operating system. Type 2 and press Enter.

Installation is complete. The next step is to configure your monitoring server.

Configuring the hub monitoring server

Use the following steps to configure the hub monitoring server:

Note: If you will be configuring user security, you should use root login ID to configure.

1. At the command line, change to the /opt/IBM/ITM/bin directory (or the directory where you installed IBM Tivoli Monitoring).
2. Run the following command:

   ```
   ./itmcmd config -S -t tems_name
   ```

   where *tems_name* is the name of your monitoring server (for example, HUB_itmdev17).
3. Press Enter to indicate that this is a hub monitoring server (indicated by the *LOCAL default).
4. 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, ip.spipe, or sna. 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 following information when prompted:

Table 32. UNIX monitoring server protocols and values

Protocol	Value	Definition
IP.UDP	IP Port Number	The port number for the monitoring server. The default is 1918.
SNA	Net 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.
	Log Mode	The name of the LU6.2 LOGMODE. The default value is ″CANCTDCS.″
IP.PIPE	IP.PIPE Port Number	The port number for the monitoring server. The default is 1918.
IP.SPIPE	IP.SPIPE Port Number	The port number for the monitoring server. The default is 3660.

8. Press Enter to *not* specify the name of the KDC_PARTITION. You can configure the partition file at a later time, as described in Appendix C, “Firewalls,” on page 427.
9. Press Enter when prompted for the path and name of the KDC_PARTITION.
10. If you want to use Configuration Auditing, press Enter. If you do not want to use this feature, type 2 and press Enter.
11. Press Enter to accept the default setting for the Hot Standby feature (none).

    For best results, wait until after you have fully deployed your environment to configure the Hot Standby feature for your monitoring server. See “Configuring failover support” on page 221 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).

    Important: Do *not* change this to set **Security: Validate User**. You can configure security after configuring the monitoring server, as described in “Configuring user authentication” on page 211.
14. If you want to forward situation events to either IBM Tivoli Enterprise Console (TEC) or the IBM Tivoli Netcool/OMNIbus console, type 1 and press Enter to enable the Tivoli Event Integration Facility. Complete the following additional steps:
    a. For EIF Server, type the hostname of the TEC event server or the hostname of the Netcool/OMNIbus EIF probe and press Enter.
    b. For EIF Port, type the EIF reception port number for the TEC event server or the Netcool/OMNIbus EIF probe and press Enter.
15. To disable Workflow Policy Activity event forwarding, type 1 and press Enter. Otherwise, press Enter to accept the default (2=NO). See the note in “Event integration with Tivoli Enterprise Console” on page 52 for more information.
16. Type 5 to accept the default SOAP configuration and exit the configuration.

    Note: You can configure any SOAP information at a later time. See Chapter 11, “Configuring IBM Tivoli Monitoring Web Services (SOAP Server),” on page 255 for information.

The monitoring server is now configured.

A configuration file is generated in the *install_dir*/config directory with the format *host_name*_ms_*tems_name*.config (for example, itmdev17_ms_HUBitmdev17.config).

Adding application support to the hub monitoring server

All monitoring agents require that application support files be installed on the monitoring servers (hub and remote), portal server, and portal desktop clients in your environment. Application support files contain the information required for agent-specific workspaces, helps, predefined situations, and other data.

When you installed the monitoring server on Linux or UNIX, following the instructions in "Installing the monitoring server" on page 119, the application support files for all base monitoring agents and other supported agents were automatically installed on the monitoring server. (The *base* monitoring agents are the monitoring agents included on the IBM Tivoli Monitoring installation media. Now you must enable the application support for those agents. The process of enabling application support is also referred to as *activating* or *adding* application support, and in the case of the monitoring server, as *seeding* the monitoring server.

Follow the instructions in this section to add application support for agents to a monitoring server on Linux or UNIX. For detailed information about application support, and for instructions to install and enable application support for non-base agents, refer to "Installing and enabling application support" on page 159 and "Configuring application support for non-Base monitoring agents" on page 164.

Use one of the following procedures to add application support for Base monitoring agents to a monitoring server:

Command-line procedure: Complete the following steps to enable application support on the monitoring server for base monitoring agents, using the Linux or UNIX command line:

1. Start the monitoring server by running the following command:

   ```
   ./itmcmd server start tems_name
   ```

2. Run the following command to add the application support:

   ```
   ./itmcmd support -t tems_name pc pc pc
   ```

   where *tems_name* is the name of the monitoring server (for example, HUB_itmserv16) and *pc* is the product code for each agent for which you want to enable application support.

   To view the product codes for the applications installed on this computer, run the following command:

   ```
   ./cinfo
   ```

   Type 1 when prompted to display the product codes for the components installed on this computer. See your product documentation for the product code for other agents.

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
   ```

GUI procedure: This section describes how to use the Manage Tivoli Enterprise Services window on a Linux Intel or UNIX computer to enable application support on a monitoring server that is located on the local computer. You can use this procedure as an alternative to the **itmcmd support** command. (This command

applies only to monitoring servers that are installed on the local computer. To enable application support on a monitoring server that is located on a remote computer, see "Configuring application support on a non-local monitoring server from a Linux or UNIX system" on page 179.)

This procedure assumes that you have installed the support files on this computer, and that X Windows is enabled on this computer.

Complete the following steps to enable application support from the Manage Tivoli Enterprise Services window on the local Linux or UNIX monitoring server:

1. Log on to the computer where the Tivoli Enterprise Portal Server is installed.
2. Start the Manage Tivoli Enterprise Monitoring Services utility:
   a. Change to the bin directory:
      `cd install_dir/bin`
   b. Run the following command using the parameters described in Table 33:
      `./itmcmd manage [-h ITMinstall_dir]`

      where:

Table 33. Parameters for the itmcmd manage command

-h	(optional) An option used to specify the installation directory.
ITMinstall_dir	The directory where the monitoring server is installed. The default installation directory is /opt/IBM/ITM.

   The Manage Tivoli Enterprise Monitoring Services window is displayed.
3. Start the monitoring server if it is not already started: Right-click **Tivoli Enterprise Monitoring Server** and click **Start**.
4. Right-click **Tivoli Enterprise Monitoring Server** and select one of the following options:
   - To enable all application support packages installed on this computer, click **Quick (all available support)**.
   - To select which application support packages you want to enable, click **Advanced . . .**
5. If you selected the **Advanced** option, the Install Product Support windows is displayed. Select the application support packages you want to install and click **Install**.
6. Stop and restart the monitoring server:
   a. Right-click **Tivoli Enterprise Monitoring Server** and click **Stop**.
   b. Right-click **Tivoli Enterprise Monitoring Server** and click **Start**.

Installing and configuring the remote monitoring servers

The following sections provide detailed information for installing and configuring a remote monitoring server:

- "Windows: Installing a remote monitoring server" on page 124
- "Linux or UNIX: Installing a remote monitoring server" on page 127

Note: IBM Tivoli Monitoring does not support multiple monitoring servers (hub or remote) on the same computer.

Windows: Installing a remote monitoring server

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

1. Launch the installation wizard by double-clicking the setup.exe file in the \WINDOWS subdirectory on the IBM Tivoli Monitoring V6.2.0 Base DVD or DVD image.

   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.

   Note: If you have another IBM Tivoli Monitoring component already installed on this computer, select **Modify** on the Welcome window to indicate that you are updating an existing installation. Click **OK** on the message telling you about preselected items. Then skip to Step 8.

3. On the Install Prerequisites window, read the information about the required levels of IBM Global Security Toolkit (GSKit) and IBM Java.

   The check box for each prerequisite is cleared if the correct level of the software is already installed. Otherwise, the check box is selected to indicated that the software is to be installed.

4. Click **Next**. The prerequisite software is installed if necessary.
5. Click **Accept** to accept the license agreement.
6. Choose the directory where you want to install the product. The default directory is C:\IBM\ITM. Click **Next**.
7. Type a 32-character encryption key. You can use the default key.

   Notes:

   a. Do not use any of the following characters in your key:
      - =
      - ’
      - |

   b. 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.

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

8. On the Select Features window, select the check box for **Tivoli Enterprise Monitoring Server**.

   When you select the **Tivoli Enterprise Monitoring Server** checkbox, all of the check boxes in the attached subtree are automatically selected. These check boxes are for installing application support files for base monitoring agents and other to the monitoring server. (The *base* monitoring agents are included with the base IBM Tivoli Monitoring installation package.) If you leave all of the application support check boxes selected, you do not need to reconfigure application support as new agent types are added to your environment. However, installing support for many agents at a time can increase the installation time and you may still have to add support for an agent later if it has been updated. For detailed information about application support, see “Installing and enabling application support” on page 159.

Notes:

a. If you have purchased monitoring agents that run on z/OS, but have not purchased IBM Tivoli Monitoring as a separate product, expand the **Tivoli Enterprise Monitoring Server** node. Clear all check boxes in the subtree except the check boxes labeled **Tivoli Enterprise Monitoring Server** and **Summarization and Pruning Agent**.

b. If you are updating an existing installation (you selected **Modify** on the Welcome window), all check boxes on the Select Features window reflect your choices during the initial installation. Clearing a check box has the effect of *uninstalling* the component. Clear a check box only if you want to remove a component.

9. If you want to install any agents on this remote monitoring server, expand **Tivoli Enterprise Monitoring Agents** and select the agents you want to install.

10. Click **Next** to display the Agent Deployment window.

    The Agent Deployment window lists monitoring agents on this installation image that you can add to the agent depot. The agent depot contains agents that you can deploy to remote computers. For information about how to deploy agents in the agent depot to remote computers, see Chapter 7, "Deploying monitoring agents across your environment," on page 195.

    Note: By default, the agent depot is located in the *<itm_installdir>*/CMS/depot directory on Windows. If you want to use a different directory, create the directory (if it does not exist) and specify the directory using the DEPOTHOME key in the KBBENV file.

    Select the agents, if any, that you want to add to the agent depot. (You can add agents to the agent depot at a later time by updating your installation.) Click **Next**.

11. If no IBM Tivoli Monitoring component has been previously installed on this computer, a window is displayed for you to select a program folder for the Windows Start menu. Select a program folder and click **Next**. The default program folder name is IBM Tivoli Monitoring.

12. If the TEPS Desktop and Browser Signon ID and Password window is displayed, enter and confirm the password to be used for logging on to the Tivoli Enterprise Portal. The default logon user ID, `sysadmin`, cannot be changed on this window. The logon password must match the password that you specified for sysadmin when you configured the hub monitoring server.

    This window is not displayed if the sysadmin user ID has already been defined in the operating system.

13. Review the installation summary details. The summary identifies the components you are installing. Click **Next** to begin the installation.

    After the components are installed, a configuration window (called the Setup Type window) is displayed.

14. Clear the check boxes for any components that have already been installed and configured (at the current release level) on this computer, unless you want to modify the configuration. Click **Next** to start configuring all selected components.

15. Configure the Tivoli Enterprise Monitoring Server:

    a. Select the type of monitoring server you are configuring: **Hub** or **Remote**. For this procedure, select **Remote**.

    b. Verify that the name of this monitoring server is correct in the **TEMS Name** field. If it is not, change it.

The default name is REMOTE_*host_name*, for example, REMOTE_itmserv16. *This name must be unique in the enterprise*.

c. Identify the communications protocol for the monitoring server. You have four choices: IP.UDP, IP.PIPE, IP.SPIPE, or SNA. You can specify up to three methods for communication. If the method you identify as Protocol 1 fails, Protocol 2 is used as a backup. If Protocol 2 fails, Protocol 3 is used as a backup.

d. Click **OK**.

e. Complete the following fields for the communications protocol for the monitoring server.

Table 34. Remote monitoring server communications protocol settings

Field	Description
IP.UDP Settings: Primary Hub TEMS	
Host name 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. The default port is 1918.
IP.PIPE Settings: Primary Hub TEMS	
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.
IP.SPIPE Settings: Primary Hub TEMS	
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.
SNA Settings: Remote TEMS	
Local LU Alias	The LU alias.
TP Name	The transaction program name for this monitoring server.
SNA Settings: Primary Hub TEMS	
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.

f. 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.

g. Click **OK** to continue.

16. Enable application support on the monitoring server.

In Step 8 on page 124, you selected the base monitoring agents for which you wanted to install application support files on the monitoring server. In this step, you activate the application support through a process known as *seeding* the monitoring server.

a. Specify the location of the monitoring server to which to add application support. You have two choices:
   - **On this computer**
   - **On a different computer**

   Click **OK**.

b. Click **OK** on the Select the application support to add to the TEMS window.

   This window lists the monitoring agents that you selected in Step 8 on page 124. Click **OK** to begin seeding the monitoring server (using the SQL files listed on this window). This process can take up to 20 minutes.

c. Click **Next** on the message that provides results for the process of adding application support. A return code of 0 (rc: 0) indicates that the process succeeded.

   Note: If the Application Support Addition Complete window is not displayed after 20 minutes, look in the IBM\ITM\CNPS\Logs\ seedk*pc*.log files (where *pc* is the two-character product code for each monitoring agent) for diagnostic messages that help you determine the cause of the problem. For a list of product codes, see Appendix D, "IBM Tivoli product codes," on page 437.

17. Configure the communication between any IBM Tivoli Monitoring component and the monitoring server:

    a. Specify the default values for IBM Tivoli Monitoring components to use when they communicate with the monitoring server.

       1) If agents must cross a firewall to access the monitoring server, select **Connection must pass through firewall**.

       2) 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 up to three methods for communication. If the method you identify as Protocol 1 fails, Protocol 2 is used as a backup. If Protocol 2 fails, Protocol 3 is used as a backup.

       Click **OK**.

    b. Complete the communication protocol fields for the monitoring server. See Table 34 on page 126 for definitions of these fields. Click **OK**.

18. Click **Finish** to complete the installation.
19. Click **Finish** on the Maintenance Complete window if you are updating an existing installation.

Linux or UNIX: Installing a remote monitoring server

Use the following steps to install and configure the remote monitoring server on a Linux or UNIX computer.

Table 35. Steps for installing a remote monitoring server on a Linux or UNIX computer

Steps	Where to find information
Install the remote monitoring server. Use the same instructions as for installing the hub monitoring server.	"Installing the monitoring server" on page 119
Configure the remote monitoring server.	"Configuring the remote monitoring server"
Add application support to the remote monitoring server. Use the same instructions as for adding application support to the hub monitoring server.	"Adding application support to the hub monitoring server" on page 122

Note: IBM Tivoli Monitoring does not support multiple monitoring servers (hub or remote) on the same computer.

Configuring the remote monitoring server

Use the following steps to configure the remote monitoring server:

1. At the command line change to the /opt/IBM/ITM/bin directory (or the directory where you installed IBM Tivoli Monitoring).
2. Run the following command:

   ```
   ./itmcmd config -S -t tems_name
   ```

   where *tems_name* is the name of your monitoring server (for example, remote_itmdev17).
3. Type `remote` to indicate that this is a remote monitoring server.
4. Press Enter to accept the default host name for the hub monitoring server. This should be the host name for hub 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, ip.spipe, or sna. 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 following information when prompted:

Table 36. UNIX monitoring server protocols and values

Protocol	Value	Definition
IP.UDP	IP Port Number	The port number for the monitoring server. The default is 1918.
SNA	Net 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.
	Log Mode	The name of the LU6.2 LOGMODE. The default value is "CANCTDCS."

Table 36. UNIX monitoring server protocols and values (continued)

Protocol	Value	Definition
IP.PIPE	IP.PIPE Port Number	The port number for the monitoring server. The default is 1918.
IP.SPIPE	IP.SPIPE Port Number	The port number for the monitoring server. The default is 3660.

8. Press Enter to *not* specify the name of the KDC_PARTITION.

   Note: You can configure the partition file at a later time, as described in Appendix C, "Firewalls," on page 427.
9. Press Enter when prompted for the path and name of the KDC_PARTITION.
10. If you want to use Configuration Auditing, press Enter. If you do not want to use this feature, type `n` and press Enter.
11. Press Enter to accept the default setting for the Hot Standby feature (none).

    For best results, wait until after you have fully deployed your environment to configure the Hot Standby feature for your monitoring server. See "Configuring failover support" on page 221 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).

    Note: This option is valid only for a hub monitoring server.
14. For Tivoli Event Integration, type `2` and press Enter.

    Note: This option is valid only for a hub monitoring server.
15. At the prompt asking if you want to disable Workflow Policy/Tivoli Emitter Agent event forwarding, press Enter to accept the default (2=NO).

    Note: This option is valid only for a hub monitoring server.
16. At the prompt asking if you want to configure the SOAP hubs, press Enter to save the default settings and exit the installer.

    Note: This option is valid only for a hub monitoring server.

The monitoring server is now configured.

A configuration file is generated in the *install_dir*`/config` directory with the format *host_name*`_ms_`*tems_name*`.config` (for example, `itmdev17_ms_HUBitmdev17.config`).

Installing the Tivoli Enterprise Portal Server

You can install the Tivoli Enterprise Portal Server on Windows, Linux or AIX. Follow the instructions for your operating system:

- "Windows: Installing the portal server" on page 130
- "Linux or AIX: Installing the portal server" on page 136

Note: When you install or upgrade the Tivoli Enterprise Portal Server, the Tivoli Enterprise Portal Server Extensions software is automatically installed in the

same directory as the portal server. Tivoli Portal Server Extensions is required for some products that use the Tivoli Enterprise Portal (for example, IBM Tivoli Composite Application Manager for Service Oriented Architecture). The Tivoli Portal Server Extensions software is supported on the same operating systems as the Tivoli Enterprise Portal Server.

Windows: Installing the portal server

The installation procedure for a portal server on Windows includes steps for configuring the connection between the portal server and the following components:

- The hub monitoring server
- The portal server database
- The Tivoli Data Warehouse database

Note: If you have not set up the Tivoli Data Warehouse, complete this procedure but click **No** when asked if you want to configure the connection to the data warehouse. You can reconfigure the connection after you set up the warehouse. See Step 17 on page 134 for more information.

Complete the following steps to install the Tivoli Enterprise Portal Server and portal client on a Windows computer:

1. Launch the installation wizard by double-clicking the setup.exe file in the \WINDOWS subdirectory of the IBM Tivoli Monitoring V6.2.0 Base DVD.
2. Click **Next** on the Welcome window.

   Note: If you have another IBM Tivoli Monitoring component already installed on this computer, select **Modify** on the Welcome window to indicate that you are updating an existing installation. Click **OK** on the message telling you about preselected items. Then skip to Step 9.
3. On the Install Prerequisites window, read the information about the required levels of IBM Global Security Toolkit (GSKit) and IBM Java.

   The check box for each prerequisite is cleared if the correct level of the software is already installed. Otherwise, the check box is selected to indicate that the software is to be installed.
4. Click **Next**. The prerequisite software is installed if necessary.
5. Read and accept the software license agreement by clicking **Accept**.
6. If you do not have an RDBMS (IBM DB2 or Microsoft SQL Server) installed on this computer, a message regarding potentially missing required software is displayed. Stop the installation, install the RDBMS, and begin the installation again.
7. Specify the directory where you want to install the portal server software and accompanying files. The default location is C:\IBM\ITM. Click **Next**.
8. Type an encryption key to use. This key should be the same as what was used during the installation of the hub monitoring server to which this portal server will connect. Click **Next** and then **OK** to confirm the encryption key.
9. On the Select Features window, select **Tivoli Enterprise Portal Server** from the list of components to install.

   When you select the **Tivoli Enterprise Portal Server** check box, all of the check boxes in the attached subtree are automatically selected. The support check boxes in the subtree are for installing application support files for base monitoring agents to the monitoring server. (The *base* monitoring agents are included with the base IBM Tivoli Monitoring installation package.) It is best

to leave all of the support check boxes selected so you do not need to reconfigure application support as new agent types are added to your environment. For detailed information about application support, see "Installing and enabling application support" on page 159.

Notes:

a. If you have purchased monitoring agents that run on z/OS, but have not purchased IBM Tivoli Monitoring as a separate product, expand the **Tivoli Enterprise Portal Server** node. Clear all check boxes in the subtree except the check boxes labeled **Tivoli Enterprise Portal Server** and, optionally, **TEC GUI Integration**. (See Step 10a.)

b. If you are updating an existing installation (you selected **Modify** on the Welcome window), all check boxes on the Select Features window reflect your choices during the initial installation. Clearing a check box has the effect of *uninstalling* the component. Clear a check box only if you want to remove a component.

c. The IBM Eclipse Help Server is automatically selected when you select the portal server.

10. Optionally select the following additional components to install:

    a. If you want to view events on the IBM Tivoli Enterprise Console event server through the Tivoli Enterprise Portal, expand **Tivoli Enterprise Portal Server** and ensure that **TEC GUI Integration** is selected.

    b. If you want to install a portal desktop client on this computer, select **Tivoli Enterprise Portal Desktop Client**.

       When you select the **Tivoli Enterprise Portal Desktop Client** check box, all of the check boxes in the attached subtree are automatically selected. These check boxes are for installing application support files for base monitoring agents to the portal desktop client. Leave these check boxes selected as you did for the portal server in Step 9 on page 130.

       Note: If you have purchased monitoring agents that run on z/OS, but have not purchased IBM Tivoli Monitoring as a separate product, expand the **Tivoli Enterprise Portal Desktop Client** node. Clear all check boxes in the subtree except the check boxes labeled **Tivoli Enterprise Portal Desktop Client** and, optionally, **TEC GUI Integration**.

11. Click **Next**.

12. If a monitoring server is not installed on this computer, go to Step 13 on page 132.

    If you are installing the portal server on a computer that already has a monitoring server installed, the Agent Deployment window is displayed.

    The Agent Deployment window lists monitoring agents on this installation image that you can add to the agent depot. The agent depot contains agents that you can deploy to remote computers. For information about how to deploy agents in the agent depot to remote computers, see Chapter 7, "Deploying monitoring agents across your environment," on page 195.

    Note: By default, the agent depot is located in the *<itm_installdir>*/CMS/depot directory on Windows. If you want to use a different directory, create the directory (if it does not exist) and specify the directory using the DEPOTHOME key in the KBBENV file.

Select the agents, if any, that you want to add to the agent depot. (You can add agents to the agent depot at a later time by updating your installation.) Click **Next**.

13. If no IBM Tivoli Monitoring component has been previously installed on this computer, a window is displayed for you to select a program folder for the Windows Start menu. Select a program folder and click **Next**. The default program folder name is IBM Tivoli Monitoring.
14. Review the installation summary details. The summary identifies what you are installing and where you chose to install it. Click **Next** to start the installation.

    After installation is complete, a configuration window (called the Setup Type window) is displayed.
15. Clear the check boxes for any components that have already been installed and configured (at the current release level) on this computer, unless you want to modify the configuration. (For example, clear the check box for the Tivoli Enterprise Monitoring Server if it has already been installed and configured on this computer.) Click **Next** to start configuring all selected components.
16. Configure communications for the Tivoli Enterprise Portal Server:
    a. Type the host name of the computer where you are installing the portal server. (The host name of this computer is displayed by default.) Click **Next**.
    b. If more than one RDBMS product is installed on this computer, a window is displayed for you to choose the RDBMS product you want to use. Choose **IBM DB2** or **SQL Server** and click **Next**.

       Note: Each instance of the restricted-use version of DB2 UDB Enterprise Edition V9.1 provided for use with the portal server and the Tivoli Data Warehouse must be registered. See "Registering the DB2 product license key using the db2licm command" on page 79.
    c. A window is displayed for you to configure the connection between the portal server and the *portal server database* (TEPS database).

       The installation program uses the information on this window to automatically perform the following tasks:
       - Create the portal server database.
       - Create a database user for the portal server to use to access the database.
       - Configure the ODBC connection between the portal server and the database.

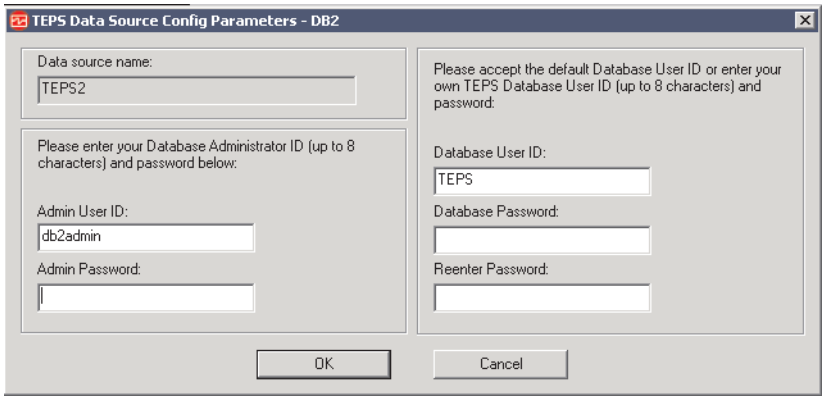


Figure 21. Configuration window for the portal server database using DB2

Figure 21 shows the configuration window for a portal server database using DB2. The configuration window for a Microsoft SQL Server database is similar. The fields on the configuration window are described in the following table:

Table 37. Configuration information for the portal server database

Field	DB2 default	MS SQL default	Description
Admin User ID	db2admin	sa	The database administrator ID.
Admin Password	(no default)	(no default)	The password for the database administrator ID.
Database User ID	TEPS	cnps	The login name of the database user that the portal server will use to access the database.
Database Password	(no default)	(no default)	The password for the database login user. If your environment requires complex passwords (passwords that require both alpha and numeric characters), specify a password that complies with these requirements.
Reenter password	(no default)	(no default)	Confirm the password by entering it again.

d. Optionally change the default values for the administrator ID and database user ID. Enter passwords for the administrator and database user. Click **OK**.

e. Click **OK** on the message that tells you that the portal server configuration was successful.

f. Click **Next** to accept the default Tivoli Data Warehouse user ID and password. (You can change these values in a later step.)

   This is the warehouse user ID. The same ID and password must be used by all components connecting to the Tivoli Data Warehouse, including the Tivoli Enterprise Portal Server, Warehouse Proxy Agents and the Summarization and Pruning Agent.

g. Configure the connection between the portal server and the hub Tivoli Enterprise Monitoring Server:

   1) Select the communications protocol that the monitoring server uses from the **Protocol** drop-down list. You can also specify whether the

connection between the portal server and the hub monitoring server passes through a firewall. Click **OK**.

2) Enter the host name or IP address and the port number for the hub monitoring server. Click **OK**.

17. A message is displayed asking if you want to reconfigure the warehouse connection for the portal server. Do one of the following:
    - Click **No** if you have not set up a Tivoli Data Warehouse.

      Follow the instructions later in this book for implementing a Tivoli Data Warehouse solution, beginning with Chapter 12, "Tivoli Data Warehouse solutions," on page 265. These instructions will direct you to reconfigure the connection between the portal server and the warehouse database after you have completed all preliminary setup tasks.

      If you select **No**, go to Step 22 on page 136.
    - Click **Yes** if you have completed the tasks for setting up a Tivoli Data Warehouse and want to configure the connection between the portal server and the Tivoli Data Warehouse database at this time. (You can choose to configure the connection later.) The prerequisite tasks and the information you need to configure the connection for each database type are described in the following steps.
18. To configure a connection between the portal server and a DB2 data warehouse, complete the following steps:
    a. Verify that you have completed the following tasks:
       - Created a warehouse database using DB2
       - Created a warehouse user on the computer where you created the warehouse database.

         The *warehouse user* is the user account (user ID and password) used by the portal server and other warehousing components to access the warehouse database.
       - Activated the UNIX listeners on the computer where the warehouse database is located if the warehouse database is installed on UNIX
       - Installed a DB2 client on the portal server if the data warehouse is remote and the portal server database does not use DB2
       - Cataloged the warehouse database on the computer where you are installing the portal server if the warehouse database is remote from the portal server.

       These tasks are described in Chapter 13, "Tivoli Data Warehouse solution using DB2," on page 273.

    b. Gather the following information: data source name, database name, database administrator ID and password, warehouse user ID and password. The warehouse user ID is the one declared in the configuration panel of the Warehouse Proxy Agent. This user ID serves as the first part of the name of all the tables created in the Warehouse database. If you do not declare the same user ID when configuring the Tivoli Enterprise Portal server you will not be able to see the Warehouse tables with the portal client even if they exist in the database.

    c. Complete the Configuring a Windows portal server (ODBC connection) procedure, starting from Step 4 on page 293.
19. To configure a connection between the portal server and a Microsoft SQL Server data warehouse, complete the following steps:
    a. Verify that you have completed the following tasks:
       - Created a warehouse database using Microsoft SQL Server

- Created a warehouse user on the computer where you created the warehouse database.

  The *warehouse user* is the user account (user ID and password) used by the portal server and other warehousing components to access the warehouse database.
- Installed a Microsoft SQL Server client on the portal server if the data warehouse is remote and the portal server database does not use Microsoft SQL Server
- Configured a remote client connection on the computer where you are installing the portal server if the warehouse database is remote from the portal server.

These tasks are described in Chapter 14, "Tivoli Data Warehouse solution using Microsoft SQL Server," on page 299.

b. Gather the following information: data source name, database name, database administrator ID and password, warehouse user ID and password. The warehouse user ID is the one declared in the configuration panel of the Warehouse Proxy Agent. This user ID serves as the first part of the name of all the tables created in the Warehouse database. If you do not declare the same user ID when configuring the Tivoli Enterprise Portal server you will not be able to see the Warehouse tables with the portal client even if they exist in the database.

c. Complete the procedure Configuring the portal server (ODBC connection), starting from Step 4 on page 312.

20. To configure a connection between the portal server and an Oracle data warehouse, complete the following steps:

    a. Verify that you have completed the following tasks:
    - Created a warehouse database using Oracle
    - Created a warehouse user on the computer where you created the warehouse database.

      The *warehouse user* is the user account (user ID and password) used by the portal server and other warehousing components to access the warehouse database.
    - Activated the Oracle listener on the computer where the warehouse database is located
    - Installed an Oracle client on the portal server
    - Created a TNS Service Name on the computer where you are installing the portal server if the warehouse database is remote from the portal server.

    These tasks are described in Chapter 15, "Tivoli Data Warehouse solution using Oracle," on page 315.

    b. Gather the following information: the data source name, database name, database administrator ID and password, and the warehouse user ID and password. The warehouse user ID is the one declared in the configuration panel of the Warehouse Proxy Agent. This user ID serves as the first part of the name of all the tables created in the Warehouse database. If you do not declare the same user ID when configuring the Tivoli Enterprise Portal server you will not be able to see the Warehouse tables with the portal client even if they exist in the database.

    c. Complete the procedure Configuring a Windows portal server (ODBC connection), starting from Step 4 on page 331.

21. Configure the default connector for the Common Event Console.

The default connector retrieves situation events reported to Tivoli Enterprise Monitoring Servers for display in the Common Event Console. You can configure connectors for other event management systems after you have completed the product installation. For configuration instructions, see *IBM Tivoli Monitoring: Administrator's Guide*.

Click **OK** to accept the default values or specify values for the following fields, then click **OK**:

Enable this connector
Select `Yes` to enable the connector to collect and display situation events in the common event console, or `No` to configure the connector without enabling it. The connector is enabled by default.

Connector name
The name that is to be displayed in the common event console for this connector. The default name is ITM1.

Maximum number of events for this connector
The maximum number of events that are to be available in the common event console for this connector. The default is 100 events.

View closed events
Select `No` to display only active events in the Common Event Console for this connector. Select `Yes` to view both active and closed events. By default, only active events are displayed.

22. Configure the default communication between any monitoring agents installed on this computer and the hub Tivoli Enterprise Monitoring Server:
    a. Click **OK** to accept the default communications protocol.
    b. Ensure that the host name and port number of the Tivoli Enterprise Monitoring Server are correct. Click **OK**.
23. Click **Finish** to complete the installation.
24. Click **Finish** on the Maintenance Complete window if you are updating an existing installation.

Linux or AIX: Installing the portal server

Complete the procedures in this section to install and configure the Tivoli Enterprise Portal Server and portal client on a Linux or AIX computer.

Important: Run these installation and configuration procedures as either the root user or as the DB2 administrator. If you are configuring the Tivoli Enterprise Portal Server using the DB2 administrator ID, then:

- The configuration ID must be the same as the ID used to install the Tivoli Enterprise Portal Server.
- The configuration ID must be the same as the ID specified during the configuration dialog for the DB2 Admin ID.
- The configuration ID must have the proper DB2 authority/rights to attach to the DB2 Instance Name specified during the configuration dialog.
- The ID specified during the configuration dialog for the DB2 User ID must be an already existing ID. You may not allow the configuration dialog to attempt to create the user. For the GUI dialog, ensure that the check box for **Create the user** is cleared. For the CLI dialog, ensure that the response for Create New User is NO. After you have installed and configured the portal server, you can use a different user to run the portal server, as long as that user has access to the binaries used by the portal server.

GSKit must be installed from a user ID with root or administrator authority. If you are running the installer program interactively as non-root, the installer will prompt you for the root password. If you do not supply the root password when prompted or supply an invalid password, then GSKit must be installed manually from a user ID with root or administrator authority when the installation has completed. If you perform the installation using a silent installation as non-root, the prompt for the root password is bypassed, and GSKit must be installed manually from a user ID with root or administrator authority after the silent installation has completed.

Table 38. Steps for installing a portal server on a Linux or AIX computer

Steps	Where to find information
Install the portal server.	"Installing the portal server on Linux or AIX"
Configure the portal server.	"Configuring the portal server on Linux or AIX: command-line procedure" on page 139 –OR– "Configuring the portal server on Linux or AIX: GUI procedure" on page 143
Start the portal server.	"Starting the portal server" on page 148

Installing the portal server on Linux or AIX

Complete the following steps to install the portal server:

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 type the full path to a different directory.
3. If the installation directory does not already exist, you are asked if you want to create it. Type y to create this directory and press Enter.
4. The following prompt is displayed:

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

   Please enter a valid number:
   ```

   Type 1 to start the installation and display the software license agreement.
5. Press Enter to read through the agreement.
6. Type 1 to accept the agreement and press Enter.
7. Enter a 32-character encryption key or press Enter to accept the default key. This key should be the one used during the installation of the monitoring server to which this portal server will connect.

   A numbered list of available operating systems is displayed.
8. Type the number for the operating system on which you are installing the portal server. The default value is your current operating system. Press Enter.
9. Type 1 to confirm the operating system and press Enter.

   A numbered list of products available for installation is displayed.

10. Type the number for `Tivoli Enterprise Portal Server` and press Enter.

    A message is displayed indicating that the Tivoli Enterprise Portal Server is about to be installed.

    Note: The IBM Eclipse Help Server is automatically installed when you install the Tivoli Enterprise Portal.

11. Type 1 to confirm the installation.

    The installation begins.

12. After the Tivoli Enterprise Portal Server is installed, you are asked whether you want to install additional products or product support packages. Type 1 and press Enter.

    The installer presents a numbered list of products and application support packages.

13. Install the required application support packages.

    All monitoring agents require that application support files be installed on the monitoring servers (hub and remote), portal server, and portal desktop clients in your environment. Application support files contain the information required for agent-specific workspaces, helps, predefined situations, and other data.

    This step installs the application support files for base monitoring agents. The *base* monitoring agents are included with the base IBM Tivoli Monitoring installation package. For detailed information about application support, see "Installing and enabling application support" on page 159.

    When you entered 1 in the preceding step, the installer presents a numbered list of items, including the following application support packages:

    ```
    Tivoli Enterprise Portal Browser Client support
    Tivoli Enterprise Portal Server support
    ```

    Note: The Tivoli Enterprise Portal Browser Client support package is portal server code that supports the browser clients. You must install the browser client support package on the computer where you install the portal server if you want to connect to it using a browser client.

    Complete the following steps to install the portal server and browser client support packages for the base monitoring agents:

    a. Type the number that corresponds to `Tivoli Enterprise Portal Browser Client support` and press Enter.

       A numbered list of base monitoring agents is displayed.

    b. Type the numbers that correspond to the base monitoring agents for which you want to install the application support package, or type the number that corresponds to `All of the above`. Type the numbers on the same line separated by spaces or commas (,). Press Enter.

       It is best to select all of the base monitoring agents (`All of the above`) so you do not need to reconfigure application support as new agent types are added to your environment.

    c. Type 1 to confirm the installation and press Enter.

       The installation begins.

    d. After the support package is installed, you are asked whether you want to install additional products or product support packages. Enter 1 and repeat the preceding steps for the `Tivoli Enterprise Portal Server support` package.

Note: This step installs the application support files. However, you must *enable* the application support by configuring the portal server. The next two sections show you how to configure the portal server.

14. After you are finished installing the portal server and browser client packages, you are asked whether you want to install additional products or product support packages. Type 2 and press Enter.

Configuring the portal server on Linux or AIX: command-line procedure

Configure the portal server using either the command line procedure in this section or the GUI procedure in "Configuring the portal server on Linux or AIX: GUI procedure" on page 143.

Either of these configuration procedures accomplishes the following tasks:

- Automatically enables application support on the portal server for the base monitoring agents. (See Step 13 on page 138 of the installation procedure.)
- Includes steps for configuring the connection between the portal server and the following components:
  - The hub monitoring server
  - The portal server database
  - The Tivoli Data Warehouse database

Note: If you have not set up the Tivoli Data Warehouse, complete this procedure but accept the defaults at the prompts for configuring the connection to the data warehouse. You can reconfigure the connection after you set up the warehouse. See Step 8 on page 141 for more information.

Complete the following steps to configure the Tivoli Enterprise Portal Server from the command line on Linux or AIX:

1. Log on to the computer where the Tivoli Enterprise Portal Server is installed.
2. At the command line change to the *ITMinstall_dir*/bin directory, where *ITMinstall_dir* is the directory where you installed the product.
3. Run the following command to start configuring the Tivoli Enterprise Portal Server:

   ```
   ./itmcmd config -A cq
   ```

   where `cq` is the product code for the portal server.
4. Edit the ITM Connector settings.

   The ITM Connector retrieves situation events reported to Tivoli Enterprise Monitoring Servers for display in the Common Event Console. If you do not enable the connector, you will not see any events in the Common Event Console. You can configure connectors for other event management systems after you have completed the product installation. For configuration instructions, see the *IBM Tivoli Monitoring: Administrator's Guide*.

   To enable the connector:

   a. Press Enter to accept the default for the following prompt:

      ```
      Edit 'ITM Connector' settings? [ 1=Yes, 2=No ] (default is: 1):
      ```

   b. Press Enter to enable the connector.

   c. Press Enter to accept the default name of ITM1 or type your preferred name and press Enter. This is the name that is to be displayed in the common event console for this connector.

d. Press Enter to accept the default number of events (100) that are to be available in the common event console for this connector, or type the number of events you would like to see displayed and press Enter.

e. Type 2 and press Enter to display only active events in the Common Event Console for this connector. Type 1 and press Enter to view both active and closed events. By default, only active events are displayed.

f. Type 2 and press Enter to skip defining data for extra columns in the Common Event Console.

When you define a Tivoli Enterprise Console or Tivoli Netcool/OMNIbus connector, you can define the information that is to be mapped to each of these customizable columns. See the *IBM Tivoli Monitoring: Administrator's Guide* for information on configuring these connectors.

5. Press Enter when you are asked if the agent connects to a monitoring server. (Although the prompt refers to an *agent*, this command is used to configure the portal server.)
6. Configure the connection between the portal server and the hub monitoring server:
   a. Type the host name for the hub monitoring server and press Enter.
   b. Type the protocol that the hub monitoring server uses to communicate with the portal server. You have four choices: IP.UDP, SNA, IP.PIPE, or IP.SPIPE.
   c. If you want to set up a backup protocol, enter that protocol and press Enter. If you do not want to use a backup protocol, press Enter without specifying a protocol.
   d. Depending on the type of protocol you specified, provide the following information as described in Table 39 when prompted:

Table 39. Hub monitoring server protocols and values

Protocol	Value	Definition
IP.UDP	IP Port Number	The port number for the monitoring server. The default is 1918.
SNA	Net 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.
	Log Mode	The name of the LU6.2 LOGMODE. The default value is `CANCTDCS`.
IP.PIPE	IP.PIPE Port Number	The port number for the monitoring server. The default is 1918.
IP.SPIPE	IP.SPIPE Port Number	The port number for the monitoring server. The default is 3660.

   e. Press Enter when you are asked if you want to configure the connection to a secondary monitoring server. The default value is `none`.
   f. Press Enter to accept the default for the Optional Primary Network Name (none).

g. Press Enter to accept the default setting for SSL between the portal server and clients (N). By default, SSL is disabled. To enable SSL, type 1 and press Enter.

7. Configure the connection between the portal server and the portal server database:
   a. Type the DB2 instance name. The default value is db2inst1. Press Enter.
   b. Type the DB2 administrator ID. The default is db2inst1. Press Enter.

      Note: The DB2 Administrator account was created during DB2 installation. Each instance of the restricted-use version of DB2 UDB Enterprise Edition V9.1 provided for use with the portal server and the Tivoli Data Warehouse must be registered. See "Registering the DB2 product license key using the db2licm command" on page 79.
   c. Type the password for the DB2 administrator ID and press Enter.
   d. Confirm the password for the DB2 administrator ID by typing it again. Press Enter.
   e. Type the name of the portal server database. The default is TEPS. Press Enter.
   f. Type the login name of the database user that the portal server will use to access the database. The default is itmuser. Press Enter.
   g. Type the password for the database user and press Enter.
   h. Confirm the password for the database user by typing it again. Press Enter.
   i. You are asked if you want to create the DB2 login user if it does not exist. Type 1 and press Enter.
8. You are asked if you are using DB2 or Oracle for the Tivoli Data Warehouse. Enter D for DB2, J for Oracle JDBC. DB2 is the default.

> **Note**
> This prompt and all remaining prompts ask for information to configure the connection between the portal server and the Tivoli Data Warehouse database. If you have not set up a Tivoli Data Warehouse, accept the defaults at these prompts. Follow the instructions later in this book for implementing a Tivoli Data Warehouse solution, beginning with Chapter 12, "Tivoli Data Warehouse solutions," on page 265. These instructions will direct you to reconfigure the connection between the portal server and the warehouse database after you have completed all preliminary setup tasks.

9. Do one of the following:
   - If you have not set up a Tivoli Data Warehouse:
     a. Press Enter to accept the DB2 default (even if you are going to create the Tivoli Data Warehouse using Oracle).
     b. Press Enter at all remaining prompts to accept the defaults.

     –OR–
   - Configure a connection between the portal server and a DB2 warehouse database.

     Before you configure the connection, verify that you have already completed the following tasks:

     – Created a warehouse database using DB2

– Created a warehouse user on the computer where you created the warehouse database.

  The *warehouse user* is the user account (user ID and password) used by the portal server and other warehousing components to access the warehouse database.

– Cataloged the warehouse database on the computer where you are installing the portal server if the warehouse database is remote from the portal server

– Activated the UNIX listeners on the computer where the warehouse database is located if the warehouse database is installed on UNIX.

These tasks are described in Chapter 13, "Tivoli Data Warehouse solution using DB2."

To perform the steps for configuring the connection between the portal server and the DB2 data warehouse, you will need the name of the warehouse database and the user ID and password of the warehouse user. Press Enter after answering each prompt:

a. Press Enter to accept the DB2 default.

b. Enter the name of the Tivoli Data Warehouse database. The default is `WAREHOUS`.

c. Enter the user ID of the warehouse user. The default is `itmuser`.

   Note: The warehouse user ID must be the one declared in the configuration panel of the Warehouse Proxy Agent. This user ID serves as the first part of the name of all the tables created in the Warehouse database. If you do not declare the same user ID when configuring the Tivoli Enterprise Portal server you will not be able to see the Warehouse tables with the portal client even if they exist in the database.

d. Enter the password of the warehouse user.

e. Confirm the password by entering it again.

–OR–

- Configure a connection between the portal server and an Oracle warehouse database.

  Before you configure the connection, verify that you have already completed the following tasks:

  – Created a warehouse database using Oracle

  – Created a warehouse user on the computer where you created the warehouse database.

    The *warehouse user* is the user account (user ID and password) used by the portal server and other warehousing components to access the warehouse database.

  – Activated the Oracle listener on the computer where the warehouse database is located

  – Installed an Oracle JDBC Type 4 driver on the portal server.

  These tasks are described in Chapter 15, "Tivoli Data Warehouse solution using Oracle."

  To perform the steps for configuring the connection between the portal server and the Oracle data warehouse, you will need:

  – The name of the warehouse database and the user ID and password of the warehouse user

– The location, name, and URL of the JDBC driver

Press Enter after answering each prompt:

a. Enter `oracle` at the prompt asking if you are using DB2 or Oracle for the Warehouse.
b. Enter the name of the Tivoli Data Warehouse database. The default is `WAREHOUS`.
c. Enter the user ID of the warehouse user. The default is `itmuser`.

   Note: The warehouse user ID must be the one declared in the configuration panel of the Warehouse Proxy Agent. This user ID serves as the first part of the name of all the tables created in the Warehouse database. If you do not declare the same user ID when configuring the Tivoli Enterprise Portal server you will not be able to see the Warehouse tables with the portal client even if they exist in the database.
d. Enter the password of the warehouse user.
e. Confirm the password by entering it again.
f. Enter the full path name of the Oracle Type 4 JDBC driver JAR file as follows:

   oracleinstalldir`/jdbc/lib/ojdbc14.jar`

   where *oracleinstalldir* is the directory location of the JDBC driver JAR file on this computer.
g. Enter the following JDBC driver name:

   `oracle.jdbc.driver.OracleDriver`
h. Enter the JDBC driver URL. This is the Oracle-defined URL that identifies the locally or remotely installed Oracle instance used for the Tivoli Data Warehouse. The following entry is an example:

   `jdbc:oracle:thin:@localhost:1521:WAREHOUS`

   – If the warehouse database is located on a remote computer, replace `localhost` with the host name of the remote computer.
   – Change the default port number (`1521`) and Tivoli Data Warehouse name (`WAREHOUS`) if they are different.
i. Enter any user-defined attributes that are used to customize the behavior of the driver connection. Use semi-colons (;) to delimit the attributes. Press Enter to finish the configuration.

A message is displayed telling you that InstallPresentation is running, and then a message telling you that the installation has completed.

Configuring the portal server on Linux or AIX: GUI procedure

Configure the portal server using either the GUI procedure in this section or the command line procedure in “Configuring the portal server on Linux or AIX: command-line procedure” on page 139.

Either of these configuration procedures accomplishes the following tasks:

- Automatically enables application support on the portal server for the base monitoring agents.
- Includes steps for configuring the connection between the portal server and the following components:
  – The hub monitoring server
  – The portal server database

– The Tivoli Data Warehouse database

Note: If you have not set up the Tivoli Data Warehouse, complete this procedure but accept the defaults at the prompts for configuring the connection to the data warehouse. You can reconfigure the connection after you set up the warehouse. See Step 8 on page 141 for more information.

Complete the following steps to configure the Tivoli Enterprise Portal Server from the Tivoli Enterprise Monitoring Services window on Linux or AIX:

1. Log on to the computer where the Tivoli Enterprise Portal Server is installed.
2. Start the Manage Tivoli Enterprise Monitoring Services utility:
   a. Change to the bin directory:
      `cd install_dir/bin`
   b. Run the following command using the parameters described in Table 40:
      `./itmcmd manage [-h ITMinstall_dir]`

      where:

Table 40. Parameters for the itmcmd manage command

-h	(optional) An option used to specify the installation directory.
ITMinstall_dir	The directory where the portal server is installed. The default installation directory is /opt/IBM/ITM.

   The Manage Tivoli Enterprise Monitoring Services window is displayed.
3. Right-click **Tivoli Enterprise Portal Server** and click **Configure**.
   The Common Event Console Configuration window is displayed.
4. Click **OK** to accept the default values for the ITM Connector, or specify your preferred values and then click OK.
   The ITM Connector retrieves situation events reported to Tivoli Enterprise Monitoring Servers for display in the Common Event Console. You can configure connectors for other event management systems after you have completed the product installation. For configuration instructions, see *IBM Tivoli Monitoring: Administrator's Guide*.
   The Configure Tivoli Enterprise Portal Server window is displayed.

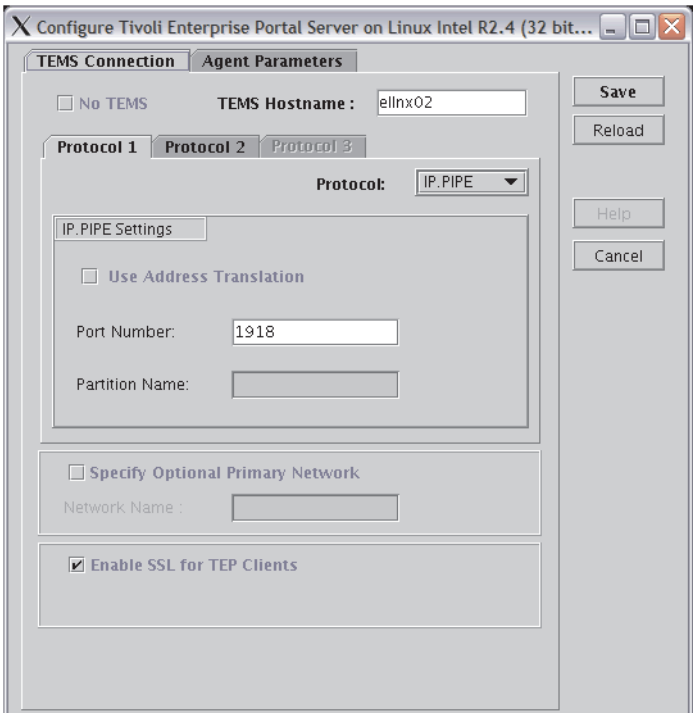


Figure 22. Registering the portal server with the Tivoli Enterprise Monitoring Server

5. On the TEMS Connection page, enter information about the Tivoli Enterprise Monitoring Server to which the Tivoli Enterprise Portal Server connects:
   - Enter the host name of the monitoring server in the **TEMS Hostname** field. (If the field is not active, clear the **No TEMS** check box.)
   - Select the communications protocol that the monitoring server uses from the **Protocol** drop-down list.
     - If you select SNA, enter information in the **Net Name**, **LU Name**, and **LOG Mode** fields.
     - If you select IP.UDP, IP.PIPE, or IP.SPIPE, enter the port number of the monitoring server in the **Port Number** field.

     For information about these fields, refer to Table 39 on page 140.
6. Click the **Agent Parameters** tab.

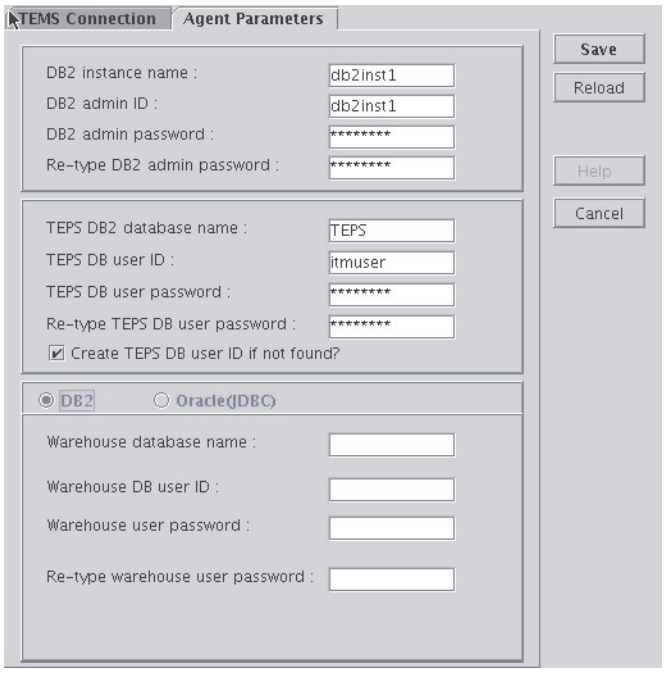


Figure 23. Configuring database connections for the portal server

7. Configure the connection between the portal server and the portal server database by entering information in the fields described in the following table:

Table 41. Configuration information for the Tivoli Enterprise Portal Server database

Field	Default value	Description
DB2 instance name	db2inst1	The DB2 instance name.
DB2 admin ID	db2inst1	The DB2 Administrator ID. The DB2 Administrator account was created during DB2 installation.
DB2 admin password	(no default)	The password for the DB2 Administrator ID.
Re-type DB2 admin password	(no default)	The password for the DB2 Administrator ID.
TEPS DB2 database name	TEPS	The Tivoli Enterprise Portal Server database name.
TEPS DB user ID	itmuser	The login name of the warehouse user that the portal server will use to access the database.
TEPS DB user password	(no default)	The password for the warehouse user ID.
Re-type TEPS DB user password	(no default)	The password for the warehouse user ID.
Create TEPS DB user ID if not found?	yes	This check box is selected by default. If the database login account (user ID and password) that you specified in the preceding fields does not exist, it is created.

8. Optionally configure the connection between the portal server and the Tivoli Data Warehouse database.

Note

The bottom section of the **Agent Parameters** tab contains fields for configuring the connection between the portal server and a Tivoli Data Warehouse database using DB2 or Oracle. (See Figure 23 on page 146.) If you have not set up a Tivoli Data Warehouse, accept the defaults for these fields. Follow the instructions later in this book for implementing a Tivoli Data Warehouse solution, beginning with Chapter 12, "Tivoli Data Warehouse solutions," on page 265. These instructions will direct you to reconfigure the connection between the portal server and the warehouse database after you have completed all preliminary setup tasks.

Do one of the following:

- If you have not set up the Tivoli Data Warehouse, click **Save** to save your settings and close the window.

  –OR–

- Configure a connection between the portal server and a DB2 warehouse database.

  Before you configure the connection, verify that you have already completed the following tasks:

  – Created a warehouse database using DB2
  – Created a warehouse user on the computer where you created the warehouse database.

    The *warehouse user* is the user account (user ID and password) used by the portal server and other warehousing components to access the warehouse database.
  – Cataloged the warehouse database on the computer where you are installing the portal server if the warehouse database is remote from the portal server
  – Activated the UNIX listeners on the computer where the warehouse database is located if the warehouse database is installed on UNIX.

  These tasks are described in Chapter 13, "Tivoli Data Warehouse solution using DB2."

  To configure the connection between the portal server and the DB2 data warehouse, you will need the name of the warehouse database and the user ID and password of the warehouse user.

  Note: Each instance of the restricted-use version of DB2 UDB Enterprise Edition V9.1 provided for use with the portal server and the Tivoli Data Warehouse must be registered. See "Registering the DB2 product license key using the db2licm command" on page 79.

  To perform the configuration, complete the procedure Configuring a Linux or AIX portal server (DB2 CLI connection), starting from Step 4 on page 294.

  –OR–

- Configure a connection between the portal server and an Oracle warehouse database.

  Before you configure the connection, verify that you have already completed the following tasks:

  – Created a warehouse database using Oracle

– Created a warehouse user on the computer where you created the warehouse database.

  The *warehouse user* is the user account (user ID and password) used by the portal server and other warehousing components to access the warehouse database.
– Activated the Oracle listener on the computer where the warehouse database is located
– Installed an Oracle JDBC Type 4 driver on the portal server.

These tasks are described in Chapter 15, "Tivoli Data Warehouse solution using Oracle."

To configure the connection between the portal server and the Oracle data warehouse, you will need:

– The name of the warehouse database and the user ID and password of the warehouse user
– The location, name, and URL of the JDBC driver

To perform the configuration, complete the procedure Configuring a Linux or AIX portal server (JDBC connection), starting from Step 4 on page 332.

Starting the portal server

From the bin directory of /opt/IBM/ITM (or where you installed IBM Tivoli Monitoring), run the following command to start the portal server:

```
./itmcmd agent start cq
```

Installing monitoring agents

This section describes how to install distributed monitoring agents. A *distributed* monitoring agent is one that is installed on a distributed (not z/OS) operating system. These instructions also apply to the Warehouse Proxy and Summarization and Pruning agents. For instructions on how to install a z/OS monitoring agent, refer to the agent documentation for your z/OS agent product.

To install a distributed monitoring agent, use the appropriate installation media:

- Use the IBM Tivoli Monitoring base product DVD to install the agents in the following list. This is the same product DVD that you use to install the monitoring servers, portal server, and portal desktop clients.
  – IBM Tivoli Monitoring 5.x Endpoint
  – Linux OS
  – UNIX Logs
  – UNIX OS
  – Universal Agent
  – Warehouse Proxy Agent
  – Warehouse Summarization and Pruning Agent
  – Windows OS
- You can also use the IBM Tivoli Monitoring base product DVD to install application support for any IBM Tivoli Monitoring V6.x based distributed monitoring agent you intend to install. Installing and configuring application support on base components (monitoring servers, portal server, desktop clients) when you install them means that you do not have to stop and restart those components later when you install the agent. However, if the monitoring agents you install have been updated since the DVD was issued, you must install the application support files from the monitoring agent product CD.

- Use the agent product CDs to install distributed monitoring agents that are delivered separately from the IBM Tivoli Monitoring base installation package. For example, use the IBM Tivoli Monitoring for Databases product CDs to install a monitoring agent for DB2 or Oracle. Depending on the agent that you are installing, there might be additional configuration steps required. See the agent documentation for more information.

All monitoring agents require that agent-specific application support be installed on the monitoring servers, portal server, and portal desktop clients. See "Installing and enabling application support" on page 159 for information.

The following sections provide instructions for installing a monitoring agent:

- "Windows: Installing a monitoring agent"
- "Linux or UNIX: Installing a monitoring agent" on page 152

Windows: Installing a monitoring agent

Use the following steps to install a distributed monitoring agent on a Windows computer:

1. Launch the installation wizard by double-clicking the setup.exe file in the \WINDOWS subdirectory on the installation media.

   Use either an IBM Tivoli Monitoring base product DVD or a distributed agent product CD for Windows. Do *not* use a Data Files for z/OS CD.

   Note: If you are installing on Windows Itanium, launch the installation wizard by double-clicking on the setup.exe file in the \wia64 directory of the base DVD.
2. Click **Next** on the Welcome window.

   Note: If you have another IBM Tivoli Monitoring component already installed on this computer, select **Modify** on the Welcome window to indicate that you are updating an existing installation. Click **OK** on the message telling you about preselected items. Then skip to Step 9 on page 150.
3. On the Install Prerequisites window, read the information about the required levels of IBM Global Security Toolkit (GSKit) and IBM Java.

   The check box for each prerequisite is cleared if the correct level of the software is already installed. Otherwise, the check box is selected to indicated that the software is to be installed.

   Note: Windows Itanium does not support Java 1.5. Java 1.4 will be installed if it is not already present.
4. Click **Next**. The prerequisite software is installed if necessary.
5. Read and accept the software license agreement by clicking **Accept**.
6. 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 install a monitoring agent on this computer, so you can click **Next** and ignore this message.
7. Choose the directory where you want to install the product. Click **Next**.

   Note: This step applies only to those agents that you install from the IBM Tivoli Monitoring installation image. Agents installed from the agent installation image do not have this step. If you are installing an agent from an agent installation image, skip to step 9 on page 150.

8. Type a 32-character encryption key. This key must be the same as the key that was 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.
9. On the Select Features window, expand **Tivoli Enterprise Monitoring Agents**.
10. Select the names of the agents that you want to install and click **Next**.

    Note: Agents available on the IBM Tivoli Monitoring installation image include the Warehouse Proxy agent and the Summarization and Pruning agent. Before you install these agents, follow the instructions later in this book for setting up a Tivoli Data Warehouse solution, beginning with Chapter 12, "Tivoli Data Warehouse solutions," on page 265. On Windows Itanium, only the Windows agent, the Universal Agent, and the agent framework are available for installation.
11. If a monitoring server is not installed on this computer, go to Step 12.

    If you are installing monitoring agents on a computer that already has a monitoring server installed, the Agent Deployment window is displayed.

    The Agent Deployment window lists monitoring agents on this installation image that you can add to the agent depot. The agent depot contains agents that you can deploy to remote computers. For information about how to deploy agents in the agent depot to remote computers, see Chapter 7, "Deploying monitoring agents across your environment," on page 195.

    Note: By default, the agent depot is located in the *<itm_installdir>*/CMS/depot directory on Windows. If you want to use a different directory, create the directory (if it does not exist) and specify the directory using the DEPOTHOME key in the KBBENV file.

    Select the agents, if any, that you want to add to the agent depot. (You can add agents to the agent depot at a later time by updating your installation.) Click **Next**.
12. This step applies only to agents that you install from the IBM Tivoli Monitoring installation image. If you are installing agents from an agent product installation image, go to Step 13.

    If no IBM Tivoli Monitoring component has been previously installed on this computer, a window is displayed for you to select a program folder for the Windows Start menu. Select a program folder and click **Next**. The default program folder name is IBM Tivoli Monitoring.
13. Review the installation summary details. The summary identifies what you are installing and where you chose to install it. Click **Next** to start the installation.

    After installation is complete, a configuration window (called the Setup Type window) is displayed.
14. Clear the check boxes for any components that have already been installed and configured (at the current release level) on this computer, unless you want to modify the configuration. (For example, clear the check box for the Tivoli Enterprise Monitoring Server if it has already been installed and configured on this computer.) Click **Next** to start configuring all selected components.
15. Define the communications between the monitoring agents and the monitoring server:
    a. If the 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 monitoring server.

   You have four choices: IP.UDP, IP.PIPE, IP.SPIPE, or SNA. You can specify up to three methods for communication. If the method you have identified as Protocol 1 fails, Protocol 2 is used. If Protocol 2 fails, Protocol 3 is used. When you configure the protocol for the Warehouse Proxy agent, configure the same protocols used by the application agents and by the hub monitoring. If the proxy agent does not have the same protocol as the hub monitoring server, it cannot register with the hub. If the proxy does not have the same protocol as the application agents, then the application agents cannot communicate with the proxy when they to create a route to it.

   Note: Do not select **Optional Secondary TEMS Connection**. You can set up the failover support for agents after installation, as described in "Configuring failover support" on page 221.

c. Click **OK**. A second configuration window is displayed.

d. Complete the fields shown in the following tableTable 42 for the protocol that you specified.

Table 42. Communications protocol settings

Field	Description
IP.UDP Settings	
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. The default number is 1918.
IP.PIPE Settings	
Hostname 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 number is 1918.
IP.SPIPE Settings	
Hostname or IP Address	The host name or IP address for the hub monitoring server.
Port number	The listening port for the hub monitoring server. The default value is 3660.
SNA Settings	
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.
Local LU Alias	The LU alias.

e. Click **OK** to exit the Configuration Defaults for Connecting to a TEMS window.

16. Click **Finish** to complete the installation.
17. Click **Finish** on the Maintenance Complete window if you are updating an existing installation.
18. Open the Manage Tivoli Monitoring Services utility (if it does not open automatically) to see if the monitoring agents that you installed have been configured and started. If **Yes** is displayed in the **Configured** column, the agent has been configured and started during the installation process.
19. If the value in the **Configured** column is blank and **Template** is displayed in the **Task/Subsystem** column, right-click the Template agent and complete the following steps:
    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.

       Note: Do not type non-ASCII characters on any of these windows. Typing characters from other character sets has unpredictable results.
    c. Repeat this step as necessary to create monitoring agent instances for each application instance you want to monitor.

Linux or UNIX: Installing a monitoring agent

Use the following steps to install and configure a distributed monitoring agent on a Linux or UNIX computer.

Table 43. Steps for installing a monitoring agent on Linux or UNIX

Steps	Where to find information
Install the monitoring agent.	"Installing the monitoring agent"
Configure the monitoring agent.	"Configuring the monitoring agent" on page 153 Some agents require additional, agent-specific configuration parameters. See the agent documentation for the specific agents that you are configuring.
Change the file permissions for files on the computer where you installed the agent.	"Changing the file permissions for agents" on page 155
Start the monitoring agent.	"Starting the monitoring agents" on page 155

Installing the monitoring agent

Use the following steps to install a monitoring agent on a Linux or UNIX computer:

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 type the full path to a different directory.
3. If the installation directory does not already exist, you are asked if you want to create it. Type `y` to create this directory and press Enter.
4. The following prompt is displayed:

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

Please enter a valid number:
```

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

Type 1 to start the installation and display the software license agreement.

5. Press Enter to read through the agreement.
6. Type 1 to accept the agreement and press Enter.
7. Type a 32 character encryption key and press Enter. This key should be the same as the key that was used during the installation of the monitoring server to which this monitoring agent connects.

   Note: This step applies only to those agents that you install from the IBM Tivoli Monitoring installation image. Agents installed from the agent installation image do not need to provide the encryption key.

   A numbered list of available operating systems is displayed.
8. Type the number for the operating system on which you are installing the monitoring agents. The default value is your current operating system. Press Enter.
9. Type 1 to confirm the operating system and press Enter.

   A numbered list of available components is displayed.
10. Type the number that corresponds to the monitoring agent or agents that you want to install. If you want to install more than one agent, use a comma (,) or a space to separate the numbers for each agent. Press Enter.

    Note: Before you install the Warehouse Proxy agent or Summarization and Pruning agent, follow the instructions later in this book for setting up a Tivoli Data Warehouse solution, beginning with Chapter 12, "Tivoli Data Warehouse solutions," on page 265.

    A list of the components to be installed is displayed.
11. Type 1 to confirm the installation.

    The installation begins.
12. After all of the components are installed, you are asked whether you want to install additional products or product support packages. Type 2 and press Enter. Continue with "Configuring the monitoring agent."

Configuring the monitoring agent

Use the following steps to configure your monitoring agent:

1. Run the following command:

   ```
   ./itmcmd config -A pc
   ```

   where *pc* is the product code for your agent. For the UNIX agent, use the product code "ux"; for Linux, use "lz". See Appendix D, "IBM Tivoli product codes," on page 437 for a list of agent product codes.
2. Press Enter when you are asked if the agent connects to a monitoring server.
3. Type the host name for the monitoring server.

4. Type the protocol that you want to use to communicate with the monitoring server. You have four choices: ip, sna, ip.spipe, or ip.pipe. Press Enter to accept the default protocol (IP.PIPE).
5. 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.
6. Depending on the type of protocol you specified, provide the following information when prompted:

Table 44. UNIX monitoring server protocols and values

Protocol	Value	Definition
IP.UDP	IP Port Number	The port number for the monitoring server. The default is 1918.
SNA	Net 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.
	Log Mode	The name of the LU6.2 LOGMODE. The default value is "CANCTDCS."
IP.PIPE	IP.PIPE Port Number	The port number for the monitoring server. The default is 1918.
IP.SPIPE	IP.SPIPE Port Number	The port number for the monitoring server. The default is 3660.

7. Press Enter to *not* specify the name of the KDC_PARTITION.
8. Press Enter when you are asked if you want to configure the connection to a secondary monitoring server. The default value is no.
9. Press Enter to accept the default for the Optional Primary Network Name (none).

You must complete the configuration of the Warehouse Proxy agent using the Manage Tivoli Monitoring Services graphical user interface (GUI), which requires an X11 GUI interface. See the instructions for configuring the Warehouse Proxy for the appropriate Data Warehouse:

- DB2: "Configuring a Warehouse Proxy agent on Linux or AIX (JDBC connection)" on page 288
- SQL Server: "Configuring a Warehouse Proxy agent on Linux or AIX (JDBC connection)" on page 309
- Oracle: "Configuring a Warehouse Proxy agent on Linux or AIX (JDBC connection)" on page 326

If you used a non-root user to install a monitoring agent on a UNIX computer, the file permissions are initially set to a low level. Use the procedure in "Changing the file permissions for agents" on page 155 to change these file permissions:

Changing the file permissions for agents

If you used a non-root user to install a monitoring agent on a UNIX computer, the file permissions are initially set to a low level. Run the following procedure to change these file permissions:

1. Log in to the computer as root, or become the root user by running the **su** command.
2. Create a new group (such as "itmusers") to own all of the files in the IBM Tivoli Monitoring installation directory.

   For Linux, Solaris, and HP-UX computers, run the following command:

   ```
   groupadd itmusers
   ```

   For an AIX computer, run the following command:

   ```
   mkgroup itmusers
   ```
3. Run the following command to ensure that the CANDLEHOME environment variable correctly identifies IBM Tivoli Monitoring installation directory:

   ```
   echo $CANDLEHOME
   ```

   If you run the following steps in the wrong directory, you can change the permissions on every file in every file system on the computer.
4. Change to the directory returned by the previous step:

   ```
   cd $CANDLEHOME
   ```
5. Run the following command to ensure that you are in the correct directory:

   ```
   pwd
   ```
6. Run the following commands:

   ```
   chgrp -R itmusers .
   chmod -R o-rwx .
   ```
7. Run the following command to change the ownership of additional agent files:

   ```
   bin/SetPerm
   ```
8. If you want to run the agent as a particular user, add the user to the itmusers group. To do this, edit the /etc/group file and ensure that the user is in the list of users for the itmusers group.

   For example, if you want to run the agent as user test1, ensure that the following line is in the /etc/group file:

   ```
   itmusers:x:504:test1
   ```
9. Run the **su** command to switch to the user that you want to run the agent as or log in as that user.
10. Start the agent as described in "Starting the monitoring agents."

Starting the monitoring agents

You can either start all agents running on a computer or start individual agents by using the product codes.

To start all monitoring agents, run the following command:

```
./itmcmd agent start all
```

To start specific agents, run the following command:

```
./itmcmd agent start pc pc pc
```

where *pc* is the product code for the agent that you want to start. See Appendix D, "IBM Tivoli product codes," on page 437 for a list of agent product codes.

Installing the Tivoli Enterprise Portal desktop client

There are two methods of deploying the desktop client: You can install the desktop client from the installation media and run and maintain it on the local system. You can also use IBM Web Start for Java to download and run the desktop client from the Tivoli Enterprise Portal Server. See "Planning considerations for the Tivoli Enterprise Portal client" on page 26 for a discussion of the advantages and disadvantages of each type of portal server client available with IBM Tivoli Monitoring.

This section describes how to install the desktop client from the installation media on Windows and Linux computers. When you install the desktop client from the installation media, you must also install support for all the applications that you will be using.

- "Windows: Installing the desktop client"
- "Linux: Installing the desktop client" on page 158

See "Using Web Start to download and run the desktop client" on page 189 for instructions on downloading and running the desktop client from the portal server.

Windows: Installing the desktop client

Complete the following steps to install the Tivoli Enterprise Portal desktop client from the *IBM Tivoli Monitoring Base DVD*:

1. On the computer where you want to install the desktop client, start the installation wizard by launching the setup.exe file in the \WINDOWS subdirectory on the installation media.
2. Click **Next** on the Welcome window.

   Note: If you have another IBM Tivoli Monitoring component already installed on this computer, select **Modify** on the Welcome window to indicate that you are updating an existing installation. Click **OK** on the message telling you about preselected items. Then skip to Step 8.
3. On the Install Prerequisites window, read the information about the required levels of IBM Global Security Toolkit (GSKit) and IBM Java.

   The check box for each prerequisite is cleared if the correct level of the software is already installed. Otherwise, the check box is selected to indicated that the software is to be installed.
4. Click **Next**. The prerequisite software is installed if necessary.
5. Read and accept the software license agreement by clicking **Accept**.
6. Specify the directory where you want to install the portal desktop client software and accompanying files. The default location is C:\IBM\ITM. Click **Next**.
7. Type an encryption key to use. This key must be the same as what was used during the installation of the hub monitoring server to which the client will connect. Click **Next** and then **OK** to confirm the encryption key.
8. On the Select Features window, select **Tivoli Enterprise Portal Desktop Client** from the list of components to install.

   When you select the **Tivoli Enterprise Portal Desktop Client** check box, all of the check boxes in the attached subtree are automatically selected. The support check boxes in the subtree are for installing application support files for distributed monitoring agents to the portal desktop client. It is best to leave all of the support check boxes selected so you do not need to

reconfigure application support as new agent types are added to your environment. However, if you purchased an OMEGAMON XE monitoring product and you did not separately purchase IBM Tivoli MonitoringIBM Tivoli Monitoring, you should not install support for the distributed operating system monitoring agents nor the Universal Agent. If you are installing from the base DVD, you may see application support for component that are not supported on the operating system. For detailed information about application support, see "Installing and enabling application support" on page 159.

Note: If you are updating an existing installation (you selected **Modify** on the Welcome window), all check boxes on the Select Features window reflect your choices during the initial installation. Clearing a check box has the effect of *uninstalling* the component. Clear a check box only if you want to remove a component.

9. If you want to view IBM Tivoli Enterprise Console events through the Tivoli Enterprise Portal, expand **Tivoli Enterprise Portal Desktop Client** and ensure that **TEC GUI Integration** is selected.
10. Click **Next**.
11. If a monitoring server is not installed on this computer, go to Step 12.

    If you are installing the desktop client on a computer that already has a monitoring server installed, the Agent Deployment window is displayed.

    The Agent Deployment window lists monitoring agents on this installation image that you can add to the agent depot. The agent depot contains agents that you can deploy to remote computers. For information about how to deploy agents in the agent depot to remote computers, see Chapter 7, "Deploying monitoring agents across your environment," on page 195.

    Note: By default, the agent depot is located in the <*itm_installdir*>/CMS/depot directory on Windows. If you want to use a different directory, create the directory (if it does not exist) and specify the directory using the DEPOTHOME key in the KBBENV file.

    Select the agents, if any, that you want to add to the agent depot. (You can add agents to the agent depot at a later time by updating your installation.) Click **Next**.
12. If no IBM Tivoli Monitoring component has been previously installed on this computer, a window is displayed for you to select a program folder for the Windows Start menu. Select a program folder and click **Next**. The default program folder name is IBM Tivoli Monitoring.
13. Review the installation summary details. The summary identifies what you are installing and where you chose to install it. Click **Next** to start the installation.

    After installation is complete, a configuration window (called the Setup Type window) is displayed.
14. Clear the check boxes for any components that have already been installed and configured (at the current release level) on this computer, unless you want to modify the configuration. (For example, clear the check box for the Tivoli Enterprise Monitoring Server if it has already been installed and configured on this computer.) Click **Next** to start configuring all selected components.
15. Type the host name of the portal server and click **OK**.
16. Click **Finish** to complete the installation.

Linux: Installing the desktop client

Use the following steps to install the Tivoli Enterprise Portal 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 type the full path to a different directory.
3. If the installation directory does not already exist, you are asked if you want to create it. Type 1 to create this directory and press Enter.
4. The following prompt is displayed:

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

   Please enter a valid number:
   ```

   Type 1 to start the installation and display the software license agreement.
5. Press Enter to read through the agreement.
6. Type 1 to accept the agreement and press Enter.
7. Type an 32-character 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.
8. Type the number for the operating system on which you are installing the desktop client. The default value is your current operating system. Press Enter.
9. Type 1 to confirm the operating system and press Enter.

   A numbered list of available components is displayed.
10. Type the number for `Tivoli Enterprise Portal Desktop Client` and press Enter.

    A message is displayed indicating that the Tivoli Enterprise Portal Desktop Client is about to be installed.
11. Type 1 to confirm the installation.

    The installation begins.
12. After the portal desktop client is installed, you are asked whether you want to install additional products or product support packages. Type 1 and press Enter.

    A numbered list is displayed, including the following application support package:

    ```
    Tivoli Enterprise Portal Desktop Client support
    ```
13. Install the application support package for the portal desktop client.

    All monitoring agents require that application support files be installed on the monitoring servers (hub and remote), portal server, and portal desktop clients in your environment. Application support files contain the information required for agent-specific workspaces, helps, predefined situations, and other data.

    This step installs the application support files for base monitoring agents. The *base* monitoring agents are included with the base IBM Tivoli Monitoring installation package. For detailed information about application support, see "Installing and enabling application support" on page 159.

a. Type the number that corresponds to `Tivoli Enterprise Portal Desktop Client support` and press Enter.

   A numbered list of base monitoring agents is displayed.

b. Type the numbers of the base monitoring agents for which you want to install application support, or type the number that corresponds to `All of the above`. Type the numbers on the same line separated by spaces or commas. Press Enter.

   It is best to select all of the base monitoring agents (`All of the above`) so you do not need to reconfigure application support as new agent types are added to your environment.

c. Type `1` to confirm the installation and press Enter.

   The installation begins.

   Note: This step installs the application support files. However, you must *enable* the application support by configuring the portal desktop client. The next sections shows you how to configure the portal desktop client.

14. After application support for the monitoring agents is installed, you are asked whether you want to install additional products or product support packages. Type `2` and press Enter.

The next step is to configure the desktop client. Use the instructions in "Linux: Configuring the desktop client."

Linux: Configuring the desktop client

Complete the following steps to configure the desktop client if you installed the client from the IBM Tivoli Monitoring installation media. You do not need to complete this procedure if you obtained the desktop client by using IBM Web Start for Java to download it from the Tivoli Enterprise Portal Server.

1. At the command line /opt/IBM/ITM/bin directory (or the `/bin` subdirectory where you installed the product), run the following command:

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

2. Press Enter to use the default instance name.
3. Type the host name for the portal server and press Enter.
4. Press Enter when you are asked if you want to use HTTP Proxy support. The default value is no.
5. Start the desktop client:

   ```
   /itmcmd agent start cj
   ```

Installing and enabling application support

Before you can view data collected by monitoring agents, you must install and enable application support for those agents. Application support files provide agent-specific information for workspaces, helps, situations, templates, and other data. Application support for a monitoring agent includes two types of files:

- **SQL files** are required for adding product-provided situations, templates, and policies to the Enterprise Information Base (EIB) tables maintained by the hub monitoring server. These SQL files are also called *seed data*, and installing them on a monitoring server is also called *seeding* the monitoring server.
- **Catalog and attribute (cat and atr) files** are required for presenting workspaces, online help, and expert advice for the agent in Tivoli Enterprise Portal.

All monitoring agents require that application support be configured on all instances of the following infrastructure components:

- Tivoli Enterprise Monitoring Server (both hub and remote monitoring servers)
- Tivoli Enterprise Portal Server
- Tivoli Enterprise Portal desktop client, if the desktop client was installed from the installation media.

  You do not need to configure application support for desktop clients are downloaded from the Tivoli Enterprise Portal Server using IBM Web Start for Java.

Application support for monitoring agents is installed independently of where and when the monitoring agents themselves are installed:

- Install application support for a particular type of monitoring agent on the monitoring servers, portal server, and portal desktop clients. Install agents of that type on any managed system in the environment that is compatible with the agent.
- Install application support for a type of monitoring agent *before* or *after* any monitoring agents of that type are installed. After you install application support for a particular type of monitoring agent, you can add any number of agents of that type to your environment without having to install application support again.

For example, you can install application support for a Linux OS monitoring agent (the agent *type*) to a Windows monitoring server (using the IBM Tivoli Monitoring installation media for Windows). Later, you can install any number of Linux OS monitoring agents to Linux computers in your environment (using the IBM Tivoli Monitoring installation media for Linux).

Important: If you are installing an non-OS agent remotely through the Tivoli Enterprise Portal (see "Deploying non-OS agents" on page 202), application support for the agent must be installed on the Tivoli Enterprise Portal Server *before* the agent is deployed.

Because application support for some IBM Tivoli Monitoring 6.x based distributed agents is included on the Base installation DVD, you may see application support files that do not apply to all systems.

Configuring application support is a two-step process:

1. Installing the application support files (from installation media).
2. Enabling the application support (sometimes referred to as *adding* or *activating* the application support).

On the portal server and portal desktop clients, application support is enabled when the component is configured. On monitoring servers, application support is enabled by *seeding* the database with agent-specific information.

The procedures for configuring application support differ by operating system, as summarized in Table 45 on page 161. On Windows, both installation and enablement of application support are accomplished during the installation of the monitoring servers, portal server, and desktop clients. On Linux or UNIX, this two-step process is more visible, with the enablement step done separately from the installation.

Table 45. Procedures for installing and enabling application support

Operating system	Monitoring servers	Portal server	Desktop clients[1]
Windows	Install and enable application support using installation media.	Install and enable application support using installation media.	Install and enable application support using installation media.
Linux or UNIX	1. Install application support files from installation media. 2. *Seed* the monitoring server using: • **itmcmd support**[2] command, OR • Manage Tivoli Monitoring Services window	1. Install application support files from installation media. 2. *Configure* the portal server using: • **itmcmd config** command, OR • Manage Tivoli Monitoring Services window	1. Install application support files from installation media. 2. *Configure* the desktop client using: • **itmcmd config** command, OR • Manage Tivoli Monitoring Services window
z/OS[4]	This book does not describe configuring application support for a monitoring server installed on a z/OS system. See *Configuring the Tivoli Enterprise Monitoring Server on z/OS* for information and instructions. The portal server and desktop client are not supported on z/OS. If you have a monitoring server on z/OS, use the procedures in this book to configure application support on the portal server and desktop clients.		

1. You need to configure application support for desktop clients that are installed from the installation media. You do not need to configure application support for desktop clients that are installed by using IBM Java Web Start to download the client from the Tivoli Enterprise Portal Server.
2. You can seed a non-local monitoring server, even if one is not installed on the local computer, by installing the support using option `3`, `Install TEMS support for remote seeding`, then using Manage Tivoli Monitoring Services to seed the non-local monitoring server. You cannot use **itmcmd support** to seed a non-local monitoring server.
3. There is no way to uninstall the application support files laid down without uninstalling the Tivoli Enterprise Monitoring Server.

Selecting the correct support media

Application support for IBM Tivoli Monitoring V6.1 distributed agents is found on the following DVDs:

- *IBM Tivoli Monitoring V6.2 Base DVD*
- *IBM Tivoli Monitoring V6.2: Agent Support for Tivoli Enterprise Portal Server on AIX*
- *IBM Tivoli Monitoring V6.2: Agent Support for Tivoli Enterprise Management Server on HP-UX on Itanium*
- *IBM Tivoli Monitoring V6.2: Agent Support for Tivoli Enterprise Portal Server for DB2 9.1*
- Agent product installation CDs

The *IBM Tivoli Monitoring V6.2 Base DVD* contains application support files for the base operating system (OS) monitoring agents, the Warehouse Proxy agent, the Summarization and Pruning agent, and the monitoring agents listed in Table 46 on page 162. To install application support for these agents on distributed

components, use the procedures documented in this chapter for installing the monitoring servers (hub and remote), the Tivoli Enterprise Portal, and the portal desktop client. See "Configuring application support for agents on the Base DVD" on page 164 for more information. For instructions on installing application support for the monitoring agents on a monitoring server on z/OS, see *IBM Tivoli Monitoring: Configuring IBM Tivoli Enterprise Monitoring Server on z/OS*.

Table 46. Product support on the IBM Tivoli Monitoring V6.2.0 Base DVD

Product Code	Product Name
A4	Monitoring Agent for i5 OS
HD	Warehouse Proxy Agent
LZ	Monitoring Agent for Linux OS
NT	Monitoring Agent for Windows OS
OQ	Monitoring Agent for Microsoft SQL Server
OR	Monitoring Agent for Oracle
OY	Monitoring Agent for Sybase Server
P5	Base Monitoring Agent for AIX
PH	Base Monitoring Agent for HMC
PK	Base Monitoring Agent for CEC
PV	Base Monitoring Agent for VIOS
PX	Premium Monitoring Agent for AIX
QR	Monitoring Agent for Microsoft Virtual Server
QV	Monitoring Agent for VMware ESX
QX	Monitoring Agent for Citrix Access Suite
SY	Warehouse Summarization and Pruning Agent
TM	Monitoring Agent for IBM Tivoli Monitoring 5.x Endpoint
UD	Monitoring Agent for DB2
UL	Monitoring Agent for UNIX Logs
UM	Universal Agent
UX	Monitoring Agent for UNIX OS
VA	Premium Monitoring Agent for VIOS

The agent support DVDs delivered with IBM Tivoli Monitoring V6.2 must be used instead of the agent installation CDs if you are installing support for the agents listed in the follow tables on the specified component. The installer on the agent installation CDs does not support these components on these platforms. To install application support for these agents on distributed components, see "Configuring application support for non-Base monitoring agents" on page 164. To install application support for the monitoring agents on a z/OS monitoring server, see *IBM Tivoli Monitoring: Configuring IBM Tivoli Enterprise Monitoring Server on z/OS*.

- If you are installing support for the products listed in Table 47 on page 163 on a Tivoli Enterprise Portal Server on AIX, use the *IBM Tivoli Monitoring V6.2: Agent Support for Tivoli Enterprise Portal Server on AIX* DVD.

Table 47. Product support on the Agent Support for Tivoli Enterprise Portal Server on AIX DVD

Product Code	Product Name
T2	IBM Tivoli Composite Application Manager for Response Time Tracking
VW	IBM Tivoli NetView for z/OS
YN	IBM Tivoli Composite Application Manager for WebSphere Application Server V6.1.0

- If you are installing support for the products listed in Table 48 on a Tivoli Enterprise Monitoring Server on HP-UX on Itanium, use the *IBM Tivoli Monitoring V6.2: Agent Support for Tivoli Enterprise Monitoring Server on HP-UX on Itanium* DVD.

Table 48. Product support on the Agent Support for Tivoli Enterprise Monitoring Server on HP-UX on Itanium DVD

Product Code	Product Name
BC	Monitoring Agent for DataPower
D4	IBM Tivoli Composite Application Manager for Service Oriented Architecture V6.1.0
EX	Monitoring Agent for Exchange
GB	Monitoring Agent for Domino
HT	IBM Tivoli Composite Application Manager for Web Servers
KA	Monitoring Agent for Tivoli Enterprise Console Health
Q5	Monitoring Agent for Microsoft Cluster Server
YN	IBM Tivoli Composite Application Manager for WebSphere Application Server V6.1.0
YJ	IBM Tivoli Composite Application Manager for J2EE

- If you are installing any of the following agents listed in Table 49 on a Tivoli Enterprise Portal Server that is using DB2 V9.1 for its database, use the *IBM Tivoli Monitoring V6.2: Agent Support for Tivoli Enterprise Portal Server for DB2 9.1* DVD.

Table 49. Product support on the Agent Support for Tivoli Enterprise Portal Server for DB2 9.1 DVD

Product code	Product name
BC	Monitoring Agent for DataPower
D4	IBM Tivoli Composite Application Manager for Service Oriented Architecture
EX	Monitoring Agent for Exchange
GB	Monitoring Agent for Domino
HT	IBM Tivoli Composite Application Manager for Web Servers
KA	Monitoring Agent for Tivoli Enterprise Console Health
Q5	Monitoring Agent for Microsoft Cluster Server
YJ	IBM Tivoli Composite Application Manager for J2EE
YN	IBM Tivoli Composite Application Manager for WebSphere Application Server

For all other distributed agents, install application support from the product installation CDs. See "Configuring application support for non-Base monitoring agents" for instructions.

Configuring application support for agents on the Base DVD

You install and configure application support for the agents on the Base DVD when you install and configure distributed monitoring servers, the portal server, and the portal desktop clients using the instructions in this chapter.

- When you install a monitoring server on Linux or UNIX, support files for all agent types on the Base are installed automatically. When you install the portal server and portal desktop client, you can specify which agent types to support.
- When you install a monitoring server, portal server, or portal desktop client on Windows, you can select the Base monitoring agents for which you want to install application support on the Select Features window. By default, all the agents are selected.

In both cases, it is best to install and enable application support for all agent types on the Base DVD during the initial installation to avoid having to reconfigure application support on all monitoring servers, the portal server, and portal desktop clients as new agent types are added to your environment.

If you need to reconfigure application support, restart the installation from the IBM Tivoli Monitoring installation media. Update the installation by installing application support for additional Base monitoring agents. When you update an installation, keep in mind the following considerations:

- Following an installation update on Linux or UNIX, you must reseed the monitoring server and reconfigure the portal server and desktop clients.
- When you update an installation on Windows, proceed through the installation as you did for the initial installation except as follows:
  - All check boxes on the Select Features window reflect your choices during the initial installation. Do not clear any check boxes. Clearing a check box has the effect of *uninstalling* the component.

    For example, if you are updating the installation to add application support for the i5/OS agent, select only the application support check box for the i5/OS agent. Do not clear any application support check boxes that are already checked unless you want to remove support for those agents.
  - You do not need to reconfigure any components (such as the monitoring server or portal server) that have already been configured.
- You must update the installation on all computers where a monitoring server, portal server, or desktop client is installed.

Configuring application support for non-Base monitoring agents

The term *non-Base* is used here to refer to distributed monitoring agents for which support is included on the V6.2 Agent Support DVDs, and to other products such as IBM Tivoli Monitoring for Applications, OMEGAMON XE monitoring agents, and IBM Tivoli Composite Application Manager monitoring agents that provide their own support files.

Some monitoring agents that run on z/OS or z/VM are packaged with their own CD that contains the data files for adding application support to distributed components. Other monitoring agents that run on z/OS are packaged with a CD

that contains data files for a number of agents. If in doubt, refer to the configuration guide for each of your monitoring agents to find the exact name of the CD to use.

The following table shows you which installation media to use and where to find instructions for installing application support, according to the type of agent (distributed or z/OS) and whether the agent reports to a distributed or z/OS monitoring server.

Table 50. Installation media and instructions for installing application support for non-Base monitoring agents

Agent	Monitoring server	Installation media	Instructions for installing application support
Distributed	Distributed	*IBM Tivoli Monitoring V6.2: Agent Support* DVDs Agent product installation CDs	Follow the instructions in this section to install application support on the monitoring server, portal server, and desktop client.
Distributed	z/OS	*IBM Tivoli Monitoring V6.2: Agent Support* DVDs Agent product installation CDs	• Follow the instructions in this section to install application support on the portal server and desktop clients. • Follow the instructions in *Configuring the Tivoli Enterprise Monitoring Server on z/OS* to install application support on the monitoring servers.
z/OS	Distributed	Data Files CD	Follow the instructions in this section to install application support on the monitoring server, portal server, and desktop client.
z/OS	z/OS	Data Files CD	• Follow the instructions in this section to install application support on the portal server and desktop clients. • Follow the instructions in *Configuring the Tivoli Enterprise Monitoring Server on z/OS* to install application support on the monitoring servers.

Use the instructions in the following sections to install application support for non-Base distributed or z/OS monitoring agents on the distributed monitoring servers, portal server, and portal desktop clients in your environment:

- "Installing application support on monitoring servers"
- "Installing application support on the Tivoli Enterprise Portal Server" on page 170
- "Installing application support on the Tivoli Enterprise Portal desktop client" on page 174

Each of these sections provides information for installing application support files to a single component, such as the monitoring server. If you have multiple components on the same computer (such as the monitoring server and the portal server), combine steps from the individual sections to install application support to all components.

Installing application support on monitoring servers

Use the following procedures to install application support for non-Base monitoring agents on distributed monitoring servers (hub and remotes) in your environment:

- "Windows: Installing application support on a monitoring server" on page 166

- "Linux or UNIX: Installing application support on a monitoring server" on page 168

Windows: Installing application support on a monitoring server: Complete the following steps to install application support for monitoring agents on Windows monitoring servers.

Note: The monitoring server is stopped during this process.

1. In the /WINDOWS subdirectory on the agent product CD (for distributed products) or data files CD (for z/OS products), double-click the setup.exe file to launch the installation.
2. Click **Next** on the Welcome window.

   Note: If a monitoring agent is already installed on this computer, select **Modify** on the Welcome window to indicate that you are updating an existing installation. Click **OK** on the message telling you about preselected items. Then skip to Step 6.
3. On the Install Prerequisites window, read the information about the required levels of IBM Global Security Toolkit (GSKit) and IBM Java.

   The check box for each prerequisite is cleared if the correct level of the software is already installed. Otherwise, the check box is selected to indicated that the software is to be installed. If you are installing support from the data files CD for z/OS agent products, you might be prompted to install Sun Java Runtime Environment (JRE) 1.4.2, even if you have already installed IBM JRE 1.5 with the distributed components of Tivoli Management Services. The two versions can coexist, and installation of application support for some monitoring agents requires Sun Java 1.4.2. You might also see a message indicating that you can decline the installation of JRE 1.4.2 and that accepting installation of JRE 1.4.2 results in uninstallation of other Java versions. Ignore this message, because you cannot proceed without accepting the installation of Sun Java 1.4.2, and accepting the installation does not uninstall IBM Java 1.5.
4. Click **Next**. The prerequisite software is installed if necessary.

   If the installation program installs IBM GSKit or IBM JRE, you might be prompted to reboot the computer when the installation is complete. If so, you receive an `abort` message with a **Severe error** heading. This is normal and does not indicate a problem.

   If you are prompted to reboot, do the following:

   a. Click **OK** on the window prompting you to reboot.
   b. Click **No** on the window asking whether you want to view the abort log.
   c. Restart the computer.
   d. Restart the installation program.
5. Click **Accept** to accept the license agreement.
6. If you see a message regarding installed versions being newer than the agent installation, click **OK** to ignore this message.
7. Select the application support packages that you want to install:

   a. On the Select Features window, select **Tivoli Enterprise Monitoring Server**.
   b. Expand the **Tivoli Enterprise Monitoring Server** node to display a list of application support packages that you can install on the monitoring server.

      The following example shows the application support packages available with the IBM Tivoli Monitoring for Databases product:

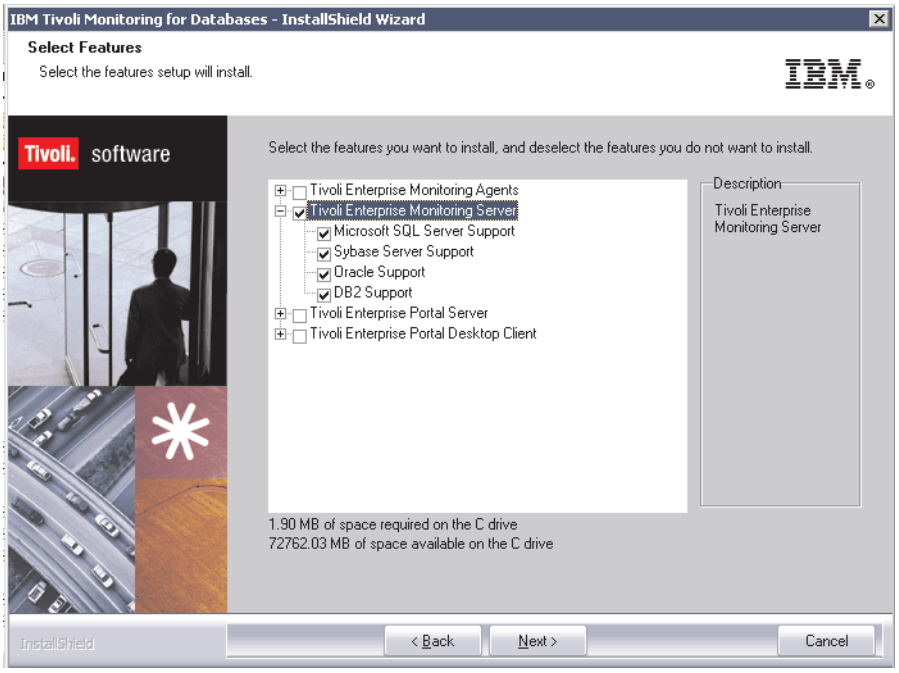


Figure 24. IBM Tivoli Monitoring for Databases: application support packages

Initially, all application support packages are selected.

c. Clear the check boxes for application support packages that you do not want to install.

   Note: If you are updating an existing installation (you selected **Modify** on the Welcome window), all check boxes on the Select Features window reflect your choices during the initial installation. Clearing a check box has the effect of *uninstalling* the component (for example, the Tivoli Enterprise Monitoring Server) or product package. Clear a checkbox for an application support package only if you want to remove the application support.

d. If you have other components installed on the same computer, such as the desktop client, also select those components to install the component-specific application support.

e. Click **Next**.

8. (*Distributed agents only*) If you want to add the agent to the deployment depot, select the agent and click **Next**.

   This step does not occur for z/OS agents. z/OS agents cannot be added to the deployment depot.

9. On the Start Copying Files window, read the list of actions to be performed and click **Next** to start the installation.

   The application support packages that you selected are installed.

10. On the Setup Type window, do the following:

    a. Select **Install application support for a local/remote Tivoli Enterprise Monitoring Server**.

    b. Optionally, select the check box for launching the Manage Tivoli Enterprise Monitoring Services window. (If selected, this window is displayed when the installation procedure is finished.)

c. Clear the check boxes for any components that you have already installed on this computer, such as the monitoring server.
d. Click **Next**.

11. On the two Tivoli Enterprise Monitoring Server configuration windows that are displayed, make sure the information is correct and click **Next**.
12. Enable application support on the monitoring server:

    In Step 7 on page 166, you selected the application support packages that you wanted to install on the monitoring server. In this step, you activate the application support through a process known as *seeding* the monitoring server.

    a. Specify the location of the monitoring server to which to add application support. You have two choices:
       - **On this computer**
       - **On a different computer**

       Click **OK**.
    b. Click **OK** on the Select the application support to add to the TEMS window.

       This window lists the application support packages that you selected in Step 7 on page 166. Click **OK** to begin seeding the monitoring server (using the SQL files listed on this window). This process can take up to 20 minutes.
    c. Click **Next** on the message that provides results for the process of adding application support. A return code of 0 (rc: 0) indicates that the process succeeded.

       Note: If the Application Support Addition Complete window is not displayed after 20 minutes, look in the IBM\ITM\CNPS\Logs\ seedk*pp*.log files (where *pp* is the two-character code for each monitoring agent) for diagnostic messages that help you determine the cause of the problem.
13. Click **Finish** to close the installation wizard.

Linux or UNIX: Installing application support on a monitoring server: Complete the following steps to install application support for monitoring agents on a UNIX or Linux monitoring server:

1. Stop the monitoring server by running the following command:

   ```
   ./itmcmd server stop tems_name
   ```
2. Run the following command from the installation media (the agent product CD for distributed agent products or the data files CD for z/OS agent products):

   ```
   ./install.sh
   ```
3. When prompted for the IBM Tivoli Monitoring home directory, press Enter to accept the default (/opt/IBM/ITM) or type the full path to the installation directory you used.
4. The following prompt is displayed:

   ```
   Select one of the following:

   1) Install products to the local host.
   2) Exit install.

   Please enter a valid number:
   ```

   Enter 1 to start the installation.

The software license agreement is displayed.

5. Read through the agreement, then type 1 and press Enter to accept it.

   The installer presents a list of currently installed products, the operating systems for which product packages are available, and component support categories. The support options displayed depend upon the components installed on the system.

6. (*Distributed agent products only, optional*) If you are using a distributed agent product CD, optionally install monitoring agents to this computer. For example, you can install an OS monitoring agent to monitor the operating system. Complete the following steps if you want to install monitoring agents. If you do not want to install monitoring agents, skip to Step 8 on page 170.

   a. Enter the number of the operating system. The default value is the current operating system.

   b. Enter 1 to confirm your selection.

      The installer presents a numbered list of monitoring agents that you can install.

   c. Enter the numbers of the monitoring agents that you want to install or enter the number that corresponds to `All of the above`. Enter more than one number on the same line separated by spaces or commas (,).

      A list of the monitoring agents to be installed is displayed.

   d. Enter 1 to confirm the installation.

   e. After the monitoring agents are installed, the installer asks if you want to install additional products or support packages. Enter 1 and go to Step 8 on page 170.

7. (*z/OS agent products only, required*) If you are using a data files CD, complete the following steps to install required metaprobes. (helper programs) for the monitoring agents that you want to support.

   a. Enter the number of the operating system. The default value is the current operating system.

   b. Enter `y` to confirm your selection.

      The installer presents a numbered list of monitoring agents.

   c. Enter the numbers of the monitoring agents for which you want to install application support, or enter the number that corresponds to `All of the above`. Enter more than one number on the same line separated by spaces or commas (,).

      The installer displays the list of monitoring agents that you selected. For example:

      ```
      The following products will be installed:

        OMEGAMON XE for CICS on z/OS v 4.1.0
        OMEGAMON XE for DB2 PE and PM on z/OS v 4.1.0
        OMEGAMON XE for IMS on z/OS  v 4.1.0
        OMEGAMON XE on z/OS  v 4.1.0
      ```

      Note: The prompt (`The following products will be installed`) seems to indicate that the installer is about to install the listed monitoring agents, which is true for distributed agents. However, for z/OS agents, only metaprobes for the monitoring agents are installed. You cannot install z/OS agents on a monitoring server on Linux or UNIX (and you cannot install monitoring agents from a data files CD).

   d. Enter 1 to confirm the installation.

e. After the metaprobes are installed, the installer asks if you want to install additional products or support packages. Enter `y`.

8. Install the application support package for the Tivoli Enterprise Monitoring Server:
   a. Enter the number for `Tivoli Enterprise Monitoring Server support`.

      A list of the monitoring agents for which you can install application support is displayed.
   b. Enter the numbers of the monitoring agents for which you want to install application support, or enter the number that corresponds to `All of the above`. Enter the numbers on the same line separated by spaces or commas (,).
   c. Enter `1` to confirm the installation.

      The installation begins.
9. After application support for all monitoring agents is installed, you are asked whether you want to install additional products or product support packages. Enter `2`.
10. Start the monitoring server by running the following command:

    `./itmcmd server start` *`tems_name`*
11. Run the following command to activate the application support on the monitoring server:

    `./itmcmd support -t` *`tems_name pc pc pc pc pc ...`*

    where *tems_name* is the name of the monitoring server and *pc* is the product code of each agent.

    To view the product codes for the application support you just installed, run the following command:

    `./cinfo`

    Type `1` when prompted to display the product codes for the components installed on this computer.

    Activate support only for the monitoring agents for which you installed support. For example, if you installed support for the DB2 agent, run the following command:

    `./itmcmd support -t hub_itmdev17 ud`

    where `ud` is the product code for the DB2 agent.

    Note: You can also use Manage Tivoli Monitoring Services to enable application support. See "GUI procedure" on page 122
12. Stop the monitoring server by running the following command:

    `./itmcmd server stop` *`tems_name`*
13. Run the following command to restart the monitoring server:

    `./itmcmd server start` *`tems_name`*

Installing application support on the Tivoli Enterprise Portal Server

Use the following procedures to install application support for non-base monitoring agents on your portal server:

- "Windows: Installing application support on a portal server" on page 171
- "Linux or AIX: Installing application support on a portal server" on page 172

Windows: Installing application support on a portal server: Complete the following steps to install application support for monitoring agents on a Windows portal server:

1. Stop the portal server:
   a. Open Manage Tivoli Monitoring Services.
   b. Right-click **Tivoli Enterprise Portal Server** and click **Stop**.
2. In the /WINDOWS subdirectory on the agent product CD (for distributed products) or data files CD (for z/OS products), double-click the setup.exe file to launch the installation.
3. Click **Next** on the Welcome window.

   Note: If a monitoring agent is already installed on this computer, select **Modify** on the Welcome window to indicate that you are updating an existing installation. Click **OK** on the message telling you about preselected items. Then skip to Step 7.
4. On the Install Prerequisites window, read the information about the required levels of IBM Global Security Toolkit (GSKit) and IBM Java.

   The check box for each prerequisite is cleared if the correct level of the software is already installed. Otherwise, the check box is selected to indicated that the software is to be installed. If you are installing support from the data files CD for z/OS agent products, you might be prompted to install Sun Java Runtime Environment (JRE) 1.4.2, even if you have already installed IBM JRE 1.5 with the distributed components of Tivoli Management Services. The two versions can coexist, and installation of application support for some monitoring agents requires Sun Java 1.4.2. You might also see a message indicating that you can decline the installation of JRE 1.4.2 and that accepting installation of JRE 1.4.2 results in uninstallation of other Java versions. Ignore this message, because you cannot proceed without accepting the installation of Sun Java 1.4.2, and accepting the installation does not uninstall IBM Java 1.5.
5. Click **Next**. The prerequisite software is installed if necessary.

   If the installation program installs IBM GSKit or IBM JRE, you might be prompted to reboot the computer when the installation is complete. If so, you receive an `abort` message with a **Severe error** heading. This is normal and does not indicate a problem.

   If you are prompted to reboot, do the following:
   a. Click **OK** on the window prompting you to reboot.
   b. Click **No** on the window asking whether you want to view the abort log.
   c. Restart the computer.
   d. Restart the installation program.
6. Click **Accept** to accept the license agreement.
7. If you see a message regarding installed versions being newer than the agent installation, click **OK** to ignore this message.
8. Select the application support packages that you want to install:
   a. On the Select Features window, select **Tivoli Enterprise Portal Server**.
   b. Expand the **Tivoli Enterprise Portal Server** node to display a list of application support packages that you can install on the portal server.

      Initially, all application support packages are selected.
   c. Clear the check boxes for application support packages that you do not want to install.

Note: If you are updating an existing installation (you selected **Modify** on the Welcome window), all check boxes on the Select Features window reflect your choices during the initial installation. Clearing a check box has the effect of *uninstalling* the component (for example, the Tivoli Enterprise Portal Server) or product package. Clear a checkbox for an application support package only if you want to remove the application support.

d. If you have other components installed on the same computer, such as the desktop client, also select those components to install the component-specific application support.

e. Click **Next**.

9. On the Start Copying Files window, read the list of actions to be performed and click **Next** to start the installation.

   The application support packages that you selected are installed.

10. On the Setup Type window, clear any components that you have already installed and configured on this computer. Click **Next**.
11. Type the host name for the portal server and click **Next**.
12. Click **Finish** to complete the installation wizard.
13. Restart the portal server.

Linux or AIX: Installing application support on a portal server: Complete the following steps to install application support for monitoring agents on a Linux or AIX portal server:

1. Stop the portal server by running the following command:

   ```
   ./itmcmd agent stop cq
   ```

2. Run the following command from the installation media (the agent product CD for distributed agent products or the data files CD for z/OS agent products):

   ```
   ./install.sh
   ```

3. When prompted for the IBM Tivoli Monitoring home directory, press Enter to accept the default (/opt/IBM/ITM) or enter the full path to the installation directory you used.
4. The following prompt is displayed:

   ```
   Select one of the following:

   1) Install products to the local host.
   2) Exit install.

   Please enter a valid number:
   ```

   Enter 1 to start the installation.

   The software license agreement is displayed.

5. Read through the agreement, then type 1 and press Enter to accept it.

   The installer presents a list of currently installed products, the operating systems for which product packages are available, and component support categories.

6. (*Distributed agent products only, optional*) If you are using a distributed agent product CD, optionally install monitoring agents to this computer. For example, you can install an OS monitoring agent to monitor the operating system. Complete the following steps if you want to install monitoring agents. If you do not want to install monitoring agents, skip to Step 7 on page 173.

a. Enter the number for the operating system. The default value is the current operating system.
b. Enter 1 to confirm your selection.

   The installer presents a numbered list of monitoring agents that you can install.
c. Enter the numbers of the monitoring agents that you want to install or enter the number that corresponds to `All of the above`. Enter more than one number on the same line separated by spaces or commas (,).

   A list of the monitoring agents to be installed is displayed.
d. Enter 1 to confirm the installation.
e. After the monitoring agents are installed, the installer asks if you want to install additional products or support packages. Enter 1.

7. Install the application support packages for the portal server and browser client. Install application support packages for the portal desktop client if a desktop client is installed on this computer.

   The numbered list of items presented by the installer includes the following application support packages. (The numbers might vary from this example.)

   ```
   28) Tivoli Enterprise Portal Browser Client support
   29) Tivoli Enterprise Portal Desktop Client support
   30) Tivoli Enterprise Portal Server support
   ```

   Note: The Tivoli Enterprise Portal Browser Client support package is portal server code that supports the browser clients. You *must* install the browser client support package on the computer where you install the portal server.

   Repeat the following steps for each support package:
   a. Enter the number that corresponds to the support package (for example, 28).

      A numbered list of monitoring agents is displayed.
   b. Enter the numbers that correspond to the monitoring agents for which you want to install the application support package, or enter the number that corresponds to `All of the above`. Type the numbers on the same line separated by spaces or commas (,).
   c. Enter 1 to confirm the installation.

      The installation begins.
   d. After the support package is installed, you are asked whether you want to install additional products or product support packages. Enter 1 to install an additional package and repeat the preceding steps. Enter 2 if you are finished installing support packages.
8. Stop the portal server by running the following command:

   ```
   ./itmcmd agent stop cq
   ```
9. Run the following command to configure the portal server with the new agent information:

   ```
   ./itmcmd config -A cq
   ```

   Complete the configuration as prompted. For information about configuring the portal server, see "Configuring the portal server on Linux or AIX: command-line procedure" on page 139.
10. Restart the portal server by running the following command:

    ```
    ./itmcmd agent start cq
    ```

Installing application support on the Tivoli Enterprise Portal desktop client

Use the following procedures to install application support for non-base monitoring agents on each computer where you are running a desktop client.

Note: You must install application support on desktop clients that were installed from the installation media. You do not need to install application support on desktop clients that were obtained by using IBM Web Start for Java to download the client from the Tivoli Enterprise Portal Server.

- "Windows: Installing application support on a desktop client"
- "Linux: Installing application support on a desktop client" on page 176

Windows: Installing application support on a desktop client: Complete the following steps to install application support for monitoring agents on a Windows desktop client:

1. Stop the portal desktop client:
   a. Open Manage Tivoli Monitoring Services.
   b. Right-click **Tivoli Enterprise Portal Desktop Client** and click **Stop**.
2. In the /WINDOWS subdirectory on the agent product CD (for distributed products) or data files CD (for z/OS products), double-click the setup.exe file to launch the installation.
3. Click **Next** on the Welcome window.

   Note: If a monitoring agent is already installed on this computer, select **Modify** on the Welcome window to indicate that you are updating an existing installation. Click **OK** on the message telling you about preselected items. Then skip to Step 7.
4. On the Install Prerequisites window, read the information about the required levels of IBM Global Security Toolkit (GSKit) and IBM Java.

   The check box for each prerequisite is cleared if the correct level of the software is already installed. Otherwise, the check box is selected to indicated that the software is to be installed. , you might be prompted to install Sun Java Runtime Environment (JRE) 1.4.2, even if you have already installed IBM JRE 1.5 with the distributed components of Tivoli Management Services. The two versions can coexist, and installation of application support for some monitoring agents requires Sun Java 1.4.2. You might also see a message indicating that you can decline the installation of JRE 1.4.2 and that accepting installation of JRE 1.4.2 results in uninstallation of other Java versions. Ignore this message, because you cannot proceed without accepting the installation of Sun Java 1.4.2, and accepting the installation does not uninstall IBM Java 1.5.

Tip

If you are installing support from the data files CD for z/OS agent products, you might be prompted to install Java Runtime Environment (JRE) 1.4.2, even if you have already installed IBM JRE 1.5 with the distributed components of Tivoli Management Services. You might also see a message indicating that you can decline the installation of JRE 1.4.2 and that accepting installation of JRE 1.4.2 results in uninstallation of other Java versions. Ignore this message, because you cannot proceed without accepting the installation of Java 1.4.2, and accepting the installation of Java 1.4.2 does not uninstall IBM Java 1.5. The two versions can coexist. However, the most recently installed version of Java becomes the active version, and the distributed components of Tivoli Management Services V6.2.0 require that JRE 1.5 be the active version.

To change the active version back to JRE 1.5 after you complete installation of application support, follow these steps:

a. Open the Windows Control Panel by selecting **Start > Settings > Control Panel**.
b. From the Windows Control Panel, select **IBM Control Panel for Java**.
c. On the Java tab of the Java Control Panel, click the View button in the Java Application Runtime Settings section.
d. On the JNLP Runtime Settings window, select version 1.5, and make sure the **Enabled** checkbox is selected.
e. Click **OK** twice to save your settings and exit the Java Control Panel.
f. From the Windows Control Panel, select **Java Plug-in**.
g. On the Advanced tab of the Java Plug-in Control Panel, make sure that **JRE 1.5.0** is selected. If you change the setting, click **Apply**.
h. Close the Java Plug-in Control Panel window and the Windows Control Panel.

5. Click **Next** to continue. The prerequisite software is installed if necessary.

   If the installation program installs IBM GSKit or IBM JRE, you might be prompted to reboot the computer when the installation is complete. If so, you receive an `abort` message with a **Severe error** heading. This is normal and does not indicate a problem.

   If you are prompted to reboot, do the following:

   a. Click **OK** on the window prompting you to reboot.
   b. Click **No** on the window asking whether you want to view the abort log.
   c. Restart the computer.
   d. Restart the installation program.
6. Read the software license agreement and click **Accept**.
7. If you see a message regarding installed versions being newer than the agent installation, click **OK** to ignore this message.
8. Select the application support packages that you want to install:
   a. On the Select Features window, select **Tivoli Enterprise Portal Desktop Client**.
   b. Expand the **Tivoli Enterprise Portal Desktop Client** node to display a list of application support packages that you can install on the portal server.

      Initially, all application support packages are selected.

c. Clear the check boxes for application support packages that you do not want to install.

   Note: If you are updating an existing installation (you selected **Modify** on the Welcome window), all check boxes on the Select Features window reflect your choices during the initial installation. Clearing a check box has the effect of *uninstalling* the component or product package. Clear a check box for an application support package only if you want to remove the application support.

d. Click **Next**.

9. On the Start Copying Files window, read the list of actions to be performed and click **Next** to start the installation.

   The application support packages that you selected are installed.

10. On the Setup Type window, clear any components that you have already installed and configured on this computer. Click **Next**.
11. Type the host name for the portal server and click **Next**.
12. Click **Finish** to complete the installation wizard.

Linux: Installing application support on a desktop client: Complete the following steps to install application support for monitoring agents on a Linux desktop client:

Note: Stop the desktop client before performing this procedure.

1. Stop the desktop client by running the following command:

   ```
   ./itmcmd agent stop cj
   ```

2. Run the following command from the installation media (the agent product CD for distributed agent products or the data files CD for z/OS agent products):

   ```
   ./install.sh
   ```

3. When prompted for the IBM Tivoli Monitoring home directory, press Enter to accept the default (/opt/IBM/ITM) or enter the full path to the installation directory you used.
4. The following prompt is displayed:

   ```
   Select one of the following:

   1) Install products to the local host.
   2) Exit install.

   Please enter a valid number:
   ```

   Enter 1 to start the installation.

5. Read through the software license agreement, then type 1 and press Enter to accept the agreement.

   The installer presents a list of currently installed products, the operating systems for which product packages are available, and component support categories.

6. (*Distributed agent products only, optional*) If you are using a distributed agent product CD, optionally install monitoring agents to this computer. For example, you can install an OS monitoring agent to monitor the operating system. Complete the following steps if you want to install monitoring agents. If you do not want to install monitoring agents, skip to Step 7 on page 177.

   a. Enter the number for the operating system. The default value is the current operating system.

b. Enter 1 to confirm your selection.

   The installer presents a numbered list of monitoring agents that you can install.

c. Enter the numbers of the monitoring agents that you want to install or enter the number that corresponds to `All of the above`. Enter more than one number on the same line separated by spaces or commas (,).

   A list of the monitoring agents to be installed is displayed.

d. Enter 1 to confirm the installation.

e. After the monitoring agents are installed, the installer asks if you want to install additional products or support packages. Enter 1.

7. Install the application support package for the portal desktop client:

   a. Enter the number that corresponds to `Tivoli Enterprise Portal Desktop Client support`.

      A numbered list of monitoring agents is displayed.

   b. Enter the numbers that correspond to the monitoring agents for which you want to install the application support package, or enter the number that corresponds to `All of the above`. Type the numbers on the same line separated by spaces or commas (,).

   c. Enter 1 to confirm the installation.

      The installation begins.

8. After application support for all monitoring agents is installed, you are asked whether you want to install additional products or product support packages. Enter 2.

9. Run the following command to configure the desktop client with the new agent information:

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

   Complete the configuration as prompted. For information about configuring the desktop client, see "Linux: Configuring the desktop client" on page 159.

10. Restart the desktop client by running the following command:

    ```
    ./itmcmd agent start cj
    ```

Configuring application support on non-local monitoring servers

The following sections contain procedures for installing and enabling application support on a monitoring server (hub or remote) that is located on a remote computer. For example, you might need to install application support on a hub monitoring server on z/OS for a monitoring agent running on Windows or a Linux operating system. Or you might want to install application support on a monitoring server or client on a different computer than the one on which you are installing an agent or a portal server. If you are using a z/OS hub and you want to aggregate and prune historical data for any agent, you must transfer the catalog and attribute files for the Summarization and Pruning agent to the hub.

The procedures in this section require that either a Tivoli Enterprise Portal Server or a Tivoli Enterprise Monitoring Server be installed on the Windows, Linux, or UNIX computer and configured to communicate with the monitoring server on the non-local computer.

- "Configuring application support on a non-local monitoring server from a Windows system" on page 178

- "Configuring application support on a non-local monitoring server from a Linux or UNIX system" on page 179

Configuring application support on a non-local monitoring server from a Windows system

This section describes how you can install and enable application support on a non-local monitoring server from your local Windows system. The non-local monitoring server can be a hub or remote monitoring server installed on a Windows, Linux, UNIX, or z/OS computer. A monitoring server or a portal server must be installed on the local computer and application support for the agent or agents must be installed on it.

You add support to a non-local monitoring server by copying the k*pp*.cat and k*pp*.atr files for each from the local computer to the non-local computer. If you are adding support to a non-local hub monitoring server, you use Manage Tivoli Monitoring Services to transfer the k*pp*.sql files for each agent.

Copying the CAT and ATR files to the non-local monitoring server: Copy the .cat and .atr files for the agents you want to support from the local Windows monitoring server to the non-local monitoring server. If you use ftp, copy the files in ASCII format. The .cat and .atr files are located in the following directories on the local monitoring server:

- .cat files are located in <*install_dir*>\cms\RKDSCATL
- .atr files are located in <*install_dir*>\cms\ATTRIB

Copy the files to the following directories on the remote computer:

Table 51. Locations of CAT and ATR files for the monitoring server

Remote computer on:	File type	Directory
Windows	.cat	<*install_dir*>\cms\RKDSCATL
	.atr	<*install_dir*>\cms\ATTRIB
Linux or UNIX	.cat	<*install_dir*>/tables/cicatrsq/RKDSCATL
	.atr	<*install_dir*>/tables/cicatrsq/ATTRIB

where <*install_dir*> specifies the IBM Tivoli Monitoring installation directory. The IBM Tivoli Monitoring installation directory is represented by the %CANDLE_HOME% (Windows) or $CANDLEHOME (Linux and UNIX) environment variable. The default installation directory on Windows is /IBM/ITM. The default installation directory on Linux and UNIX is /opt/IBM/ITM.

Note: If you are adding support to a monitoring server on z/OS, you can use the FTP utility provided with Manage Tivoli Monitoring Services. See *IBM Tivoli Monitoring: Configuring IBM Tivoli Enterprise Monitoring Server on z/OS* for instructions.

Adding application support (SQL files) to a non-local hub: If you are adding application support to a non-local hub monitoring server, you must add the SQL files used by the EIB, in addition to the catalog and attribute files. Use the following procedure to seed the hub with SQL files using the Manage Tivoli Enterprise Services utility on your local Windows system:

1. Ensure that the hub monitoring server is started.
2. In the Manage Tivoli Monitoring Services window, select **Actions > Advanced > Add TEMS application support**.

3. On the Add Application Support to the TEMS window, Select **On a different computer** and click **OK**.
4. When you are prompted to ensure that the hub monitoring server is configured and running, click **OK**.
5. On the Non-Resident TEMS Connection window, provide the hub monitoring server TEMS name (node ID) and select the communication protocol to use in sending the application support SQL files to the hub monitoring server.
6. On the next window, provide any values required by the communication protocol.

   For example, if the protocol is IP.PIPE, you are prompted for the fully qualified TCP/IP host name and port number of the z/OS system where the monitoring server is installed. See for the values you recorded during installation planning.
7. On the Select the Application Support to Add to the TEMS window, select the products for which you want to add application support or click Select All to choose all available products. Click **OK**.

   The SQL application support files are added to the hub monitoring server. This might take several minutes.
8. The Application Support Addition Complete window gives you information about the status and location of the application support SQL files. Click Save As if you want to save the information in a text file. Click Close to close the window.

   If the Application Support Addition Complete window is not displayed after 20 minutes, look in the IBM\ITM\CNPS\Logs\seedkpp.log files (where pp is the two-character code for each monitoring agent) for diagnostic messages that help you determine the cause of the problem.
9. If the monitoring server is not already stopped, stop it.
10. Restart the monitoring server.

Configuring application support on a non-local monitoring server from a Linux or UNIX system

This section describes how you can install and enable application support on a non-local monitoring server from your local Linux or UNIX system. The non-local monitoring server can be a hub or remote monitoring server installed on a Windows, Linux, or UNIX system.

Before you begin:

- As a prerequisite, you must install a monitoring server, a portal server or a monitoring agent on the local Linux or UNIX computer. This step is necessary to make the Manage Tivoli Monitoring Services available on the local computer. If you do not have a monitoring server, you must install the support files on the local computer using the procedure described in "Installing application support files on a computer with no monitoring server" on page 182.
- Determine which monitoring agents you want to support on the non-local monitoring server. Ensure that the application support files (.cat, .atr, and .sql files) for those agents are available on the local monitoring server:
  - Application support files are located in the following directories on a Linux or UNIX monitoring server:

Table 52. Locations of application support files on a Linux or UNIX monitoring server

File type	Directory
.cat	<*install_dir*>/tables/cicatrsq/RKDSCATL

Table 52. Locations of application support files on a Linux or UNIX monitoring server (continued)

File type	Directory
.atr	<*install_dir*>/tables/cicatrsq/ATTRIB
.sql	<*install_dir*>/tables/cicatrsq/SQLLIB

  - The file names of the application support files have the following format:

    k*pc*.*ext*

    where *pc* is the product code for the agent and *ext* is the file extension.

    For example, kud.sql is the SQL support file for the DB2 monitoring agent. See Appendix D, "IBM Tivoli product codes," on page 437 for a list of product codes.
  - If you cannot find application support files for some agents for which you want to install application support, install the missing files on this computer.
    - To install missing support files for base monitoring agents, follow the installation steps described in "Installing the monitoring server" on page 119.
    - To install missing files for non-base monitoring agents, follow the installation steps described in "Linux or UNIX: Installing application support on a monitoring server" on page 168.
    - If no monitoring server is installed on this computer, use the procedure in "Installing application support files on a computer with no monitoring server" on page 182.
- Gather the following information about the monitoring server on the remote computer:
  - The host name or IP address
  - The protocol and port number that was specified when the monitoring server was configured

    The monitoring server on the remote computer must be configured to use the IP.UDP, IP.PIPE, or IP.SPIPE communications protocol. This procedure does not support a monitoring server that was configured to use SNA.
- Verify that the monitoring server on the remote computer is running.
- In these instructions, <*install_dir*> specifies the IBM Tivoli Monitoring installation directory. You can enter either $CANDLEHOME or the name of the directory. The default installation directory on Linux and UNIX is /opt/IBM/ITM.

Copying the CAT and ATR files to the non-local monitoring server: Copy the .cat and .atr files for the agents you want to support from the local Linux or UNIX monitoring server to the non-local monitoring server. If you use FTP, copy the files in ASCII format. The .cat and .atr files are located in the following directories on the local monitoring server:

- CAT files are located in <*install_dir*>/tables/cicatrsq/RKDSCATL
- ATR files are located in <*install_dir*>/tables/cicatrsq/ATTRIB

Copy the files to the directory shown in Table 53 on page 181 on the remote computer:

Table 53. Locations of CAT and ATR files for the monitoring server

Remote computer on:	File type	Directory
Windows	.cat	<*install_dir*>\cms\RKDSCATL
	.atr	<*install_dir*>\cms\ATTRIB
Linux or UNIX	.cat	<*install_dir*>/tables/cicatrsq/RKDSCATL
	.atr	<*install_dir*>/tables/cicatrsq/ATTRIB

where <*install_dir*> specifies the IBM Tivoli Monitoring installation directory. The IBM Tivoli Monitoring installation directory is represented by the %CANDLE_HOME% (Windows) or $CANDLEHOME (Linux and UNIX) environment variable. The default installation directory on Windows is /IBM/ITM. The default installation directory on Linux and UNIX is /opt/IBM/ITM.

Note: If you are installing support on a z/OS monitoring server, you can use the FTP utility provided by Manage Tivoli Monitoring Services to copy the .cat and .atr files. See *IBM Tivoli Monitoring: Configuring IBM Tivoli Enterprise Monitoring Server on z/OS* for instructions.

If the non-local monitoring server to which you are adding application support is a hub, you must also install the SQL files used by the EIB. See "Adding application support (SQL files) to a non-local hub."

Adding application support (SQL files) to a non-local hub: To add application support SQL files to a hub monitoring server on a non-local system, complete this procedure.

1. Enable the GUI interface.

   Your Linux or UNIX environment might already have a GUI interface enabled. Otherwise, perform the following tasks to enable it:

   a. Enable X11.
   b. Make sure you have access to a native X-term monitor or an X-Window emulator.
   c. If using an X-Window emulator, enable X11 access to the X-Window server (command example: `xhost +`).
   d. If using an X-Window emulator, set the display environment variable to point to the X-Window server:

      ```
      export DISPLAY=pc_ip_address:0
      ```

2. Ensure that the hub monitoring server is running.
3. To start Manage Tivoli Monitoring Services, go to the $CANDLEHOME bin directory (example: `/opt/IBM/ITM/bin`) and run this command:

   ```
   ./itmcmd manage &
   ```

   A GUI window opens for Manage Tivoli Monitoring Services.
4. Select **Actions > Install product support**.
5. On the Add Application Support to the TEMS window, select **On a different computer** and click **OK**.
6. When you are prompted to ensure that the hub monitoring server is configured and running, click **OK**.
7. On the Non-Resident TEMS Connection window, provide the hub monitoring server TEMS name (node ID) and select the communication protocol to use in sending the application support SQL files to the hub monitoring server.

8. Select the appropriate communications protocol and click OK.
9. On the next window, supply any values required by the selected communication protocol and click **OK**.
10. On the Install Product Support window, select the monitoring agents for which you want to add application support to the hub monitoring server, and click Install.
11. In Manage Tivoli Monitoring Services, look for this message:

    ```
    Remote seeding complete!
    ```
12. Stop and restart the hub monitoring server.

Installing application support files on a computer with no monitoring server: You can install application support files for a monitoring server on a UNIX or Linux computer where no monitoring server is installed and then use the files to configure support on a non-local monitoring server. Use the following procedure to install application support files on computer on which no monitoring server is installed for use on a monitoring server on another computer:

1. Run the following command from the installation media, either the IBM Tivoli Monitoring base media, the agent product CD for distributed agent products or the data files CD for z/OS agent products:

   ```
   ./install.sh
   ```
2. When prompted for the IBM Tivoli Monitoring home directory, press Enter to accept the default (/opt/IBM/ITM) or enter the full path to the installation directory you used.

   The following prompt is displayed:

   ```
   Select one of the following:

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

   Please enter a valid number:
   ```
3. Type 3 and press Enter.

   The software license agreement is displayed.
4. Read through the software license agreement, then type 1 and press Enter to accept the agreement.

   The installer presents a list of currently installed products, the operating systems for which product packages are available, and component support categories.
5. Type the 32-character encryption key to use and press Enter, or just press enter to use the default. This key must be the same key as that used during the installation of the portal server to which the client will connect.

   The installer presents a list of products for which support packages are available.
6. Enter the numbers of the monitoring agents that you want to install or enter the number that corresponds to `All of the above`. Enter more than one number on the same line separated by spaces or commas (,).

   A list of the monitoring agents to be installed is displayed.
7. Confirm the selection by pressing Enter.

   The installer asks if you want to install additional products or support packages.
8. Type 2 and press Enter.

The support packages are installed. When installation is complete, you will see the message

```
... finished postprocessing.
Installation step complete.
```

Installing language packs

Language support for products for which application support is shipped with IBM Tivoli Monitoring appears on the following media:

- *IBM Tivoli Monitoring V6.2 Language Support 1 of 3 DVD* (C60FPML): French, German, Italian, Portuguese Brazilian, Spanish.
- *IBM Tivoli Monitoring V6.2 Language Support 2 of 3 DVD* (C60FPML: Japanese, Korean, Simplified Chinese, Traditional Chinese.
- *IBM Tivoli Monitoring V6.2 Language Support 3 of 3 DVD* (C60FPML): Czech, Hungarian, Polish, Russian
- *IBM Tivoli Monitoring V6.2 DM Upgrade Toolkit Language Support CD*
- *IBM Tivoli Monitoring V6.2 ITM 5.1.2 Migration Toolkit Language Support CD*
- *IBM Tivoli Monitoring V6.2 Agent Builder Toolkit Language Support CD*
- *IBM Tivoli Monitoring Agents for System P Language Support CD*
- Agent product installation CDs

The *IBM Tivoli Monitoring V6.2.0 Language Support* DVDs contain the national language versions of the help and presentation files the components and agents listed in Table 54.

Table 54. Language support included on IBM Tivoli Monitoring V6.2.0 Language Support DVD

Product code	Component or product name
HD	Warehouse Proxy Agent
SY	Warehouse Summarization and Pruning Agent
NT	Monitoring Agent for Windows OS
LZ	Monitoring Agent for Linux OS
UX	Monitoring Agent for UNIX OS
UL	Monitoring Agent for UNIX Logs
UM	Universal Agent
TM	Monitoring Agent for IBM Tivoli Monitoring 5.x Endpoint
P5	IBM Tivoli Monitoring for AIX Base Agent
PX	Premium Monitoring Agent for AIX
PH	Base Monitoring Agent for HMC
PK	Base Monitoring Agent for CEC
PV	IBM Tivoli Monitoring for VIOS Base Agent
VA	Premium Monitoring Agent for VIOS

Language support for the products found on the *IBM Tivoli Monitoring V6.2.0 Tools DVD* is available on the following CDs:

- *IBM Tivoli Monitoring V6.2.0: Language Support for Distributed Monitoring Toolkit CD*

- *IBM Tivoli Monitoring V6.2.0: Language Support for Migration Toolkit CD*
- *IBM Tivoli Monitoring V6.2.0: Language Support for Agent Builder CD*

Language support for all other agents, including those agents for which application support is included on the Base DVD, is included with the installation media for the individual agent.

Install the language packs on any system where you have installed the Tivoli Enterprise Portal or where you have installed a desktop client. (If you download and run a desktop client using Web Start, you do not need to install the language packs on the local system. They are downloaded from the portal server.) *Before you can install a language pack, you must install the component in English*.

Use the following steps to install a language pack:

1. In the directory where you extracted the language pack installation image, launch the installation program as follows:
   - On Windows, double-click the **setup.exe** file.
   - On Linux and UNIX, run the following command:

     `./setup<operating_system>.bin`

     If you want to perform a console installation on Linux or UNIX (instead of a GUI installation), add the **-console** parameter to the above command.
2. Click **Next** on the Welcome window.
3. Select **I accept the terms in the license agreement** and click **Next**.
4. Type the directory where you installed the component in the **Directory Name** field. This directory must match the installation where you installed the component or the installation of the language pack will fail. Click **Next**.
5. Select the language that you want to install on this computer and click **Next**.
6. Review the installation summary and click **Next**.
7. If you are installing the language pack on the computer where you have installed the portal client (client or browser), a message telling you to restart the portal client is displayed. Click **Next**.
8. Click **Finish**.

After installing a Tivoli Monitoring V6.2 Language Pack, reconfigure the portal server and the desktop client. You can reconfigure the portal server and the desktop client using either the Manage Tivoli Monitoring Services utility or the **itmcmd config** command.

Use one of the following methods to reconfigure the affected components:

- Launch Manage Tivoli Monitoring Service, right-click the affected component and select **Reconfigure...**. (See "Starting Manage Tivoli Monitoring Services" on page 207.)
- Change to the `<install_dir>/bin` directory and enter the following commands:

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

Accept the defaults, which reflect the decisions made when the component was installed or last configured.

For SUSE Linux Enterprise Server (SLES) 10 computers only: On the SLES 10 platform, the Tivoli Enterprise Portal displays corrupted text resources in the

Japanese locale. Download the Kochi fonts contained in the kochi-substitute-20030809.tar package from the following Web site: http://sourceforge.jp/projects/efont/files/.

The downloaded tar file includes the truetype fonts (ttf files), which need to be installed on your system. Complete the following steps to install the files:

1. Extract the tar file.
2. Copy the font files (ttf) to X11 font path (for example, `/usr/X11R6/lib/X11/fonts/truetype`).
3. Run **SuSEconfig -module fonts**.

Refer the following Web site for detailed instructions for installing the additional fonts to SuSE Linux: http://www.suse.de/~mfabian/suse-cjk/installing-fonts.html .

Configuring the browser client

When the browser client connects to the Tivoli Enterprise Portal Server, it downloads a Java applet. Before you start the browser client, allocate enough memory for the applet to avoid out-of-memory problems.

To allocate sufficient memory, take the following steps:

1. In the Windows Control Panel, open the Java Control Panel.
2. If you have multiple Java versions, verify that you have the correct control panel open by confirming the Java Runtime is Version 1.5 and that the JRE is in the IBM path (such as c:\program files\IBM\Java50\jre\bin). To verify, click on the **Java(TM)** tab and check the **Location** column for the JRE.
3. Set the Java Runtime Parameters:
   a. Click the **Java** tab.
   b. Click the Java Applet Runtime Settings **View** button.
   c. Double-click the **Java Runtime Parameters** field and enter `-Xms128m -Xmx256m -Xverify:none`.
   d. Click **OK**.

   The `-Xms128m` specifies the starting size of the Java heap (128 MB) and `-Xmx256m` specifies the maximum size.
4. Confirm that the Temporary Files settings are set to Unlimited:
   a. Click the **General** tab.
   b. Click **Settings**.
   c. Select **Unlimited** for the **Amount of disk space** to use.
   d. Click **OK**.
5. Clear the browser cache:
   a. In the **General** tab, click **Delete Files**.
   b. In the window that opens, select **Downloaded Applets** and click **OK**.

Specifying the browser used for online help

If you are running the desktop client on Linux, or you want to view the online help with some browser other than Internet Explorer on Windows, you must specify to the portal server the location of the browser you want to use.

- "Windows: Specifying the browser location" on page 186
- "UNIX and Linux: Specifying the browser location" on page 186

- "Web Start: Specifying the browser location" on page 187

Windows: Specifying the browser location

Use the Manage Tivoli Monitoring Services utility to change the location of the browser that the browser or desktop client uses.

1. Launch Manage Tivoli Monitoring Services (**Start > (All) Programs > IBM Tivoli Monitoring > Manage Tivoli Monitoring Services**).
2. In the Manage Tivoli Monitoring Services window, right-click the browser or desktop client and select **Reconfigure**.

   The Configure the Tivoli Enterprise Portal Browser window is displayed. (If you are configuring the desktop client, the Configure Application Instance window is displayed.)
3. Scroll down in the list of variables until you see the `kjr.browser.default` variable.
4. Double-click `kjr.browser.default`.

   The Edit Tivoli Enterprise Portal Browser Parm window is displayed.
5. In the Value field, type the path and the application name of the alternative browser application. For example:

   ```
   C:\Program Files\Mozilla Firefox\firefox.exe
   ```
6. Click **OK** to close the editing window and save the change.
7. Click **OK** to close the reconfiguration window.

UNIX and Linux: Specifying the browser location

To change a property such as the location of the Web browser that the Tivoli Enterprise Portal browser client launches in UNIX, update the shell script file or files that are run and the template that is used when the browser client is configured to create the script file or files that are run. You might have to update one or more of the following files:

Note: All file paths are relative to your *install_dir* directory where you installed IBM Tivoli Monitoring.

Table 55. File locations for changing application properties for UNIX and Linux

File location	Purpose of file
bin/cnp.sh	The default shell script that launches the Tivoli Enterprise Portal browser client.
bin/cnp_*instance*.sh	The shell script for a specific instance you have created, where *instance* is the name of the instance that launches the Tivoli Enterprise Portal browser client.

Table 55. File locations for changing application properties for UNIX and Linux (continued)

File location	Purpose of file
platform/cj/original/cnp.sh_template	The template from which the bin/cnp.sh and bin/cnp_*instance*.sh shell scripts are generated during configuration, where *platform* is the code for the operating system platform on which IBM Tivoli Monitoring is installed. For example: *li6243* for Linux 2.4 on a 32-bit Intel CPU). If you change only `bin/cnp.sh` or `bin/cnp_instance.sh` and do not change this template, the next time you configure the client, a new version of the script is created without the changes you made to `bin/cnp.sh` or `bin/cnp_instance.sh`.

To change the location of the Web browser you must change the above file or files to include a new property:

1. Go to the *install_dir*/bin/cnp.sh and edit the cnp.sh shell script.
2. Add your Web browser location to the last line of the file. In the example below, the Web browser location is */opt/foo/bin/launcher*.
   `-Dkjr.browser.default=/opt/foo/bin/launcher`

   Important: The line is very long and has various options on it, including several other –D options to define other properties. It is very important to add the option in the correct place.

If the last line of your bin/cnp.sh originally looked like the following:

```
${JAVA_HOME}/bin/java -showversion -noverify -classpath ${CLASSPATH}
-Dkjr.trace.mode=LOCAL -Dkjr.trace.file=/opt/IBM/ITM/logs/kcjras1.log
-Dkjr.trace.params=ERROR -DORBtcpNoDelay=true -Dcnp.http.url.host=
-Dvbroker.agent.enableLocator=false
-Dhttp.proxyHost=
-Dhttp.proxyPort=candle.fw.pres.CMWApplet 2>& 1 >> ${LOGFILENAME}.log
```

To set the browser location to */opt/foo/bin/launcher*, change the line to look like the following:

```
${JAVA_HOME}/bin/java -showversion -noverify -classpath ${CLASSPATH}
-Dkjr.browser.default=/opt/foo/bin/launcher
-Dkjr.trace.mode=LOCAL -Dkjr.trace.file=/opt/IBM/ITM/logs/kcjras1.log
-Dkjr.trace.params=ERROR -DORBtcpNoDelay=true -Dcnp.http.url.host=
-Dvbroker.agent.enableLocator=false
-Dhttp.proxyHost=
-Dhttp.proxyPort=candle.fw.pres.CMWApplet 2>& 1 >> ${LOGFILENAME}.log
```

Web Start: Specifying the browser location

Java Web Start deployed applications are described in jnlp deployment files. For IBM Tivoli Monitoring, there is one deployment file that describes the core Tivoli Enterprise Portal framework component and associated jar files, and one deployment file for each and every Tivoli Enterprise Portal-based monitoring solution that is installed. The core Tivoli Enterprise Portal Server deployment file is named `tep.jnlp`. The application deployment file is typically called k*xx*_resources.jnlp or k*xx*.jnlp, where *xx* is the application identifier (a product code, such as `nt`, `ux`, or `lz`). On a Windows computer where the Tivoli Enterprise Portal Server is installed, the file is located in `<itminstall_dir>\CNB` (for example,

c:\IBM\ITM\CNB). On a Linux computer where the Tivoli Enterprise Portal Server is installed, the file is located in <*itminstall_dir*>/<arch>/cw (for example, /opt/IBM/ITM/li6263/cw).

The deployment file instances are generated whenever the Tivoli Enterprise Portal Server is installed or reconfigured (for example, when adding a new monitoring solution to the environment). The contents of these files are based upon two template deployment files (.jnlpt). The core Tivoli Enterprise Portal template deployment file is called tep.jnlpt. The application template deployment file is named component.jnlpt. On a Windows computer where the Tivoli Enterprise PortalTivoli Enterprise Portal is installed, the file is located in <*itminstall_dir*>\Config (for example: c:\IBM\ITM\Config). On UNIX, the file is located in <*itminstall_dir*>/config (for example, /opt/IBM/ITM/config).

In order to add or modify JVM arguments (such as maximum heap size) or other Tivoli Enterprise Portal-based properties (such as RAS1 trace options), it is necessary to edit either the tep.jnlp deployment file or the tep.jnlpt deployment template file. The deployment file is nothing more than XML syntax that describes the Web Start application being deployed. The <resources> element is used to define the JVM arguments, the Tivoli Enterprise Portal properties, jar files, and references to component deployment files.

- Modify the tep.jnlp file if the change will be temporary (for example, setting a trace option for gathering further diagnostics).
- Modify the tep.jnlpt file if the change will be permanent (for example, increasing the maximum heap size to accommodate a larger monitored environment or increased event load).

  If you modify the deployment template file, make sure you then reconfigure the Tivoli Enterprise Portal Server in order to regenerate the instance-level .jnlp deployment files with your changes.

To specify the location of the browser to use to display the online help, add the following property to the <resources> section of the appropriate file:

```
<property name="kjr.browser.default" value="<path where browser is located>" >
```

Starting the Tivoli Enterprise Portal client

After you have successfully installed and configured all the components of your IBM Tivoli Monitoring environment, you can verify the installation and configuration by launching the Tivoli Enterprise Portal to view monitoring data. You can access the Tivoli Enterprise Portal using either the desktop client or the browser client.

Your monitoring server and portal server must be running for the portal client to start successfully.

Starting the desktop client

Follow these steps to start the desktop client:

On Windows:

1. Click **Start → Programs → IBM Tivoli Monitoring → Tivoli Enterprise Portal**.
2. Type your user ID and password in the logon window. The default user ID is sysadmin.
3. Click **OK**.

On Linux, run the following command to start the portal desktop client:

```
./itmcmd agent start cj
```

Starting the browser client

Follow these steps to start the browser client:

1. Start the Microsoft Internet Explorer browser.
2. Type the URL for the Tivoli Enterprise Portal into the **Address** field of the browser:

   http://*TEPS_host_name*:1920///cnp/client

   where *TEPS_host_name* is the host name of the computer where the Tivoli Enterprise Portal Server and browser client are installed.
3. Click **Yes** on the Warning - Security window.
4. Type your user ID and password in the logon window. The default user ID is sysadmin.
5. Click **OK**.

Using Web Start to download and run the desktop client

A desktop client obtained from the Tivoli Enterprise Portal Server through IBM Web Start for Java benefits from centralized administration from the server. Like the browser client, it is automatically configured with the latest updates each time you start the client, and there is no need to configure application support.

Before you use IBM Web Start for Java to download the desktop client from the Tivoli Enterprise Portal Server:

- The Tivoli Enterprise Portal Server must be installed. (See "Installing the Tivoli Enterprise Portal Server" on page 129.)
- IBM 32-bit Runtime Environment for Windows, Java 2, version 5.0 must be installed on the computer to which you want to download the desktop client.

  You can download the IBM JRE installer from the Tivoli Enterprise Portal Server (see "Installing the IBM JRE"). The IBM JRE must be installed as the system JVM.

  If you want to run the desktop client on a system that already has a Tivoli Management Services base component installed (such as a monitoring server or the portal server), there is no need to install the IBM JRE. The correct version of the IBM JRE is installed with the Tivoli Management Services component.

If you run the desktop client using Web Start instead of installing it from the installation media, you must configure the JRE to enable tracing for the desktop client (see "Enabling tracing for the JRE" on page 191).

Installing the IBM JRE

If you intend to download and run the desktop client using Web Start on a computer where no IBM Tivoli Monitoring base component is installed, you must first install IBM Java 1.5. You download an installer from the computer where the Tivoli Enterprise Portal Server is installed:

- "Windows: Installing the IBM JRE"
- "Linux: Installing the IBM JRE" on page 190

Windows: Installing the IBM JRE

Complete the following steps to download the IBM JRE installer from the Tivoli Enterprise Portal Server and install the JRE on a Windows computer:

1. Start the browser on the computer to which you want to download the installer.
2. Enter the following URL in the **Address** field of the browser:

   `http://TEPS_host_name:1920///cnp/kdh/lib/java/ibm-java2.exe`

   where *TEPS_host_name* is the fully qualified host name of the computer where the portal server is installed (for example, `myteps.itmlab.company.com`).
3. When prompted, save thejava/ibm-java2.exe file to a directory on your hard drive.
4. Change to the directory where you saved the java/ibm-java2.exe file and double-click the file to launch the installer to start the installation program.
5. On the pop-up window, select the language from the drop-down list and click **OK**.
6. Click **Next** on the Welcome page.
7. Click **Yes** to accept the license agreement.
8. Accept the default location for installing the JRE or browse to a different directory. Click **Next**.
9. Click **NO** on the message asking if you want to install this JRE as the system JVM.

   Make Java 1.5 the system JVM only if there are no other JREs installed on the computer.
10. If another JRE is currently installed as the system JVM, you are prompted to overwrite the current system JVM. Click **NO**.

    Overwriting the current system JVM may cause applications depending on the current JVM to fail. However, if IBM Java 1.5 is not the system JVM, you cannot use the short cut created by Web Start the first time you download the desktop client. If you want to start the Web Start desktop client using a shortcut, you must create your own (see "Manually creating a shortcut for the Web Start client" on page 193.).
11. Click **Next** on the Start Copying Files window to start installing the JRE.
12. On the Browser Registration window, leave Microsoft Internet Browser selected as the browser to associate with the JRE. Click **Next**.
13. Click **Finish** to complete the installation.

Linux: Installing the IBM JRE

Complete the following steps to download the IBM JRE installer from the Tivoli Enterprise Portal Server and install the JRE on a Linux computer.

1. Start the browser on the computer to which you want to download the installer.
2. Enter the following URL in the **Address** field of the browser:

   ```
   http://teps_hostname:1920///cnp/kdh/lib/java
        /ibm-java2-i386-jre-5.0-5.1.i386.rpm
   ```

   where *teps_hostname* is the fully qualified host name of the computer where the portal server is installed (for example, `myteps.itmlab.company.com`).
3. When prompted, save the installer to disk.
4. Change to the directory where you saved the **ibm-java2-i386-jre-5.0-5.1.i386.rpm** file and launch the installer to start the installation program using the following command:

   ```
   rpm -ivh ibm-java2-i386-jre-5.0-5.1.i386.rpm
   ```

You can also install the JRE without downloading the installer by supplying the URL to the rpm in the command:

```
rpm -ivh http://teps_hostname:1920///cnp/kdh/lib/java
     /ibm-java2-i386-jre-5.0-5.1.i386.rpm
```

Enabling tracing for the JRE

Log files are not created for the desktop client launched through Web Start unless you enable tracing for the JRE.

The logs for a desktop client run using Web Start are located in a different place than logs for the browser client and the desktop client installed from the media. On Windows computers, the logs for the Web Start client are located in the `C:\Documents and Settings\Administrator\Application Data\IBM\Java\Deployment\log` directory. On Linux computers, the logs are located in the `.java/deployment` directory of the home directory of the user ID under which the Java JRE was installed. Java Web Start will create a uniquely named trace file for every independent launch of the application. The files are named **javaws***nnnnn***.trace**, where *nnnnn* is an arbitrary five-digit identifier.

Complete the following steps to enable tracing:

1. Launch the IBM Control Panel for Java.
   - On Windows, select **Start > Control Panel**, then double-click IBM Control Panel for Java.

     You must switch to the Classic view to see and select the Control Panel. Alternatively, you can launch the Control Panel by selecting **Start > Run >** "**C:\Program Files\IBM\Java50\jre\bin\javacpl.exe**".
   - On Linux, change to <*install_dir*>/jre/<*platform*>/bin and run Control Panel:

     ```
     ./Control Panel
     ```
2. Select the **Advanced** tab.
3. Expand the Debugging node in the **Settings** tree and check **Enable Tracing**.
4. Click **OK** to save the setting and close the Java Control Panel.

Downloading and running the desktop client

You can use any of the following three methods to download and run the desktop client using Web Start:

- Entering the URL of the portal server in a browser
- Launching the client from the IBM Java Control Panel
- Entering a URL from the command line

The first time you launch the desktop client, you are prompted to create a shortcut. After that, you can launch the client using the shortcut.

Entering the URL of the portal server in a browser:

Use the following procedure to launch the desktop client from a browser:

1. Start the browser on the computer on which you want to use the desktop client.
2. Enter the following URL in the **Address** field of the browser:

   http://*TEPS_host_name*:1920///cnp/kdh/lib/tep.jnlp

   where *TEPS_host_name* is the fully qualified host name of the computer where the Tivoli Enterprise Portal Server is installed (for example, `myteps.itmlab.company.com`).
3. Click **Run** on the security message.

4. You are asked if you want to create a shortcut on your desktop for the Tivoli Enterprise Portal. Click **Yes** if you want to create the shortcut.

   The desktop client starts and displays the logon window.

   Note: If IBM Java 1.5 is not the system JVM, you cannot use this shortcut. You must create your own. See "Manually creating a shortcut for the Web Start client" on page 193.
5. Enter the user ID and password to log on to the Tivoli Enterprise Portal or click **Cancel** if you do not want to log on at this time. (The default user ID is sysadmin.)

Note: If you set the RAS trace option for the Tivoli Enterprise Portal client as documented in *IBM Tivoli Monitoring: Problem Determination Guide*, when you recycle the client the kcjras1.log should be created in the location from which the client was launched. On Windows this defaults to \Documents and Settings\<*userid*>\Desktop.

Launching the desktop client from IBM Java Control Panel:

IBM Java 1.5 introduces a new control panel for managing both Java applets deployed via the Java plug-in, and Java applications deployed via Web Start. Complete the following steps to launch the desktop client using the control panel:

1. Launch the IBM Java Control Panel:
   - Windows: In the Windows control panel, double-click **IBM Java Control Panel**.

     Note: You must be in the Classic view to see **IBM Java Control Panel**.
   - Linux: Change to `<install_dir>/jre/<platform>/bin` directory (the default is `/opt/IBM/ITM/jre/<platform>/bin` and enter `./Control Panel`.
2. On the **General** tab, in the Temporary Internet Files section, click **Settings**. The Temporary Files Settings window is displayed.
3. Click **View Applications**.
4. On the **User** tab, select Tivoli Enterprise Portal, then click **Launch Online**.

   Web Start downloads and starts the desktop client. When the application is launched, you can close the Control Panel windows.

Launching the desktop client from the command line:

Complete the following steps to launch the desktop client using Web Start from the command line:

1. Open a command prompt and change to the directory where Web Start is installed.

   On Windows, the default directory is `C:\Program Files\IBM\Java50\jre\bin`. On Linux, the default directory is `<install_dir>/jre/<platform>/bin.`.
2. Enter the following command:

   ```
   javaws http://TEPS_host_name:1920///cnp/kdh/lib/tep.jnlp (Windows)
   ./javaws http://TEPS_host_name:1920///cnp/kdh/lib/tep.jnlp (Linux)
   ```

   where *TEPS_host_name* is the fully qualified host name of the computer where the Tivoli Enterprise Portal Server is installed (for example, `myteps.itmlab.company.com`).

Web Start downloads and launches the desktop client.

Manually creating a shortcut for the Web Start client

On Windows, the Web Start executable file for the default Java JVM is copied to the Windows\System32 directory. When you let Web Start create a short cut for launching the desktop client, it uses the file in the System32 directory as the target. If the default JVM is not IBM Java 1.5, the shortcut will not launch the desktop client. You must create a shortcut manually.

To create a shortcut to use to launch the desktop client using Web Start:

1. Right-click on the Windows desktop and select **New > Shortcut** from the popup menu.
2. In the Create Shortcut window, type the following path or click **Browse** and navigate to the executable as shown:

   ```
   C:\Program Files\IBM\Java50\jre\bin\javaws.exe
   ```

3. Click **Next** and type a name for the shortcut in the Select a Title for the Program window. For example:

   ```
   ITM Web Start client
   ```

4. Click **Finish**.

   The shortcut appears on your desktop.

Chapter 7. Deploying monitoring agents across your environment

IBM Tivoli Monitoring provides the ability to deploy monitoring agents from a central location, the monitoring server. Just as there are two types of monitoring agents, there are two types of agent deployment:

- OS agent deployment from the installation image or using the **tacmd createNode** command
- Non-OS agent (such as the DB2 agent) deployment using the Tivoli Enterprise Portal GUI (for other non-OS agents) or the **tacmd addSystem** command

Table 56 describes the steps required to set up and manage remote agent deployment:

Table 56. Remote agent deployment tasks

Goal	Where to find information
Create and populate the agent deploy depot with installable agent images.	"Populating your agent depot"
View and change the contents of the agent depot.	"Managing your agent depot" on page 199
Use one agent depot for all the monitoring servers in your monitoring environment.	"Sharing an agent depot across your environment" on page 199
Deploy an OS agent.	"Deploying OS agents" on page 200
Deploy a non-OS agent.	"Deploying non-OS agents" on page 202

You can also use the remote agent deployment function to configure deployed agents and install maintenance on your agents. For information, see the *IBM Tivoli Monitoring Administrator's Guide*. See the *IBM Tivoli Monitoring Command Reference* for commands that you can use to perform these tasks.

Important:: Run the **tacmd login** command before executing commands from the tacmd library. This requirement does not apply to the addBundles command. Run the **tacmd logoff** command after you finish using the tacmd command library."

Populating your agent depot

The *agent depot* is an installation directory on the monitoring server from which you deploy agents and maintenance packages across your environment. 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 and any prerequisites.

When you add a bundle to the agent depot, you need to add the bundle that supports the operating system to which you want to deploy the bundle. For example, if you want to deploy a DB2 agent bundle to a computer running HP-UX, add the HP-UX-specific agent bundle to the depot. If your depot directory is on Windows and you want to deploy the DB2 agent to HP-UX, load the HP-UX bundle from the DB2 agent installation media for HP-UX. (If you are installing

© Copyright IBM Corp. 2005, 2007

from different media for each platform type, for example, Windows, AIX and Solaris, HP-UX, Linux, you need to add the bundle from the specific platform media for the component.)

You can have an agent depot on each monitoring server in your environment or share an agent depot, as described in "Sharing an agent depot across your environment" on page 199. If you choose to have an agent depot for each monitoring server, you can customize the agent depot based on the types of bundles that you want to deploy and manage from that monitoring server. For example, if you have a monitoring server dedicated to monitoring the DB2 agents in your environment, populate the depot with DB2-related agent bundles. If you deploy an agent from a remote monitoring server, you must have a agent bundle in the depot available to the monitoring server.

Note: Agent depots cannot be located on a z/OS monitoring server.

There are two methods to populate the agent depot:

- "Populating the agent depot from the installation image"
- "Populating the agent depot with the tacmd addBundles command" on page 198

Populating the agent depot from the installation image

Use the following sections to populate your agent depot from the installation image:

- "Windows: Populating the agent depot during installation"
- "Linux and UNIX: Populating the agent depot during installation" on page 197

You can use the installation image to populate the agent depot only when you are populating the depot with bundles for the same operating system as your monitoring server. For example, you can use the installation image to add a bundle for a Windows agent to a Windows monitoring server, but you cannot use the Linux installation image to add a Linux bundle to a Windows monitoring server. If you need to add bundles for operating systems other than that used by your monitoring server, use the **tacmd addBundles** command, as described in "Populating the agent depot with the tacmd addBundles command" on page 198.

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

Windows: Populating the agent depot during installation

The procedure to populate the agent depot from the Windows installation image differs based on the installation image (base IBM Tivoli Monitoring or application agent) that you are using. Use the procedure in this section that applies to the image you are using:

- "Base IBM Tivoli Monitoring installation image"
- "Application agent installation image" on page 197

Base IBM Tivoli Monitoring installation image: Use the following steps to populate the agent depot from the IBM Tivoli Monitoring installation image:

1. Launch the installation wizard by double-clicking the setup.exe file in the \Windows subdirectory of the installation image.

2. Select **Modify** on the Welcome window and click **Next**.
3. Click **OK** the warning message regarding existing components on this computer.
4. Click **OK** on the Add or Remove Features window without making any changes. (Do not clear any selected items because this removes them from the computer.)
5. On the Agent Deployment window, select the agents that you want to add to the depot and click **Next**.
6. Review the installation summary and click **Next** to begin the installation.

   After the agents are added to the agent depot, a configuration window (called the Setup Type window) is displayed.
7. Clear all selected components. You have already configured all components on this computer and do not need to reconfigure any now. Click **Next**.
8. Click **Finish** to complete the installation.
9. Click **Finish** on the Maintenance Complete window.

Application agent installation image: Use the following steps to populate the agent depot from an application agent installation image:

1. Launch the installation wizard by double-clicking the setup.exe file in the \Windows subdirectory of the installation image.
2. Select **Next** on the Welcome window.
3. Click **Next** on the Select Features window without making any changes.
4. On the Agent Deployment window, select the agents that you want to add to the depot and click **Next**.
5. Review the installation summary and click **Next** to begin the installation.

   After the agents are added to the agent depot, a configuration window (called the Setup Type window) is displayed.
6. Clear all selected components. You have already configured all components on this computer and do not need to reconfigure any now. Click **Next**.
7. Click **Finish** to complete the installation.

Linux and UNIX: Populating the agent depot during installation

Use the following steps to populate the agent depot from the Linux or UNIX installation image:

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.
3. If the directory you specified does not exist, you are asked whether to create it. Type `y` to create this directory.
4. The following prompt is displayed:

   ```
   Select one of the following:
   1) Install products to the local host.
   2) Install products to depot for remote deployment (requires TEMS).
   3) Install TEMS support for remote seeding
   4) Exit install.
   Please enter a valid number:
   ```

   Type `2` to start the installation and press Enter.

The end user license agreement is displayed. Press Enter to read through the agreement.

5. Type 1 to accept the agreement and press Enter.
6. Type the number that corresponds to the agent or agents that you want to add to the agent depot and press Enter. If you are going to add more than one agent, use a comma (,) to separate the numbers.

   To select all available agents, type `all`.

   You can select multiple agents with consecutive corresponding numbers by typing the first and last numbers for the agents, separated by a hyphen (-). For example, to add all of the agents between 8 and 12, type `8-12`.

   To clear an agent that you previously selected, type the number for the agent again.

   Note: Use the following keys to navigate the list of agents:

   U Moves up a line in the list.

   D Moves down a line in the list.

   F Moves forward one page in the list.

   B Moves back one page in the list.
7. When you have specified all the agents that you want to add to the agent depot, type `E` and press Enter to exit.

Populating the agent depot with the tacmd addBundles command

To populate the agent depot using the **tacmd addBundles** command, run the following command:

```
tacmd addBundles [-i IMAGE_PATH]
                 [-t PRODUCT_CODE]
                 [-p OPERATING_SYSTEM]
                 [-v VERSION]
                 [-n]
                 [-f]
```

For the full syntax, including parameter descriptions, see *IBM Tivoli Monitoring Command Reference*.

Examples:

- The following example copies every agent bundle, including its prerequisites into the agent depot on a UNIX from the installation media (cd image) located at /mnt/cdrom/:

  ```
  tacmd addbundles -i /mnt/cdrom/unix
  ```
- The following example copies all agent bundles for the Oracle agent into the agent depot on a UNIX computer from the installation media (cd image) located at /mnt/cdrom/:

  ```
  tacmd addbundles -i /mnt/cdrom/unix -t or
  ```
- The following example copies all agent bundles for the Oracle agent into the agent depot on a Windows computer from the installation media (cd image) located at D:\WINDOWS\Deploy:

  ```
  tacmd addbundles -i D:\WINDOWS\Deploy -t or
  ```
- The following example copies the agent bundle for the Oracle agent that runs on the AIX version 5.1.3 operating system into the agent depot on a UNIX computer from the installation media (cd image) located at /mnt/cdrom/:

```
tacmd addbundles -i /mnt/cdrom/unix -t or -p aix513
```

By default, the agent depot is located in the <*itm_installdir*>/CMS/depot directory on Windows and <*itm_installdir*>/tables/<*tems_name*>/depot directory on UNIX. The **tacmd addBundles** command puts the agent bundle in that location unless another location is defined in the monitoring server configuration file for DEPOTHOME.

If you want to change this location, do the following before you run the **tacmd addBundles** command:

1. Open the KBBENV monitoring server configuration file located in the <*itm_installdir*>\CMS directory on Windows and the <*itm_installdir*>/tables/<*tems_name*> directory on Linux and UNIX.
2. Locate the DEPOTHOME variable. If it does not exist, add it to the file.
3. Type the path to the directory that you want to use for the agent depot.
4. Save and close the file.
5. On UNIX or Linux only, add the same variable and location to the kbbenv.ini file located in <*itm_installdir*>/config/kbbenv.ini.

   If you do not add the variable to the kbbenv.ini file, it will be deleted from the KBBENV file the next time the monitoring server is reconfigured.

Managing your agent depot

Use the following commands to manage your agent depot:

Table 57. Agent depot management commands

Command	Description
tacmd listbundles	Lists the details for one or more bundles available to be added to the local agent depot.
tacmd removebundles	Deletes one or more bundles from the local agent depot.
tacmd viewdepot	Lists the types of bundles available in either the local or remote agent depot.

See the *IBM Tivoli Monitoring Command Reference* for the full syntax of these commands.

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

Sharing an agent depot across your environment

If your monitoring environment includes multiple monitoring servers (a hub monitoring server and remote monitoring servers), you can put your agent depot in a central location, such as a shared file system, and access the depot from all of the monitoring servers.

After populating your agent depot with either of the methods described in "Populating your agent depot" on page 195, use the following steps to share the agent depot:

1. Open the KBBENV monitoring server configuration file located in the <*itm_installdir*>\CMS directory on Windows and the <*itm_installdir*>/tables/<*tems_name*> directory on Linux and UNIX.
2. Locate the DEPOTHOME variable. By default, the agent depot is located in the <*itm_installdir*>/CMS/depot directory on Windows and <*itm_installdir*>/tables/<*tems_name*>/depot directory on UNIX.
3. Type the path to the shared agent depot for the DEPOTHOME variable.
4. Save and close the file.
5. On UNIX or Linux only, add the same variable and location to the kbbenv.ini file located in <*itm_installdir*>/config/kbbenv.ini.

   If you do not add the variable to the kbbenv.ini file, it will be deleted from the KBBENV file the next time the monitoring server is reconfigured.

If you are using a Windows monitoring server connecting to a depot on another Windows computer, you must set the service ID for the Windows monitoring server to "Administrator." Also, instead of specifying a mapped drive letter for the path to the depot directory, use the UNC path (such as \\server\share).

Use the following steps to change the service ID:

1. From the Control Panel, double-click **Administrative Tools**.
2. Double-click **Services**.
3. Right-click **Tivoli Enterprise Monitoring Svcs** and click **Properties**.
4. On the **Log On** tab, select **This Account**.
5. Type `Administrator` in the **This Account** field.
6. Type the password for the administrator in the **Password** field. Confirm the password by typing it again in the **Confirm password** field.
7. Click **Enable**.

   If the Administrator user does not have Logon as a service right, you are prompted to add it.

Deploying OS agents

Before you can deploy any non-OS agent, you must first install an OS agent on the computer where you want the non-OS agent to be deployed. In addition to monitoring base OS performance, the OS agent also installs the required infrastructure for remote deployment and maintenance.

Note: Ensure that you have populated your agent depot, as described in "Populating your agent depot" on page 195, before attempting to deploy any agents.

You can install the OS agent locally, as described in "Installing monitoring agents" on page 148 or remotely using the **tacmd createNode** command.

The **tacmd createNode** command creates a directory on the target computer called the *node*. This is the directory into which not only the OS agent is installed, but where any non-OS agents are deployed.

The **tacmd createNode** command uses one of the following protocols to connect to the computers on which you want to install the OS agent:

- Server Message Block (SMB), used primarily for Windows servers
- Secure Shell (SSH), used primarily by UNIX servers, but also available on Windows

  Note: Only SSH version 2 is supported.
- Remote Execution (REXEC), used primarily by UNIX servers, but not very secure
- Remote Shell (RSH), used primarily by UNIX servers, but not very secure

You can specify a protocol to use; if you do not, the **tacmd createNode** command selects the appropriate protocol dynamically.

Requirements for the tacmd createNode command

Before you can use the **tacmd createNode** command to deploy OS agents, ensure the following:

- On Windows, the user ID that you specify using the -u parameter *must* have administrator privileges on the target computer. On UNIX and Linux, you must specify the ″root″ user ID using the -u parameter and the root password using the -p parameter for the **tacmd createNode** command to execute correctly. No other user ID may be specified.
- Any computer to which you want to deploy the OS agent must have a supported protocol installed.
- Security in your environment must be configured to permit createNode to pass through the firewall, using the protocol that you specify in the command parameters.
- On Windows computers:
  - SMB requires that the default, hidden, and administrative share are available on the drive being accessed and on the drive that hosts the System temporary directory.
  - SMB signing is not supported when connecting using SMB. The computer to which you are deploying an OS agent cannot require SMB signing.
  - For Windows XP, disable Simple File Sharing. Simple File Sharing requires that all users authenticate with guest privileges. This is not supported for createNode. To disable Simple File Sharing, do the following:
    1. Open the Windows Explorer.
    2. Click **Tools → Folder Options**.
    3. Click the **View** tab.
    4. Scroll through the list of settings to **Use Simple File Sharing**.
    5. Clear the check box next to **Use Simple File Sharing** and click **OK**.
  - For Windows XP computers with Service Pack 2, disable the Internet Connection Firewall.
  - For Windows XP computers, set Network Access Sharing and Security to ″Classic - local users authenticate as themselves.″ Use the following steps:
    1. From the Control Panel, double-click **Administrative Tools**.
    2. Double-click **Local Security Policy**.
    3. Expand **Local Policies** and click **Security Options**.
    4. Right-click **Network access: Sharing and security for local accounts** and click **Properties**.

5. Select **Classic - local users authenticate as themselves** from the list and click **OK**.

– For all Windows computers, enable remote registry administration. (This is enabled by default.)

- On UNIX systems, if you are using the RSH protocol, run the **tacmd createNode** command as root on the monitoring server.
- If you are deploying the OS agent to a UNIX or Linux computer, that computer must have either the ksh shell. Only the Korn shell is supported for the execution of the installation and runtime scripts.
- If you are using SSH V2 (for either Windows or UNIX), configure SSH on the target computers to permit the use of password authentication. To permit this, do the following:
  1. Edit the /etc/ss/sshd_config file on the target computer.
  2. Locate the following line:
     ```
     PasswordAuthentication no
     ```
  3. Change the `no` to `yes` and save the file.
  4. Restart the daemon.

  Note: If you are using private key authentication in your environment, you do not need to set SSH to permit password authentication.

Using the tacmd createNode command

To deploy an OS agent from the command line interface, use **tacmd createNode** command. For the full syntax, including parameter descriptions, see *IBM Tivoli Monitoring Command Reference*.

For example, the following command deploys the UNIX OS monitoring agent on the server1.ibm.com computer in the /opt/IBM/ITM directory. The installation is done as the root user.

```
tacmd createNode -h server1.ibm.com -d /opt/IBM/ITM -u root
```

Important: Unless you specifically indicate otherwise, the agent that you deploy using this command assumes that the monitoring server to which it connects is the monitoring server from which you run the command. The agent also uses the default settings for the communications protocol (IP.PIPE for protocol type and 1918 for the port). To change these defaults (especially if you are not using the IP.PIPE protocol), use the following property (specified with the **-p** parameter) when running the command: SERVER=[PROTOCOL://][HOST|IP][:PORT]. For example, SERVER=IP.PIPE://server1.ibm.com:1918.

Deploying non-OS agents

You can deploy non-OS agents through the Tivoli Enterprise Portal or from the command line.

Notes:

1. The deployment and configuration of agents varies depending on the specific agent. The following procedures provide generic deployment information. For the exact values required for your agent, see the configuration information in the user's guide for the agent.
2. Ensure that you have populated your agent depot, as described in "Populating your agent depot" on page 195, before attempting to deploy any agents.

3. You must have already installed or deployed an OS agent on the computer where you are now deploying the non-OS agent and the agent must be running.

Deploying through the portal

Before you deploy an agent through the Tivoli Enterprise Portal, application support for that agent must be installed on the portal server (see "Installing and enabling application support" on page 159).

Use the following steps to deploy an agent through the portal GUI:

1. Open the Tivoli Enterprise Portal.
2. In the Navigation tree, 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. Complete 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 stop the deployment, add a new instance of the agent, if possible, or reconfigure the existing agent.

   A message will tell you when the deployment finishes successfully.

Deploying through the command line

To deploy non-OS agents from the command line, use the ***tacmd addSystem*** command. See *IBM Tivoli Monitoring Command Reference* for the full syntax of this command, including parameter descriptions. You can run the **cinfo** command (UNIX) or the **kincinfo -i** command (Windows) to list the product codes for agents installed on the current computer.

For example, the following command deploys the Universal Agent (type `um`) to the stone.ibm.com computer and specifies the UA.CONFIG property:

```
tacmd addSystem -t um -n stone.ibm.com:LZ -p UA.CONFIG="file_unix.mdl"
```

Each agent bundle has its own unique configuration parameters that you need to provide in this command. If you have an installed agent of the same type that you want to deploy, you can view the configuration parameters by running the following command from a monitoring server:

```
tacmd describeSystemType -t pc -p platform
```

An agent of the same type and platform must be deployed into the depot available to the monitoring server from which the command is run. You can also get more information about agent-specific parameters in the agent user's guide for the agent that you want to deploy.

Deploying a Universal Agent

You can use both of the deployment methods described in the previous sections to deploy a Universal Agent instance.

Before you can deploy a Universal Agent instance, you must create directory at the top level of the deploy depot, at the same level as the PACKAGES directory,

named UACONFIG, (For example, if you installed your monitoring server at /opt/IBM/ITM, and named it hub_core, then your depot directory is /opt/IBM/ITM/tables/hub_core/depot and that is where you should create the UACONFIG directory.) If you are deploying a Script Data Provider, you must also create a UASCRIPT directory.

After you create the directories, you must copy your . mdl files to the UACONFIG directory, and any script metafiles to the UASCRIPT directory. Use the agent depot on the monitoring server to which the Universal Agent connects.

To deploy the Universal Agent, add the following parameter to the addSystem command:

```
-p UA.CONFIG=metafile.mdl
```

where *metafile* is the name of the .mdl file that the Universal Agent should use.

To deploy the Universal Agent and its referenced script, add the following parameter to the addSystem command:

```
-p UA.CONFIG=metafile.mdl. UA.SCRIPT=script-filename
```

where *metafile* is the name of .mdl file that the Universal Agent should use and *script-filename* is name of script used by Universal Agent.

If a metafile belonging to a non-default type of Data Provider type (the four default Data Providers are API, Socket, File, and Script) is remotely deployed, there is no automatic mechanism to activate the appropriate Data Provider. For example, if you deploy an ODBC metafile to a remote Universal Agent and that agent has not already been configured to start the ODBC DP, the Data Provider configuration will not happen automatically as a result of the deployment. You must manually configure the ODBC Data Provider on that Universal Agent for the metafile to be usable. For instructions on configuring the Data Provider, see the *IBM Tivoli Universal Agent User's Guide*.

Part 3. Post-installation configuration and customization

The chapters in this section cover configuration procedures that you can perform at any time after you complete the installation and basic configuration.

Chapter 8, "Configuring IBM Tivoli Monitoring components," on page 207, introduces Manage Tivoli Monitoring Services, a utility you can use to start and stop components and to configure or reconfigure components. It includes instructions for starting and stopping Manage Tivoli Monitoring Services and for using the utility to reconfigure a Tivoli Enterprise Monitoring Server, to configure or change connections between agents and monitoring servers, to configure user authentication, and to configure failover support. This chapter also contains instructions for specifying network interfaces for the portal server to use when the monitoring server has multiple TCP/IP interfaces, controlling port number assignments, and configuring the heartbeat interval for agents and monitoring servers.

Chapter 9, "Additional Linux and UNIX configuration," on page 235 contains instructions for disabling fsync() calls, configuring permissions for a monitoring server on non-NIS Solaris computers, and increasing virtual memory on AIX for large environments.

Chapter 10, "Additional Tivoli Enterprise Portal configuration," on page 239 contains instructions for securing communication between clients and the portal server, creating a connection between a portal client and an external Web server, using network address translation (NAT) with a firewall, defining an interface for multiple network interface cards. It also provides serveral firewall scenarios.

Chapter 11, "Configuring IBM Tivoli Monitoring Web Services (SOAP Server)," on page 255 provides instructions on controlling access to the SOAP server installed on hub monitoring servers and for configuring connections between hubs.

© Copyright IBM Corp. 2005, 2007

Chapter 8. Configuring IBM Tivoli Monitoring components

Although the majority of configuration is done during the product installation, you can use the Manage Tivoli Monitoring Services tool to configure components at any time. You can also use the Manage Tivoli Monitoring Services tool to start and stop components.

Note: You can also perform many of these configuration and start and stop procedures from the command line. Where this is possible, the command is included. See *IBM Tivoli Monitoring Command Reference* for a complete description, including parameters, of the commands that you can use in the installation and configuration of IBM Tivoli Monitoring.

You can perform the tasks in Table 58 with the Manage Tivoli Monitoring Services tool:

Table 58. Configuration tasks available through Manage Tivoli Monitoring Services

Task	Where to find information
Start Manage Tivoli Monitoring Services	"Starting Manage Tivoli Monitoring Services"
Change the configuration of the monitoring server	"Changing the configuration of the Tivoli Enterprise Monitoring Server" on page 208
Configure agents and other monitoring components	"Configuring or changing the monitoring server connection for agents" on page 209
Start and stop components	"Starting and stopping components" on page 210
Configure security	"Configuring user authentication" on page 211
Configure failover support for monitoring servers	"Configuring failover support" on page 221
Monitor the status of remote monitoring servers and agents by configuring heartbeat monitoring.	"Configuring the heartbeat interval" on page 232

Starting Manage Tivoli Monitoring Services

Depending on the operating system you are using, the procedure for starting Manage Tivoli Monitoring Services is different.

Starting Manage Tivoli Monitoring Services on Windows computers

Use the following steps to start Manage Tivoli Monitoring Services on a computer running Windows:

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

© Copyright IBM Corp. 2005, 2007

Starting Manage Tivoli Monitoring Services on Linux or UNIX computers

Use the following steps to start Manage Tivoli Monitoring Services on a computer running Linux or UNIX:

1. Change to the bin directory:
   `cd install_dir/bin`
2. Run the following command using the parameters described in Table 59:
   `./itmcmd manage [-h install_dir] [-s]`

Table 59. Parameters for the itmcmd manage command

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

The Manage Tivoli Monitoring Services utility is displayed.

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

Changing the configuration of the Tivoli Enterprise Monitoring Server

You can change the basic configuration of the monitoring server through Manage Tivoli Monitoring Services. Use the following steps:

1. In the Manage Tivoli Monitoring Services window, right-click the monitoring server.
2. Click **Reconfigure** (on Windows) or **Configure** (on UNIX).
3. 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.
4. Click **OK**.
5. Complete the fields settings listed in Table 60for the communications protocol for the monitoring server and click **OK**.

Table 60. Communications protocol settings

Field	**Description**
IP.UDP Settings	
Hostname or IP Address	The host name or IP address for the hub monitoring server.

Table 60. Communications protocol settings (continued)

Field	Description
Port # and/or Port Pools	The listening port for the hub monitoring server.
IP.PIPE Settings	
Hostname 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 number is 1918.
IP.SPIPE Settings	
Hostname or IP Address	The host name or IP address for the hub monitoring server.
Port number	The listening port for the hub monitoring server. The default value is 3660.
SNA Settings	
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.

6. Restart the monitoring server.

On Linux and UNIX, you can also use the **itmcmd config -S** command to change the configuration of a monitoring server.

Configuring or changing the monitoring server connection for agents

To configure or change the monitoring server connection to the agents, use the following procedure.

1. In the Manage Tivoli Monitoring Services window, select the agent whose connection you want to configure. You can select multiple agents by holding down the Shift key or Control key and selecting agents.
2. Click **Actions → Reconfigure**.
3. Identify the communications protocol for communication 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've identified as Protocol 1 fails, Protocol 2 is used.
4. Click **OK**.
5. Complete the following fields and click **OK**:

Table 61. Communications protocol settings

Field	Description
IP.UDP Settings	

Table 61. Communications protocol settings (continued)

Field	Description
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.
IP.PIPE Settings	
Hostname 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 number is 1918.
IP.SPIPE Settings	
Hostname or IP Address	The host name or IP address for the hub monitoring server.
Port number	The listening port for the hub monitoring server. The default value is 3660.
SNA Settings	
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.

6. Restart the agent.

On Linux and UNIX, you can also use the **itmcmd config -A** command to change the configuration of a monitoring agent.

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

Starting and stopping components

You can start and stop the IBM Tivoli Monitoring components from Manage Tivoli Monitoring Services. Use the following steps:

1. Right-click the component (such as a specific agent or the Tivoli Enterprise Portal Server) that you want to start or stop.
2. Click **Start**, **Stop**, or **Recycle** (Windows only) from the menu.

You can also use the following commands to start and stop components:

itmcmd server
Starts and stops a UNIX monitoring server.

itmcmd agent
Starts and stops a UNIX monitoring agent

tacmd startAgent
Starts both Windows and UNIX monitoring agents.

tacmd stopAgent
Stops both Windows and UNIX monitoring agents.

See *IBM Tivoli Monitoring Command Reference* for the syntax of these commands.

Configuring user authentication

Access to the Tivoli Enterprise Portal is controlled through authentication of user IDs that are defined to the Tivoli Enterprise Portal Server. If the hub Tivoli Enterprise Monitoring Server is configured to authenticate users (**Security: Validate User**), the Tivoli Enterprise Portal user ID and a password are authenticated at the hub monitoring server, using the local system registry. Do not enable user authentication on the hub monitoring server until you have completed and tested at least a basic installation of Tivoli Management Services components and IBM Tivoli Monitoring base agents.

Note: The terms "authenticate" and "validate" when used for user ID and password purposes are equivalent. Existing Tivoli Enterprise Monitoring Server code uses the term "validate" for the same purpose that "authenticate" is used in other contexts such as LDAP.

An initial sysadmin user ID with full administrator authority is provided so you can log on to the Tivoli Enterprise Portal and add more user IDs. Before you enable user authentication on the hub monitoring server, at a minimum, add the sysadmin user ID to the network domain user accounts or to the operating system on the host where the hub monitoring server is installed. On Windows, the installer creates a sysadmin user account and asks you to specify a password for that ID. On other systems, an administrator should create the user account, if it does not already exist.

Note: The Windows installer does not set the "Password never expires" option when it creates the sysadmin account. If you do not set this option, the password will expire according to the security policy on the hub computer, and you will not be able to log in to the portal server. Use the Windows Administrative Tools to ensure that the ″Password never expired″ option is selected for the sysadmin user account. For example, on Windows XP use the following procedure:

1. Select **Start → Control Panel → Administrative Tools → Computer Management → Local Users and Groups → Users.**
2. Right-click sysadmin and select **Properties**.
3. On the **General** tab, check **Password never expires**.

If your site uses Lightweight Directory Access Protocol (LDAP) as a central authentication and authorization system, you can configure the hub monitoring server to use LDAP instead of the local registry. Before you enable LDAP authentication, the following tasks must be completed:

- The LDAP administrator must create a sysadmin account, and accounts for any Tivoli Enterprise Portal user accounts that do not already exist, on the LDAP server.
- The LDAP Administrator should provide the attributes to be used for the LDAP filter. The attribute must contain the same name as the Tivoli Enterprise Portal login ID.
- If you want to use SSL for communication between the hub and the LDAP server, a CMS key store and key store stash must be created, using GSKit and

any required certificates must be created and imported. See “Setting up asymmetric encryption” on page 240 for more information.

Note: **ldapsearch** is an LDAP command-line tool available from many LDAP server vendors. You can save a lot of time by running **ldapsearch** to verify the LDAP information before configuring a hub monitoring server for LDAP authentication. You can also use it to troubleshoot problems you encounter with the configuration. See“Running ldapsearch with LDAP configuration” on page 219 for more information.

The following sections describe the steps for configuring user authentication on the hub monitoring server on Windows, Linux, and UNIX operating systems. For hub monitoring servers installed on z/OS, see the instructions for configuring security using a supported system authorization facility on z/OS in *IBM Tivoli Monitoring: Configuring IBM Tivoli Enterprise Monitoring Server on z/OS* or the configuration guide for your monitoring agent product.

Note: LDAP is not supported for hub monitoring servers on z/OS.

Windows: Configuring user authentication

After the hub Tivoli Enterprise Monitoring Server has been installed and configured, perform the following steps to configure user authentication for an environment in which the hub is installed on Windows:

1. Create new users in the Tivoli Enterprise Portal:
   a. Log on to the Tivoli Enterprise Portal using the sysadmin user ID (and password, if Security: Validate Users was left checked when the hub was configured).
   b. In the Tivoli Enterprise Portal, click **Edit → Administer Users**.
   c. Click **Create New User**.
   d. Type a user ID, user name, and optional description for the user. You can specify user IDs already known to the operating system. The user ID can be up to 10 characters and can contain no spaces.
   e. Click **OK** and then **OK** again to close the window.

   Note that when you create a new user in the Tivoli Enterprise Portal, you specify a user ID only, but not a password. The password is created in the next step.

   For more detailed information about creating and maintaining users, see the *IBM Tivoli Monitoring: Administrator's Guide*.
2. Define the new users to the operating system of the hub monitoring server or verify that they already exist.

   From the Control Panel, select **User Accounts** to define a new user to the Windows operating system. Create user IDs that match the user IDs that you created in the Tivoli Enterprise Portal in the preceding step, and provide a password for each user ID.

   Note: If you intend to use LDAP to authenticate users, do not define the user IDs to the operating system. Have an LDAP administrator define or verify the user IDs that correspond to the Tivoli Enterprise Portal IDs on the LDAP server and create or update the filter that maps the two sets of IDs.
3. If it is not already enabled, enable security on the hub:

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

   The Manage Tivoli Monitoring Services window is displayed.

b. Right-click the hub monitoring server and select **Reconfigure**.

   The Tivoli Enterprise Monitoring Server Configuration window is displayed.

c. Check **Security: Validate User**.

   The option **LDAP Security: Validate User with LDAP** becomes available.

d. If you want to use LDAP for user authentication, check the **Validate User with LDAP** option.

e. Click **OK**.

   If you selected the LDAP option, the following panel is displayed:

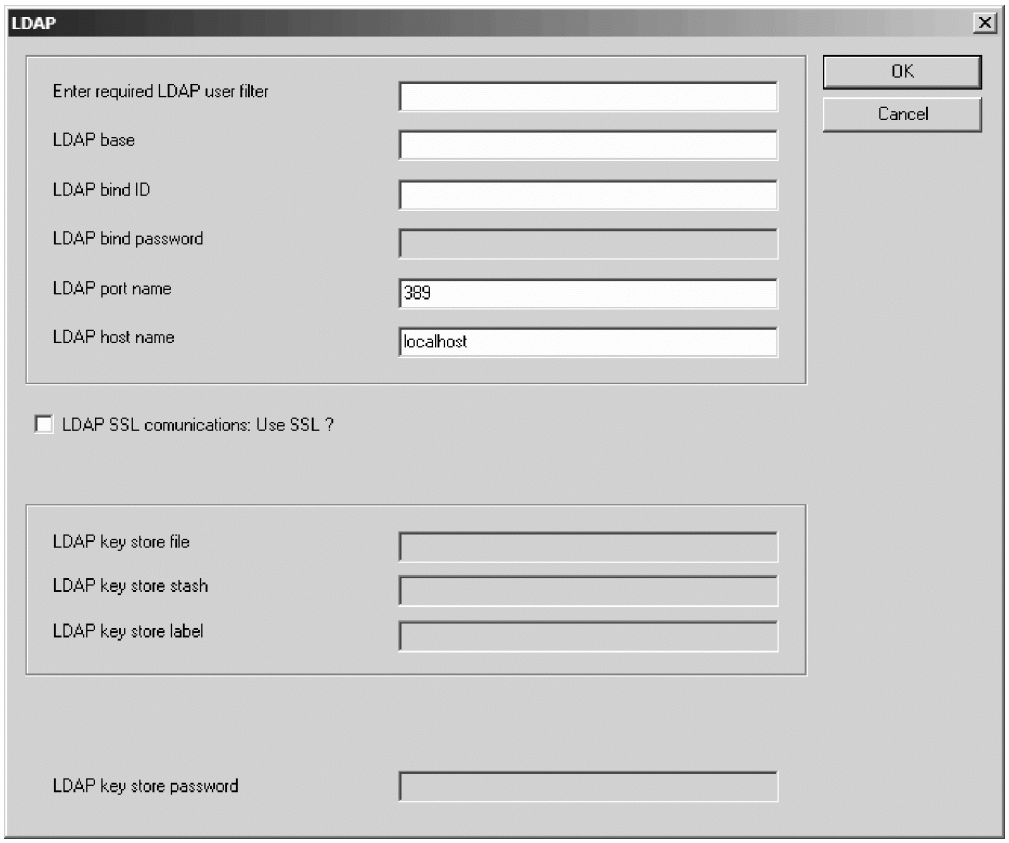


Figure 25. LDAP configuration window

f. Specify the following values, as required for your site, then click **OK**:

LDAP user filter

The LDAP user filter that maps Tivoli Enterprise Portal user IDs to LDAP login IDs. The portal user ID will usually become the "%v" in the LDAP user filter. For example:

```
IBM Tivoli Directory Server: (&(mail=%v@yourco.com)
 (objectclass=inetOrgPerson))
Microsoft Windows Active Directory: (&(mail=%v@yourco.com)
 (objectclass=user))
Sun Java System Directory Server: (&(mail=%v@yourco.com)
(objectclass=inetOrgPerson)
```

Not all LDAPs will necessarily have the mail attribute for the person. For example, the LDAP administrator might only set the common name, in which case the filter would look like the following:

```
(&(cn=%v) (objectclass=inetOrgPerson))
```

The IBM Tivoli Monitoring administrator should verify exactly which LDAP attribute must be used to search for the user. With Active Directory, for example, the **cn** equals the Full Name of the Active Directory user, and this *must* be exactly the same as the Tivoli Monitoring user, and cannot have spaces (for example, ″S Smith″ must be ″SSmith″).

LDAP base
The LDAP base which is used in searches for your LDAP server. Your LDAP administrator should provide this value. Examples:

```
IBM Tivoli Directory Server: dc=yourdomain,dc=yourco,dc=com
Microsoft Windows Active Directory: dc=yourdomain,dc=yourco,dc=com
Sun Java System Directory Server: dc=yourdomain,dc=yourco,dc=com
```

LDAP bind ID
The LDAP user ID for bind authentication. This LDAP user ID must be authorized to search for LDAP users based on the LDAP filter. This value can be omitted if an anonymous user can search for LDAP users.

LDAP bind password
The password for LDAP bind authentication. This value can be omitted if an anonymous user can bind to your LDAP server. This value is encrypted by the installer.

LDAP port name
The LDAP server port number. This value can be omitted if your LDAP server is listening on port 389.

LDAP host name
The LDAP server host name. This value can be omitted if your LDAP server is on the same host as the Tivoli Enterprise Monitoring Server. (The default is localhost.)

LDAP SSL Communications: Use SSL?
Specifies that Secure Socket Layer (SSL) communications be used to the LDAP server. If SSL is enabled, enter values for the following:

LDAP key store file
The location of GSKit key store data base file. You can specify any location. For example:

```
C:\IBM\ITM\keyfiles
```

LDAP key store stash
The location of the GSKit database password file. For example:

```
C:\IBM\ITM\keyfiles\keyfile.sth
```

LDAP key store label
The key store label. For example:

```
IBM_Tivoli_Monitoring_Certificate
```

LDAP key store password
The password required to access the key store. This value is encrypted.

The Hub TEMS Configuration window is displayed.

g. Click **OK** to accept the current settings.

4. In the Manage Tivoli Monitoring Services window, restart the hub monitoring server by right-click its name and selecting **Start**.

Linux or UNIX: Configuring user authentication

After the hub Tivoli Enterprise Monitoring Server has been installed and configured, perform the following steps to configure user authentication for an environment in which the hub is installed on Linux or UNIX:

1. Create new users in the Tivoli Enterprise Portal:
   a. Log on to the Tivoli Enterprise Portal using the sysadmin user ID. You do not need a password.

      The Tivoli Enterprise Portal recognizes the sysadmin user ID even though it has not been defined to the operating system. You do not need a password because the hub monitoring is not yet configured to validate users.
   b. In the Tivoli Enterprise Portal, click **Edit → Administer Users**.
   c. Click **Create New User**.
   d. Type a user ID, user name, and optional description for the user. You can specify user IDs already known to the operating system, such as root.
   e. Click **OK** and then **OK** again to close the window.

   Note that when you create a new user in the Tivoli Enterprise Portal, you specify a user ID only, but not a password. The password is created in the next step.

   For more detailed information about creating and maintaining users, see the *IBM Tivoli Monitoring: Administrator's Guide*.
2. Define the sysadmin user and the new users that you created in the preceding step to the operating system of the hub monitoring server, or verify that they already exist.

   Note: If you intend to use LDAP to authenticate users, do not use the following procedures. Have an LDAP administrator define or verify the user IDs that correspond to the Tivoli Enterprise Portal IDs on the LDAP server and create or update the filter that maps the IDs.

   To create a new user, follow the procedures for your operating system. For example, the following commands define a user to a hub monitoring server that is installed on a UNIX or Linux operating system:

   ```
   useradd -d <home_dir> <userID>
   passwd <userID>
   ```

   where <*userID*> is the new user ID and <*home_dir*> is any directory you specify to be the login directory for the user. After you enter the `passwd` command, follow the prompts to create a password for the specified user ID.
3. Configure the hub monitoring server to validate users. You can configure the hub from the command line or using Manage Tivoli Monitoring Services.
   - From the command line:
     a. Change to the *install_dir*/bin directory and run the following command:

        ```
        ./itmcmd config -A tems_name
        ```

        where *install_dir* is the installation directory for IBM Tivoli Monitoring, and *tems_name* is the name of the hub monitoring server. The default installation directory on Linux or UNIX is /opt/IBM/ITM.

        You see the following prompt:

        ```
        Configuring TEMS...
        ```

b. Accept the defaults for the following prompts. The defaults should reflect the selections you made during installation.

c. When you see the prompt:

```
Security: Validate User?
```

type 1 and press Enter.

d. If you do not want to use LDAP for authentication, press Enter to select the default (NO). If you want to use LDAP for authentication, type 1 and press Enter. Respond to following prompts as shown below:

Enter required LDAP user filter

The LDAP user filter that maps Tivoli Enterprise Portal user IDs to LDAP login IDs. Your LDAP administrator should provide the attribute to be used for this filter. The attribute must contain the same name as the Tivoli Enterprise Portal login ID.

The portal user ID will usually become the "%v" in the LDAP user filter. For example:

```
IBM Tivoli Directory Server: (&(mail=%v@yourco.com)
  (objectclass=inetOrgPerson))
Microsoft Windows Active Directory: (&(mail=%v@yourco.com)
  (objectclass=user))
Sun Java System Directory Server: (&(mail=%v@yourco.com)
  (objectclass=inetOrgPerson)
```

Not all LDAPs will necessarily have the mail attribute for the person. For example, the LDAP administrator might only set the common name, in which case the filter would look like the following:

```
(&(cn=%v) (objectclass=inetOrgPerson))
```

The IBM Tivoli Monitoring administrator should verify exactly which LDAP attribute must be used to search for the user. With Active Directory, for example, the **cn** equals the Full Name of the Active Directory user, and this *must* be exactly the same as the Tivoli Monitoring user, and cannot have spaces (for example, "S Smith" must be "SSmith").

LDAP base

The LDAP base which is used in searches for your LDAP server. Your LDAP administrator should provide this value. Examples:

```
IBM Tivoli Directory Server: cn=yourRealm,ou=yourOU,o=yourO,c=yourC
  or any parent branch in the tree such as ou=yourOU,o=yourO,c=yourC
  or even o=yourO,c=yourC
Microsoft Windows Active Directory: dc=yourdomain,dc=yourco,dc=com
Sun Java System Directory Server: dc=yourdomain,dc=yourco,dc=com
```

LDAP bind ID

The LDAP user ID for bind authentication. This LDAP user ID must be authorized to search for LDAP users based on the LDAP filter. This value can be omitted if an anonymous user can search for LDAP users.

LDAP bind password

The password for LDAP bind authentication. This value can be omitted if an anonymous user can bind to your LDAP server. This value is encrypted by the installer.

LDAP port name

The LDAP server port number. This value can be omitted if your LDAP server is listening on port 389.

LDAP host name
The LDAP server host name. This value can be omitted if your LDAP server is on the same host as the Tivoli Enterprise Monitoring Server. (The default is localhost.)

LDAP SSL Communications: Use SSL?
Specifies that Secure Socket Layer (SSL) communications be used to the LDAP server. If SSL is enabled, enter values for the following parameters:

LDAP key store file
The location of GSKit key store data base file. You can specify any location. For example:

```
/opt/IBM/ITM/keyfiles
```

LDAP key store stash
The location of the GSKit database password file. For example:

```
/opt/ibm/itm/keyfiles/keyfile.sth
```

LDAP key store label
The key store label. For example:

```
IBM_Tivoli_Monitoring_Certificate
```

LDAP key store password
The password required to access the key store. This value is encrypted.

e. Accept the defaults for the Tivoli Event Integration Facility and the Workflow Policy/Tivoli Emitter Agent Forwarding.

f. At the following prompt, type 6 (Save/exit) and press Enter:

```
Hubs
##      CMS_Name
1       ip.pipe:elsrmt1[4441]
```

- Using Manage Tivoli Monitoring Services:

a. Change to the *install_dir*/bin directory and run the following command:

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

where *install_dir* is the installation directory for IBM Tivoli Monitoring. The default installation directory on Linux or UNIX is /opt/IBM/ITM.

The Manage Tivoli Monitoring Services window is displayed.

b. Right-click the hub monitoring server and click **Configure**.

c. Click the **Advanced Setting** tab. Select **Security: Validate User**.

d. If you want to use LDAP to authenticate users instead of the system registry, select **LDAP user authentication**.

e. Click **OK**.

If you selected the LDAP option, the LDAP configuration panel is displayed.

f. Specify the values as shown below, then click **OK**:

Enter required LDAP user filter
The LDAP user filter that maps Tivoli Enterprise Portal user IDs to LDAP login IDs. Your LDAP administrator should provide the name of this file.

The portal user ID will usually become the "%v" in the LDAP user filter. For example:

```
IBM Tivoli Directory Server: (&(mail=%v@yourco.com)'
  (objectclass=inetOrgPerson))
Microsoft Windows Active Directory: (&(mail=%v@yourco.com)
  (objectclass=user))
Sun Java System Directory Server: (&(mail=%v@yourco.com)
  (objectclass=inetOrgPerson)
```

LDAP base
The LDAP base that is used in searches for your LDAP server. Your LDAP administrator should provide this value. Examples:

```
IBM Tivoli Directory Server: dc=yourdomain,dc=yourco,dc=com
Microsoft Windows Active Directory: dc=yourdomain,dc=yourco,dc=com
Sun Java System Directory Server: dc=yourdomain,dc=yourco,dc=com
```

LDAP bind ID
The LDAP user ID for bind authentication. This LDAP user ID must be authorized to search for LDAP users based on the LDAP filter. This value can be omitted if an anonymous user can search for LDAP users.

LDAP bind password
The password for LDAP bind authentication. This value can be omitted if an anonymous user can bind to your LDAP server. This value is encrypted by the installer.

LDAP port name
The LDAP server port number. This value can be omitted if your LDAP server is listening on port 389.

LDAP host name
The LDAP server host name. This value can be omitted if your LDAP server is on the same host as the Tivoli Enterprise Monitoring Server. (The default is localhost.)

LDAP SSL Communications: Use SSL?
Specifies that Secure Socket Layer (SSL) communications be used to the LDAP server. If SSL is enabled, enter values for the following parameters:

LDAP key store file
The location of GSKit key store data base file. You can specify any location. For example:

```
/opt/IBM/ITM/keyfiles
```

LDAP key store stash
The location of the GSKit database password file. For example:

```
/opt/ibm/itm/keyfiles/keyfile.sth
```

LDAP key store label
The key store label. For example:

```
IBM_Tivoli_Monitoring_Certificate
```

LDAP key store password
The password required to access the key store. This value is encrypted.

The Hub TEMS Configuration window is displayed.

g. Click **OK**.

This procedure stops the monitoring server.

4. Restart the hub monitoring server, using one of the following methods:

- In the Tivoli Enterprise Monitoring Services window, right-click the hub monitoring server and select **Start**.
- From the command line, enter:

  `itmcmd server` *`tems_name`*

Running ldapsearch with LDAP configuration

ldapsearch is an LDAP command-line tool available from many LDAP server vendors. You can save a lot of time by running **ldapsearch** to verify the LDAP information before configuring a hub monitoring server for LDAP authentication. You can also use it to troubleshoot problems you encounter with the configuration. Ideally, **ldapsearch** is run by the LDAP administrator.

The **ldapsearch** command operates something like the ping command. If the values you use as input to the command are correct, the command returns a version of the values you use in the search. If the values are not correct, the command returns either nothing, or an error message that can help you determine which value is involved, such as an incorrect password or a bad host name.

IBM Tivoli Directory Server (ITDS) **ldapsearch** is the best suited for Tivoli Monitoring. The ITDS **ldapsearch** supports GSKit SSL operations used in Tivoli Monitoring and has additional command-line options to support LDAP SSL searches. Tivoli Monitoring does not include ldapsearch with production installation. For information on IBM Tivoli Directory Server ldapsearch see http://publib.boulder.ibm.com/infocenter/tivihelp/v2r1/topic/com.ibm.IBMDS.doc/commandref05.htm#ldapsrch.

ldp.exe is a Microsoft Windows LDAP search tool which has the same basic features as **ldapsearch**. It can be downloaded from Microsoft Website for your version of windows. **ldp.exe** is included in the Windows Server 2003 CD support tools. For information on using Microsoft Windows **ldp** command, see http://support.microsoft.com/kb/224543.

The following sections describe the command-line options for the **ldapsearch** tool and provide examples of its use for configurations with and without SSL enabled.

- "**ldapsearch** command-line options"
- "Sample **ldapsearch** command (no SSL)" on page 220
- "Sample **ldapsearch** command (with SSL)" on page 220

ldapsearch command-line options

Table 62 shows the command line options and the corresponding LDAP setting parameters on the hub monitoring server.

Table 62. **ldapsearch** *command line options and corresponding monitoring server configuration parameters*

Option	Description	Corresponding Parameter in TEMS configuration file
-h *host*	The host name of LDAP server.	KGL_LDAP_HOST_NAME
-p *port*	The LDAP port number.	KGL_LDAP_PORT
-D *dn*	The LDAP bind ID Do not use this command-line option if LDAP bind ID is not required.	KGL_LDAP_BIND_ID

Table 62. **ldapsearch** *command line options and corresponding monitoring server configuration parameters (continued)*

Option	Description	Corresponding Parameter in TEMS configuration file
-w password	The LDAP bind password Use the unecrypted value for the **ldapsearch** command-line option. Do not use this command-line option if LDAP bind ID is not required.	KGL_LDAP_BIND_PASSWORD
-b base_dn	The LDAP base.	KGL_LDAP_BASE
-K keyfile	The LDAP key store file (used only with LDAP SSL).	KGL_KEYRING_FILE
-P key_pw	The LDAP key store password (used only with LDAP SSL). Use the unecrypted value for the ldapsearch command-line option.	KGL_KEYRING_PASSWORD decrypted value
-N key_name	The LDAP key store label (used only with LDAP SSL).	KGL_KEYRING_LABEL
Filter	LDAP user filter. Replace %v with Tivoli Enterprise Portal, SOAP, or tacmd user ID.	KGL_LDAP_USER_FILTER

Sample ldapsearch command (no SSL)

For a configuration with the following values for which SSL is not enabled and no bind ID and password are required:

LDAP host name	ldap.itm62.com
LDAP port name	389
LDAP base	ou=itm62users,o=itm62.com
LDAP user filter	″(mail=%v@us.ibm.com)″

you would use the follow command:

```
ldapsearch -h ldap.itm62.com -p 389 -b "ou=itm62users,o=itm62.com"
 -s sub "(mail=sysadmin@itm62.com)"
```

If the input values were correct, you would receive the following as output:

```
uid=12345678,ou=itm62users,o=itm62.com
objectClass=person
objectClass=organizationalPerson
...
mail=sysadmin@itm62.com
...
```

Sample ldapsearch command (with SSL)

For a configuration with SSL enabled and bind ID and password required, with the following values:

LDAP host name	ldap.itm62.com
LDAP port name	636
LDAP bind ID	uid=1,ou=itm62users,o=itm62.com
LDAP bind password	itm62
LDAP base	ou=itm62users,o=itm62.com

LDAP key store	C:\IBM\ITM\itm62keyfiles\keyfile.kdb
LDAP key stash	C:\IBM\ITM\itm62keyfiles\keyfile.sth
LDAP keystore label	BM_Tivoli_Monitoring_Certificate
LDAP keystore password	itm62
LDAP user filter	"(mail=%v@us.ibm.com)"

you would use the following command:

```
ldapsearch -h ldap.itm62.com -p 636 -D uid=1,ou=itm62users,o=itm62.com
    -w itm62 -b "ou=itm62users,o=itm62.com" -s sub
    -K C:\IBM\ITM\itm62keyfiles\keyfile.kdb -P itm62
    -N "IBM_Tivoli_Monitoring_Certificate" "(mail=sysadmin@itm62.com)"
```

If the input values were correct, you would receive the following as output:

```
uid=12345678,ou=itm62users,o=itm62.com
objectClass=person
objectClass=organizationalPerson
...
mail=sysadmin@itm62.com
...
```

Configuring failover support

The optional Hot Standby feature enables you to maintain high availability by defining a standby monitoring server to provide failover support for your hub monitoring server. If the hub monitoring server fails, hub functions automatically switch to the backup monitoring server. IBM Tivoli Monitoring automatically connects all remote monitoring servers and agents to the backup monitoring server.

Configuring the Hot Standby feature involves the following steps:

1. "Configuring the Hot Standby feature for hub monitoring servers"
2. "Configuring the Hot Standby feature for remote monitoring servers" on page 225
3. "Configuring the Hot Standby feature for monitoring agents" on page 227
4. "Verifying that failover support is working" on page 227

Configuring the Hot Standby feature for hub monitoring servers

The two hub monitoring servers that you configure for Hot Standby (the Primary Hub and the Secondary Hub) must be mirrors of each other:

- The IBM Tivoli Monitoring software on both hub monitoring servers must be at the same release and maintenance level.
- Application support for all required applications must be installed on both monitoring servers.

Perform the following procedures to configure the Primary Hub and Secondary Hub monitoring servers for the Hot Standby feature. These procedures and the examples are ordered as if both hub monitoring servers are installed on the same operating system. However, it is possible to have one hub on Windows and the other hub on UNIX. Complete the procedure that applies to each system.

Windows: Configuring the Hot Standby feature for hub monitoring servers

Complete the following steps to configure the Primary Hub and Secondary Hub monitoring servers for the Hot Standby feature on Windows. On the configuration windows shown as examples in this procedure, the Primary Hub is named HUB_PRIMARY and the Secondary Hub is named HUB_SECONDARY. Actual names can be different.

Configuring the Primary Hub: Complete the following steps to configure the Primary Hub to point to the Secondary Hub as its backup or standby server:

1. On the Manage Tivoli Monitoring Services window, right-click the name of the monitoring server that you are going to use as the Primary Hub and click **Reconfigure**.
2. Complete the following steps on the Tivoli Enterprise Monitoring Server Configuration window:
   a. Enter the name of the Primary Hub in the **TEMS Name** field.
   b. Select the **Configure Hot Standby TEMS** check box to configure the Secondary Hub as a standby server for the Primary Hub.
   c. Specify the protocols used by the Secondary Hub. These protocols must be the same for both monitoring servers (the Primary Hub and Secondary Hub).

      Figure 26 shows an example of a completed configuration window:

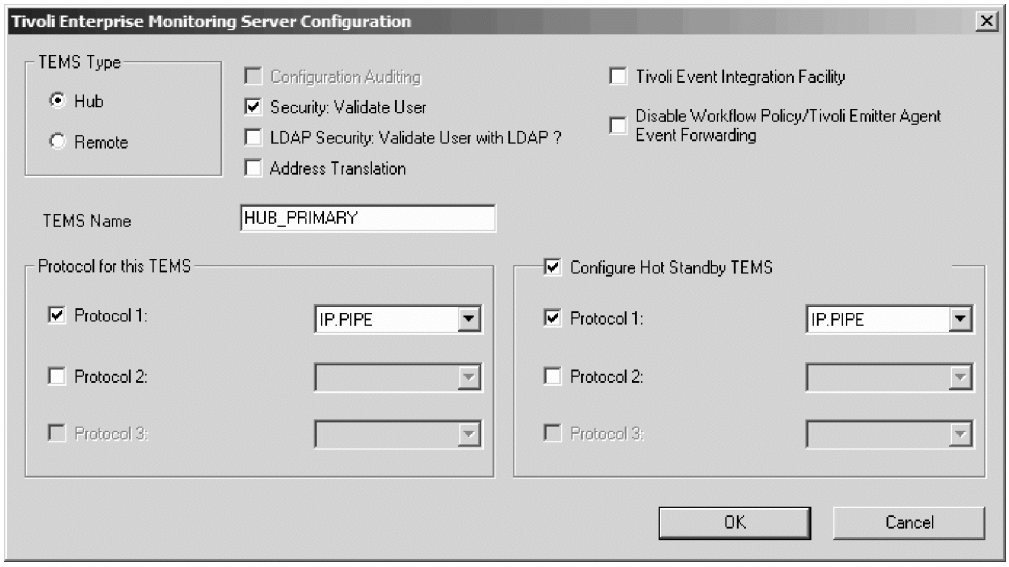


Figure 26. Tivoli Enterprise Monitoring Server Configuration window: Primary Hub configuration

   d. Click **OK**.
3. On the Hub TEMS Configuration window, enter the host name or IP address of the Primary Hub and verify the communication settings for this server. Click **OK**.
4. On the Hub TEMS Configuration for Hot Standby window, specify the Secondary Hub as the standby server for the Primary Hub. Enter the host name or IP address of the Secondary Hub in the **Hostname or IP Address** field, as

shown in the following example.

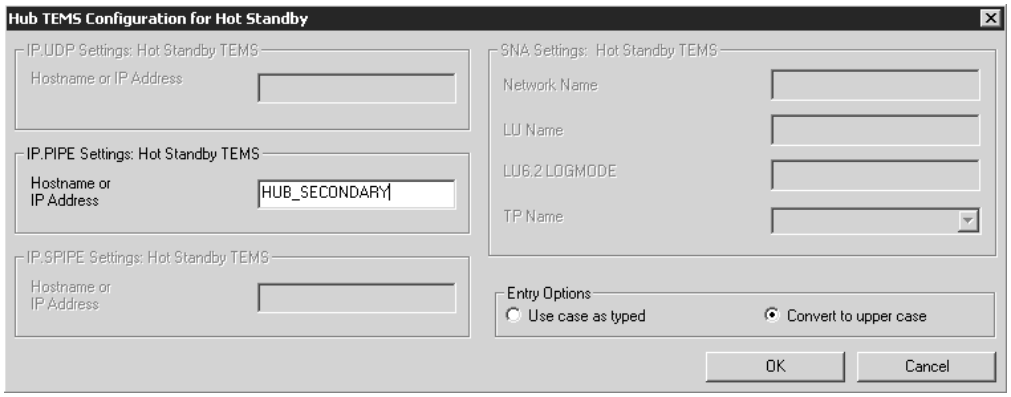


Figure 27. Specifying the Secondary Hub as a backup or standby server for the Primary Hub

5. Click **OK**.
6. Restart the monitoring server. (On Windows, the monitoring server stops automatically.)

Configuring the Secondary Hub:

Complete the following steps to configure the Secondary Hub to point to the Primary Hub as the backup or standby server:

1. On the Manage Tivoli Monitoring Services window, right-click the name of the monitoring server that you are going to use as the Secondary Hub and click **Reconfigure**.
2. Complete the following steps on the Tivoli Enterprise Monitoring Server Configuration window:
   a. Type the name of the Secondary Hub in the **TEMS Name** field.
   b. Select the **Configure Hot Standby TEMS** check box to configure the Primary Hub as a standby server for the Secondary Hub.
   c. Specify the protocols used by the Primary Hub. These protocols must be the same for both monitoring servers (the Primary Hub and Secondary Hub).

      Figure 28 on page 224 shows an example of a completed configuration window:

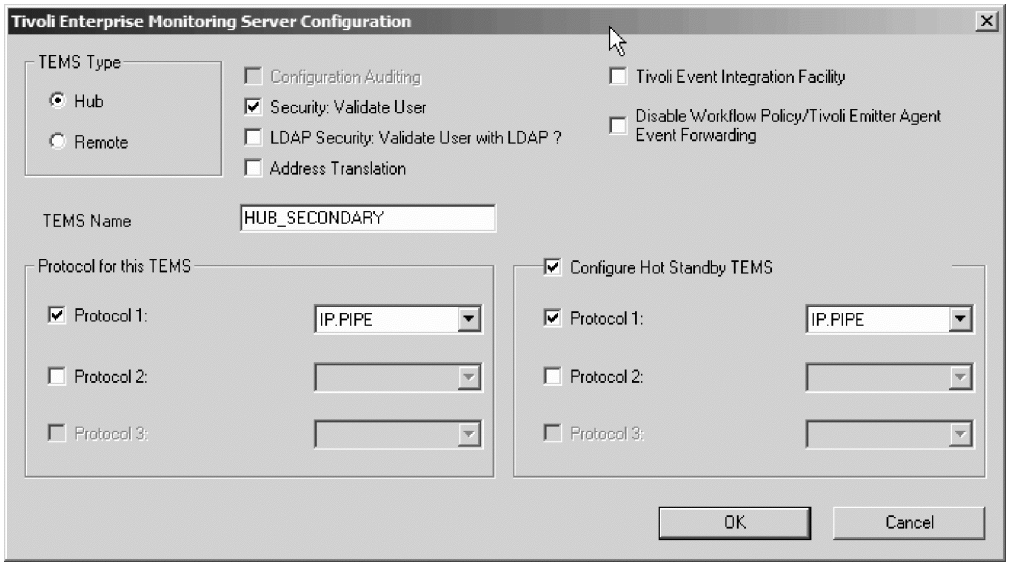


Figure 28. Tivoli Enterprise Monitoring Server Configuration window: Secondary Hub configuration

d. Click **OK**.

3. On the Hub TEMS Configuration window, enter the host name or IP address of the Secondary Hub and verify the communication settings for this server. Click **OK**.
4. On the Hub TEMS Configuration for Hot Standby window, specify the Primary Hub as the standby server for the Secondary Hub. Enter the host name or IP address of the Primary Hub in the **Hostname or IP Address** field, as shown in the following example.

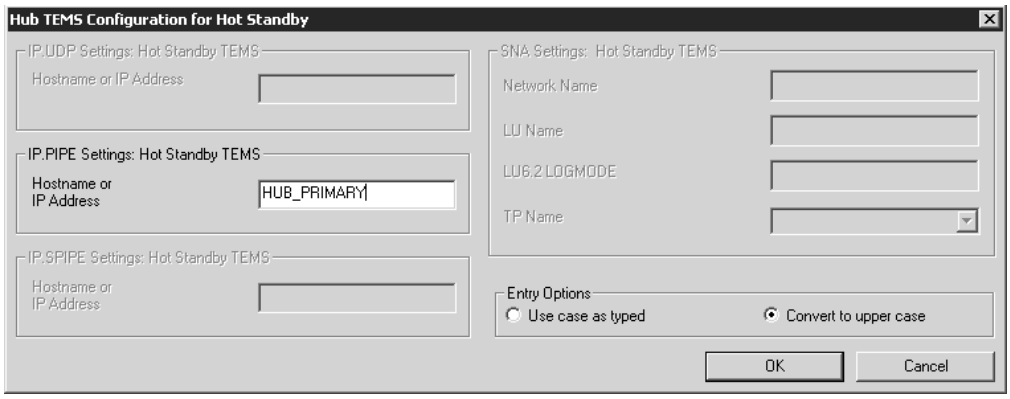


Figure 29. Specifying the Primary Hub as a backup or standby server for the Secondary Hub

5. Click **OK**.
6. Restart the monitoring server. (On Windows, the monitoring server stops automatically.)

Linux or UNIX: Configuring the Hot Standby feature for hub monitoring servers

Complete the following steps to configure the Primary Hub and Secondary Hub monitoring servers for the Hot Standby feature on Linux or UNIX computers.

Configuring the Primary Hub:

Complete the following steps to configure the Primary Hub to point to the Secondary Hub as its backup or standby server:

1. On the Manage Tivoli Monitoring Services window, right-click the name of the monitoring server that you are going to use as the Primary Hub and click **Configure**.
2. Click the **Advanced Settings** tab.
3. Select **Specify Hot Standby**.
4. Type the host name of the Secondary Hub in the **Standby TEMS Site** field.
5. Select the type of protocol to use for hot standby. This must be the same protocol on both the Primary Hub and Secondary Hub.
6. If you specified any backup protocols for the Primary Hub, specify identical protocols for the Secondary Hub.
7. Click **Save**.
8. Stop and restart the monitoring server.

Configuring the Secondary Hub:

Complete the following steps to configure the Secondary Hub to point to the Primary Hub as its backup or standby server:

1. On the Manage Tivoli Monitoring Services window, right-click the name of the monitoring server that you are going to use as the Secondary Hub and click **Configure**.
2. Click the **Advanced Settings** tab.
3. Select **Specify Hot Standby**.
4. Type the host name of the Primary Hub in the **Standby TEMS Site** field.
5. Select the type of protocol to use for hot standby. This protocol must be the same protocol that is specified on both the Primary Hub and Secondary Hub.
6. If you specified any backup protocols for the Secondary Hub, specify identical protocols for the Primary Hub.
7. Click **Save**.
8. Stop and restart the monitoring server.

Configuring the Hot Standby feature for remote monitoring servers

Configure remote monitoring servers to switch to a standby hub monitoring server when the acting hub monitoring server becomes unavailable. Configure all remote monitoring servers consistently by specifying the Primary Hub as the hub to which they connect, and the Secondary Hub as the standby hub.

Windows: Configuring the Hot Standby feature for remote monitoring servers

Complete the following steps on Windows to configure a remote monitoring server to switch to a standby hub when the acting hub monitoring server becomes unavailable:

1. On the Manage Tivoli Monitoring Services window, right-click the name of a remote monitoring server and click **Reconfigure**.
2. Complete the following steps on the Tivoli Enterprise Monitoring Server Configuration window:
   a. In the **TEMS Type** field, select **Remote** to indicate that this is a remote monitoring server.

b. Enter the name of the remote monitoring server in the **TEMS Name** field.
c. Select the **Configure Hot Standby TEMS** check box to configure a standby server.
d. Specify the protocols used by the standby server. (The protocols are the same for the Primary Hub and Secondary Hub.)

   Figure 30 shows an example of a completed configuration window:

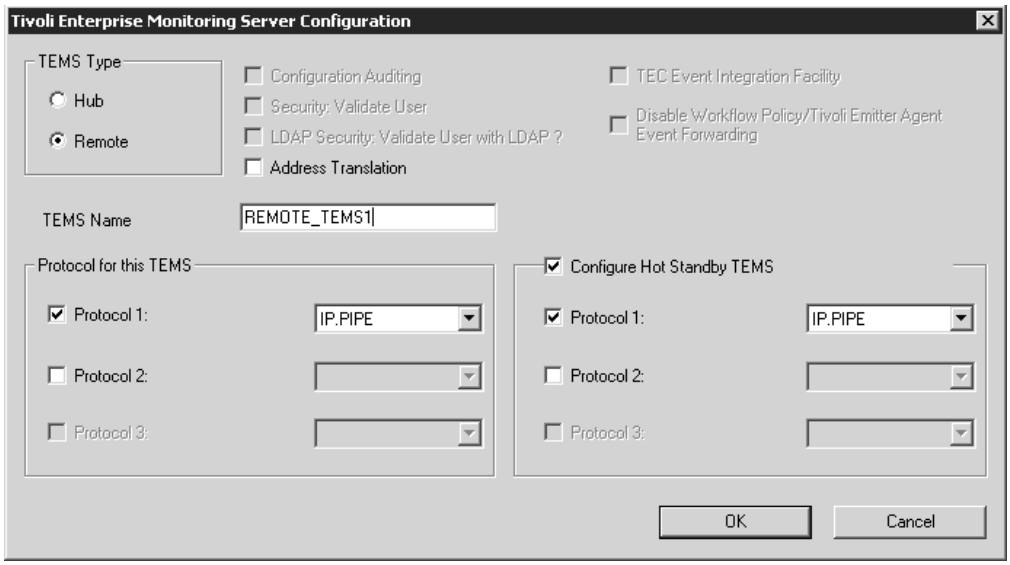


Figure 30. Configuring Hot Standby for a remote monitoring server

e. Click **OK**.

3. On the Hub TEMS Configuration window, enter the host name or IP address of the Primary Hub and verify the communication settings for this server. Click **OK**.
4. On the Hub TEMS Configuration for Hot Standby window, specify the Secondary Hub as the standby server. Enter the host name or IP address of the Secondary Hub in the **Hostname or IP Address** field.
5. Click **OK**.
6. Restart the remote monitoring server. (On Windows, the monitoring server stops automatically.)

Linux or UNIX: Configuring the Hot Standby feature for remote monitoring servers

Complete the following steps on Linux or UNIX to configure a remote monitoring server to switch to a standby hub when the acting hub monitoring server becomes unavailable:

1. On the Manage Tivoli Monitoring Services window, right-click the name of a remote monitoring server and click **Configure**.
2. Click the **Advanced Settings** tab.
3. Select **Specify Hot Standby**.
4. Type the host name of the Secondary Hub in the **Standby TEMS Site** field.
5. Select the type of protocol to use for hot standby. This is the same protocol on both the Primary Hub and Secondary Hub.

6. If you specified any backup protocols for the hub monitoring servers, specify identical protocols for the remote monitoring server.
7. Click **Save**.
8. Stop and restart the monitoring server.

Configuring the Hot Standby feature for monitoring agents

Configure any monitoring agents that report directly to the hub monitoring server, as well as the Warehouse Proxy agent and Summarization and Pruning agent, to switch to a standby hub monitoring server when the acting hub monitoring server becomes unavailable. Configure all agents consistently by specifying the Primary Hub as the hub to which they connect, and the Secondary Hub as the standby hub. All agents on the same computer must be set up with same primary and secondary servers. Otherwise, there is a chance that they will not connect back to the same monitoring server after when they are restarted.

Complete the following steps:

1. On the Manage Tivoli Monitoring Services window, right-click a monitoring agent and click **Reconfigure** (on Windows) or **Configure** (on UNIX).
2. Select **Optional: Secondary TEMS Connection** and specify the protocol for the standby monitoring server.

   On UNIX agents, click **Protocols** to display a separate window where you can configure the standby server (Secondary Hub).

   Figure 31 shows an example of a completed configuration window on Windows:

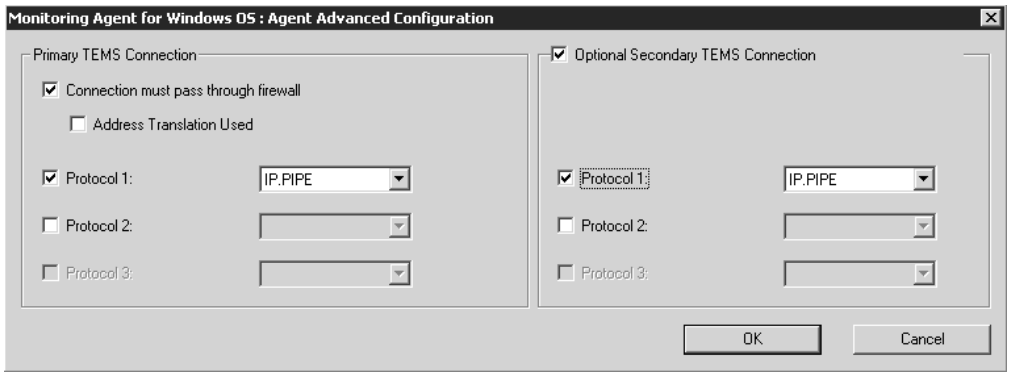


Figure 31. Configuring a monitoring agent to connect to a standby hub monitoring server

3. Click **OK**.
4. Enter the host name or IP address of the Primary Hub and the port number and click **OK**.
5. Enter the host name or IP address of the Secondary Hub and click **OK**.
6. Restart the monitoring agent.

Verifying that failover support is working

To verify that the failover support provided by the Hot Standby feature is working, take your hub monitoring server offline by stopping it in Manage Tivoli Monitoring Services. Once the hub monitoring server has stopped, reconfigure the Tivoli Enterprise Portal Server to point to the backup monitoring server and restart the portal server. Open the Tivoli Enterprise Portal. If everything is configured correctly, you can open the portal and view data.

Specifying network interfaces

If there are multiple TCP/IP interfaces on the computer on which a monitoring server is running, you need to identify which interfaces monitoring agents or the Tivoli Enterprise Portal Server should use when connecting to the monitoring server. Setting network interfaces affects all the components installed on the local computer.

To specify the network interfaces to be used by the portal to connect to a hub monitoring server, or by a monitoring agent to connect to a hub or remote, complete these steps:

Note: For instructions on configuring a network interface list on z/OS, see the *IBM Tivoli Monitoring: Configuring IBM Tivoli Enterprise Monitoring Server on z/OS*.

1. In the Manage Tivoli Monitoring Services window, select **Actions > Advanced > Set Network Interface**.
2. On the Set Desired Network Interface window specify the network interface or interface you want to use.

   Specify each network adapter by the host name or IP address to be used for input and output. Use a blank space to separate the entries. If your site supports DNS, you can specify IP addresses or short host names. If your site does not support DNS, you must specify fully qualified host names.
3. Click **OK** to close save the settings and close the window.

Controlling port number assignments

IBM Tivoli Monitoring assigns port numbers to each component in an installation to be used for communication with other components. Default well-known ports are reserved for major components such as monitoring servers and the portal server. For all other components, an algorithm calculates the listening port to reserve.

You might want to change or add to the default assignments under some conditions, for example, when the default port assigned to a monitoring agent has already been reserved by another application, or the portal server requires a second port number for communication through a firewall with Network Address Translation (NAT).

Configuring port number assignments for the monitoring server

The default IP.UDP and IP.PIPE listening port setting for the Tivoli Enterprise Monitoring Server is 1918. For IP.SPIPE, it is 3660. For SNA, it is 135. While you can specify a different port during or after installation, it is best to use the default setting. To reconfigure the port after installation, see "Configuring or changing the monitoring server connection for agents" on page 209.

Configuring port number assignments for the portal server

Communications between Tivoli Enterprise Portal clients and the Tivoli Enterprise Portal Server are controlled by a portal server interface definition. The default interface definition assigns port 15001 to the Tivoli Enterprise Portal Server and ports 1920 (for HTTP requests) and 3661 (for HTTPS) to the integrated Web server that is installed with the portal server. You can define additional interfaces to allow

access through a firewall with NAT or through a secondary Network Interface Card (NIC). See "Firewall network address translation (NAT) or multiple network interface cards" on page 247.

The following sections describe how to change port number assignments on the portal server for connections to Tivoli Enterprise Portal clients (browser clients and desktop clients).

Changing the port number for browser client connections to the portal server

A portal server on Windows, Linux, or UNIX uses port 1920 for HTTP connections and 3661 for HTTPS connections from portal browser clients.

Do not change the default port settings, especially on multifunction UNIX and Linux systems, since many components might be located on the same system and some of these components might depend on the default values being used for HTTP and HTTPS ports.

If you need to change the default settings, you can change them by using the KDE_TRANSPORT environment variable:

On Windows:

1. In the Manage Tivoli Enterprise Monitoring Services window, right-click **Tivoli Enterprise Portal Server**, point to **Advanced**, and select **Edit ENV File** to open the KFWENV file.
2. Add the following line to the file:

   ```
   KDE_TRANSPORT=HTTP:1920 HTTPS:3661
   ```

   Substitute the port numbers you want to use.
3. If a KDC_FAMILIES ennvironment variable exists in the file, copy the settings from that variable to KDE_TRANSPORT (except the ones you want to override). KDE_TRANSPORT supersedes and overrides KDC_FAMILIES.
4. Save the file.
5. Recycle the portal server. (Right-click **Tivoli Enterprise Portal Server** and select **Recycle**.)

On Linux or AIX:

1. Change to the *install_dir*/config directory (where *install_dir* is the IBM Tivoli Monitoring installation directory).
2. Add the following line to the cq.ini file:

   ```
   KDE_TRANSPORT=HTTP:1920 HTTPS:3661
   ```

   Substitute the port numbers you want to use.
3. If a KDC_FAMILIES ennvironment variable exists in the file, copy the settings from that variable to KDE_TRANSPORT (except the ones you want to override). KDE_TRANSPORT supersedes and overrides KDC_FAMILIES.
4. Recycle the portal server.

Changing the port number for desktop client connections to the portal server

Use the following procedure for each desktop client instance you want to change:

1. In the Manage Tivoli Enterprise Monitoring Services window, right-click the Tivoli Enterprise Portal Desktop instance that you want to change, and select **Reconfigure**.

   The Configure Application Instance window opens.

2. In the **Parms** list, scroll down to `cnp.http.url.port` and double-click.
3. On the Edit window, perform the following steps:
   a. Change the port number value to the port number you want.
   b. Select the **In Use** check box.

      Note: If you fail to select this check box, the port number value that you entered will revert to the original value.
   c. Click **OK**.
4. On the Configure Application Instance window, verify that the port number value (in the **Value** column) for `cnp.http.url.port` has changed.
5. Click **OK**.

Configuring port number assignments for monitoring agents

IBM Tivoli monitoring uses the following algorithm to allocate port numbers for monitoring agents to reach the monitoring server:

reserved port = *well-known port* + (N*4096)

where:

- *well-known port* is the port number assigned to the monitoring server, for example, 1918.
- *N* indicates the position of the monitoring agent in the startup sequence for agents.

For example, if there are two monitoring agents on a system, and the monitoring server uses port 1918, the first monitoring agent in the startup sequence is assigned port 6014 (1918 + 1*4096) and the second agent to start is assigned port 10110 (1918 + 2*4096).

For "piped" protocols such as IP.PIPE and IP.SPIPE (but not IP or SNA), you can control the way port numbers are assigned to a monitoring agent by using the SKIP and COUNT parameters on the KDE_TRANSPORT environment variable for the agent. See the following example:

```
KDE_TRANSPORT=IP.PIPE PORT:1918 COUNT:1 SKIP:2 IP use:n SNA use:n IP.SPIPE use:n
```

See also the following information about using the IP.PIPE and IP.SPIPE protocols and parameters:

- The PORT parameter specifies the well-known port for the monitoring server.
- The COUNT:*N* parameter is the mechanism for reserving IP.PIPE ports for components that connect to the monitoring server. *N* is the number of IP.PIPE ports to reserve on a host in addition to the well-known port for the monitoring server. Use the COUNT parameter to reserve ports for components that must be accessible from outside a firewall. Accessibility from outside the firewall requires IP.PIPE ports and because these ports must be permitted at the firewall, the ports must be predictable.

  For example, if the well-known port is 1918, COUNT:3 starts the search at port 6014 (1918 + 1*4096). If the agent process cannot bind to port 6014, the algorithm tries port 10110 (1918 + 2*4096). If port 10110 is not available, the search goes to port 14206 (1918 + 3*4096).

  The agent is assigned to the first available port encountered in the search. The process fails to start if the search reaches the highest port without a successful binding (port 14206 in this example).

- The SKIP:*N* parameter specifies the number of ports to skip when starting the search for an available port using the port assignment algorithm. Use the SKIP parameter for components that do not need access across a firewall.

  For example, if the well-known port is 1918, SKIP:2 specifies to start the search at port 10110 (1918 + 2*4096), skipping ports 1918 and 6014 (1918 + 1*4096). The algorithm continues searching until it finds an available port.
- The USE parameter enables or disables a protocol. To disable a protocol, specify `use:n`. To enable a protocol, specify `use:y`. This parameter has no default.

Example

The example in Table 63 shows the coding to use on a system that contains the components shown:

Table 63. Using COUNT and SKIP variables to assign port numbers

Component	Coding
Tivoli Enterprise Monitoring Server	The monitoring server uses port 1918.
Warehouse Proxy agent Requires firewall access	`KDE_TRANSPORT=IP.PIPE COUNT:1` This coding reserves port 6014 (1918 + 1*4096) for the Warehouse Proxy agent.
Windows OS agent Does not require firewall access	`KDE_TRANSPORT=IP.PIPE SKIP:2` With this coding, the port assignment algorithm skips ports 1918 and 6014 (reserved for the monitoring server and Warehouse Proxy agent), and starts at port 10110 (1918 + 2*4096). If the Windows OS agent fails to open port 10110, the agent tries port 14206 and so on, until it finds an available port or exhausts all possibilities.

Adding the KDE_TRANSPORT environment variable

The KDE_TRANSPORT environment variable must be added to the appropriate file (*ENV file on Windows, *.ini file on UNIX).

Note: The KDE_TRANSPORT variable supersedes and overrides the KDC_FAMILIES variable. If a KDC_FAMILIES variable exists in the file, merge the KDC_FAMILIES settings with the KDE_TRANSPORT settings. Copy the KDC_FAMILIES settings that you want to keep to the new KDE_TRANSPORT variable.

Use the following procedures to add the KDE_TRANSPORT environment variable to the appropriate file:

On Windows:

Add the KDE_TRANSPORT environment variable to the ENV file for the component.

For example, the ENV file for the Windows OS agent is named KNTENV, where NT is the product code for the Windows OS agent. For a list of product codes, see Appendix D, “IBM Tivoli product codes,” on page 437.

Edit the ENV file from the Manage Tivoli Enterprise Services window:

1. In the Manage Tivoli Enterprise Monitoring Services window, right-click the component that you want to change, point to **Advanced**, and select **Edit ENV File**.
2. Add a line similar to the following example:

   ```
   KDE_TRANSPORT=IP.PIPE PORT:1918 COUNT:N SKIP:N
        IP use:n SNA use:n IP.SPIPE use:n
   ```

   where *N* is the number of ports to reserve (COUNT:*N*) or the number of ports to skip (SKIP:*N*). This example uses the IP.PIPE protocol. It also applies to IP.SPIPE.
3. Search the file for a KDC_FAMILIES environment variable. If a KDC_FAMILIES variable exists in the file, merge its settings with the new KDE_TRANSPORT variable. The KDE_TRANSPORT variable supersedes and overrides the KDC_FAMILIES variable.
4. Save the file.
5. Recycle the component. (Right-click the component and select **Recycle**.)

On Linux or UNIX:

Add the KDE_TRANSPORT environment variable to the *pc*.ini file, where *pc* is the product code for the component.

Search the file for a KDC_FAMILIES environment variable. If a KDC_FAMILIES variable exists in the file, merge its settings with the new KDE_TRANSPORT variable. The KDE_TRANSPORT variable supersedes and overrides the KDC_FAMILIES variable.

For example, add the KDE_TRANSPORT variable for the Windows OS agent to the nt.ini file (where nt is the product code for the Windows OS agent). For a list of product codes, see Appendix D, “IBM Tivoli product codes,” on page 437.

The .ini files are located in the *install_dir*/config directory, where *install_dir* is the IBM Tivoli Monitoring installation directory. The default installation directory on Linux and UNIX is /opt/IBM/ITM.

Configuring the heartbeat interval

IBM Tivoli Monitoring uses a heartbeat mechanism to monitor the status of remote monitoring servers and monitoring agents. The different monitoring components in the monitoring architecture form a hierarchy (shown in Figure 32 on page 233) across which the heartbeat information is propagated.

The hub monitoring server maintains status for all monitoring agents. Remote monitoring servers offload processing from the hub monitoring server by receiving and processing heartbeat requests from monitoring agents, and communicating only status changes to the hub monitoring server.

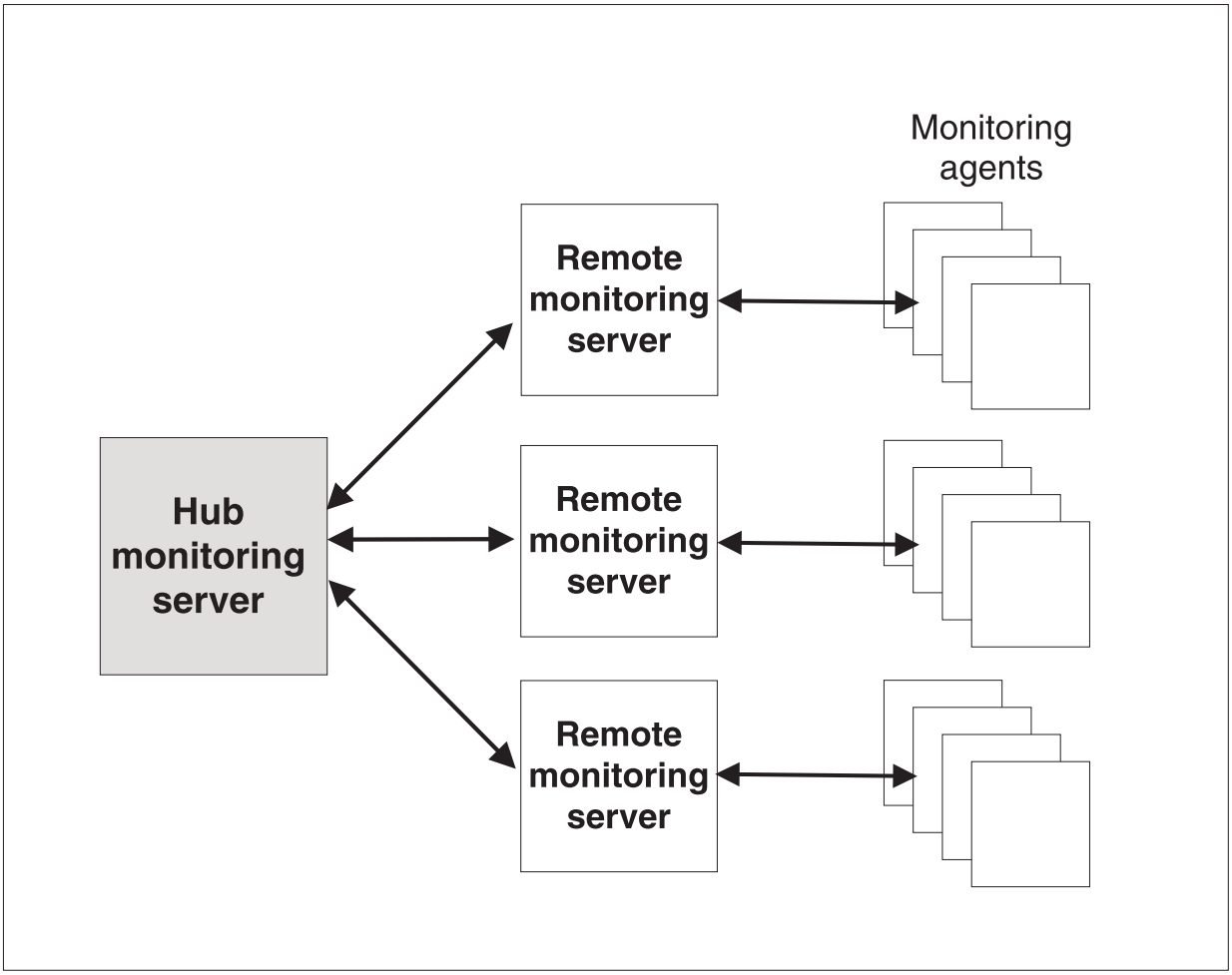


Figure 32. Hierarchy for the heartbeat interval

At the highest level, the hub monitoring server receives heartbeat requests from remote monitoring servers and from any monitoring agents that are configured to access the hub monitoring server directly (rather than through a remote monitoring server). The *default* heartbeat interval used by remote monitoring servers to communicate their status to the hub monitoring server is 3 minutes. The default heartbeat interval of 3 minutes for monitoring servers is suitable for most environments, and should not need to be changed. If you decide to modify this value, carefully monitor the system behavior before and after making the change.

At the next level, remote monitoring servers receive heartbeat requests from monitoring agents that are configured to access them. The *default* heartbeat interval used by monitoring agents to communicate their status to the monitoring server is 10 minutes.

You can specify the heartbeat interval for a node (either a remote monitoring server or a remote monitoring agent) by setting the CTIRA_HEARTBEAT environment variable. For example, specifying CTIRA_HEARTBEAT=5 sets the heartbeat interval to 5 minutes. The *minimum* heartbeat interval that can be configured is 1 minute.

- For monitoring servers on Windows computers, you can set this variable by adding the entry to the KBBENV file. You can access this file from Manage Tivoli Enterprise Monitoring Services by right-clicking **Windows OS Monitoring**

Agent and clicking **Advanced -> Edit ENV File**. Note that you must stop and restart the monitoring server for the changes to the KBBNV file to take effect.

- For monitoring servers on Linux and UNIX computers, you can set the CTIRA_HEARTBEAT variable by adding the entry to the monitoring server configuration file. The name of the monitoring server configuration file is of the form <*hostname*>_ms_<*temsname*>.config. For example, a remote monitoring server named `REMOTE_PPERF06` running on host `pperf06` has a configuration filename of `pperf06_ms_REMOTE_PPERF06.config`. Note that you must stop and restart the monitoring server for the configuration changes to take effect.
- For remote monitoring servers, you can set this variable by adding an entry to the KBBENV file. You can access this file from Manage Tivoli Monitoring Services by right-clicking **Tivoli Enterprise Monitoring Server** and clicking **Advanced → Edit ENV File**. You must stop and restart the monitoring server for changes to the KBBENV file to take effect.
- For Windows OS agents, you can set this variable by adding the entry to the KNTENV file. You can access this file from Manage Tivoli Monitoring Services by right-clicking **Windows OS Monitoring Agent** and clicking **Advanced → Edit ENV File**. You must stop and restart the monitoring agent for the changes to the KNTENV file to take effect.
- For agents on Linux and UNIX computers, you can set the CTIRA_HEARTBEAT variable by adding an entry to the agent .ini file (for example, lz.ini, ux.ini, ua.ini). When the agent is stopped and restarted, the agent configuration file is recreated using settings in the .ini file.

When a monitoring agent becomes active and sends an initial heartbeat request to the monitoring server, it communicates the desired heartbeat interval for the agent in the request. The monitoring server stores the time the heartbeat request was received and sets the expected time for the next heartbeat request based on the agent heartbeat interval. If no heartbeat interval was set at the agent, the default value is used.

Changes to offline status typically require two missed heartbeat requests for the status to change. Offline status is indicated by the node being ″grayed out″ in the portal client Navigator View. If the heartbeat interval is set to 10 minutes, an offline status change would be expected to take between 10 and 20 minutes before it is reflected on the portal client Navigator View.

Attention: Lower heartbeat intervals increase CPU utilization on the monitoring servers processing the heartbeat requests. CPU utilization is also affected by the number of agents being monitored. A low heartbeat interval and a high number of monitored agents could cause the CPU untilization on the monitoring server to increase to the point that performance related problems occur. If you reduce the heartbeat interval, you must monitor the resource usage on your servers. A heartbeat interval lower than 3 minutes is not supported.

Chapter 9. Additional Linux and UNIX configuration

The following sections provide information about additional configuration that may be required for Linux and UNIX systems:

- "Disabling fsync() calls"
- "Configuring permissions for a monitoring server on a non-NIS Solaris"
- "Increasing virtual memory on AIX for large environments"

Disabling fsync() calls

The KGLCB_FSYNC_ENABLED parameter was introduced in V6.2 for the Tivoli Enterprise Monitoring Server on UNIX and Linux operating systems. This variable can be used to specify whether the **fsync()** system call should be invoked after writes to the filesystem. This configuration variable may be set in the standard configuration file for the monitoring server.

For maximum reliability, by default **fsync()** is called. The **fsync()** system call flushes the filesystem's dirty pages to disk and protects against loss of data in the event of an operating system crash, hardware crash, or power failure. However, the call can have a significant negative effect on performance, because in many cases it defeats the caching mechanisms of the platform filesystem. On many UNIX platforms, the operating system itself syncs the entire filesystem on a regular basis. For example, by default the **syncd** daemon that runs on AIX syncs the filesystem every 60 seconds, which limits the benefit of **fsync()** calls by application programs to protecting against database corruption in the most recent 60-second window.

If the following line is added to the monitoring server configuration file, **fsync()** calls are omitted:

```
KGLCB_FSYNC_ENABLED='0'
```

Configuring permissions for a monitoring server on a non-NIS Solaris

If your monitoring server is installed on a non-NIS Solaris computer, you must set the permissions. You do not need to do this for monitoring servers running on AIX or Linux.

Set permissions for a monitoring server on a non-NIS Solaris system as follows:

1. Go to the /bin directory where kdsvlunx is located. (*install_dir*/*arch*/ms/bin, where arch is the operating system on which the monitoring was installed).
2. Change the su to ″root″ if you have the root password, otherwise obtain the password from an administrator:

   ```
   chown root kdsvlunx
   chmod u+s kdsvlunx
   ```

3. Return to your regular ID after you have changed the su to ″root.″

Increasing virtual memory on AIX for large environments

The Tivoli Enterprise Portal Server process (KfwServices) is linked with the default memory model, which allows for data and stack of only 256 MB. In large environments, this can cause the portal server to crash at startup. In smaller environments, this may not cause a problem at startup, but may at some later

© Copyright IBM Corp. 2005, 2007

point as more virtual storage is required. The problem can be predicted if the **topas** command shows KfwServices with PgSp value of 180-250 MB. If a smaller environment is close to that value, it may occur when large queries are being handled. If the **topas** output shows that KfwServices is nearing these values, the memory model should be changed in smaller environments as well as large ones.

Changing the memory model requires that KfwServices load header be modified. Also, changes must be made to DB2 configuration changes. Complete the following steps to make these changes. These steps use the default directory. Use the directory locations appropriate to your system.

Important:: You must run the **ldedit** command below each time new Tivoli Enterprise Portal Server maintenance has been applied.

To make the required memory model and DB2 configuration changes:

1. Stop the Tivoli Enterprise Portal Server:
   ```
   cd /opt/IBM/ITM/bin ./itmcmd agent stop cq
   ```
2. Issue the following commands:
   ```
   cd /opt/IBM/ITM/aix533/cq/bin
   cp KfwServices KfwServices.orig
    /usr/ccs/bin/ldedit -bmaxdata:0x80000000 KfwServices
   ```
3. To verify that the maxdata value has been set issue the following command:
   ```
   dump -ov KfwServices
   ```
   This will display the maxdata value in KfwServices. Maxdata should show as:
   ```
   maxSTACK maxDATA SNbss magic modtype 0x00000000 0x80000000 0x0003 0x010b 1L
   ```
4. Issue the following command:
   ```
   cd /opt/IBM/ITM/config
   ```
5. Using your preferred editor add the following line to cq.ini:
   ```
   EXTSHM=ON
   ```
6. Using the db2 installation user ID (the default is db2inst1), make the DB2 configuration changes as follows:
   a. Stop the DB2 server if not already stopped:
      ```
      cd /db2inst1/sqllib/adm db2stop
      ```
   b. Issue the following configuration changes:
      ```
      export EXTSHM=ON
      db2set DB2ENVLIST=EXTSHM
      db2set -all
      ```
   c. Using your preferred editor add the following lines to /db2inst1/sqllib/db2profile:
      ```
      EXTSHM=ON
      export EXTSHM
      ```
   d. Restart DB2:
      ```
      cd /db2inst1/sqllib/adm db2start
      ```
7. Restart the TEPS:
   ```
   cd /opt/IBM/ITM/bin ./itmcmd agent start cq
   ```

For more information about using the large and very large address-space models to accommodate programs requiring data areas that are larger than those provided by the default address-space model, see http://publib.boulder.ibm.com/infocenter/pseries/v5r3/index.jsp?topic=/com.ibm.aix.genprogc/doc/genprogc/lrg_prg_support.htm. For more information about using the EXTSHM environment

variable to increate the number of share memory segments to which a single process can be attached, see http://publib.boulder.ibm.com/infocenter/db2luw/v8/index.jsp?topic.

Chapter 10. Additional Tivoli Enterprise Portal configuration

This chapter discusses how to perform the following advanced configuration of Tivoli Enterprise Portal components:

- "Using SSL between the portal server and the client"
- "Configuring an external Web server to work with Tivoli Enterprise Portal" on page 243
- "Configuring a portal client connection to an external Web server" on page 246
- "Firewall network address translation (NAT) or multiple network interface cards" on page 247
- "Firewall scenarios for Tivoli Enterprise Portal" on page 249

It also includes illustrations of firewall scenarios that can help in defining the Tivoli Enterprise Portal Server interface.

Using SSL between the portal server and the client

You can choose to encrypt all communication between the portal server and portal client. IBM Tivoli Monitoring uses two protocols to provide this level of security between portal server and client server:

- Secure Hypertext Transport Protocol (HTTPS) to retrieve files and Interoperable Object Reference (IOR). The integrated browser in the client provides HTTPS support on the client side; for the server, consider using a third party web server that supports HTTPS, such as the IBM HTTP Server. See "Configuring an external Web server to work with Tivoli Enterprise Portal" on page 243 for more information.
- Internet Inter-ORB Protocol (IIOP) to secure the communications between the portal server and client. This uses Secure Socket Layer (SSL) provided by VisiBroker. This secure communication uses public key cryptography.

When you install IBM Tivoli Monitoring, the Global Security Toolkit (GSKit) and iKeyman utilities are installed by default on all components. These utilities are used to create and manage the encryption of data between components through the use of digital certificates.

Digital certificates are the vehicle that SSL uses for public-key cryptography. Public-key cryptography uses two different cryptographic keys: a private key and a public key. Public-key cryptography is also known as *asymmetric cryptography*, because you can encrypt information with one key and decrypt it with the complement key from a given public-private key pair.

Public-private key pairs are simply long strings of data that act as keys to a user's encryption scheme. The user keeps the private key in a secure place (for example, encrypted on a computer's hard drive) and provides the public key to anyone with whom the user wants to communicate. The private key is used to digitally sign all secure communications sent from the user; the public key is used by the recipient to verify the sender's signature.

Public-private key pairs are validated by a trusted third party, called a Certificate Authority (CA). An example of a CA is Verisign. If you are setting up your own key pairs, you submit them to the CA for validation.

© Copyright IBM Corp. 2005, 2007

You can configure your portal server and client are configured to use asymmetric cryptography, using the default keys provided with IBM Tivoli Monitoring. See "Setting up asymmetric encryption" for information about setting up this encryption.

For additional information about using public-private key pairs, see the iKeyman documentation available at http://www-1.ibm.com/support/docview.wss?uid=pub1sc32136300.

Enabling and disabling SSL for the Tivoli Enterprise Portal Server

IBM Tivoli Monitoring is shipped with SSL disabled as the default.

If you want to use Secure Socket Layer communication between the portal server and the portal client, use the following steps to enable it:

Note: This procedure disables the primary interface. For instructions on disabling additional interfaces, see Chapter 10, "Additional Tivoli Enterprise Portal configuration," on page 239.

On a Windows system:

1. In the Manage Tivoli Enterprise Monitoring Services window, right-click **Tivoli Enterprise Portal Server**.
2. Click **Advanced → Configure TEPS Interfaces**.
3. Highlight **cnps** and click **Edit** in the TEPS Interface Definitions window.
4. Select **Enable SSL for TEP Clients**.
5. Click **OK** to save your changes and close the window.
6. Recycle the service by stopping and starting it.

On a Linux system:

1. Change to the *install_dir*/bin directory
2. Run the following command:
   ```
   ./itmcmd manage
   ```
3. In the Manage Tivoli Monitoring Services window, right-click **Tivoli Enterprise Portal Server**.
4. Click **Configure**
5. In the first tab, select **Enable SSL for TEP Clients** to enable SSL in the Tivoli Enterprise Portal Server window.
6. Click **OK** to save your changes and close the window.
7. Recycle the service by stopping and starting it.

Setting up asymmetric encryption

Setting up asymmetric encryption through the use of public-private key files requires the following steps:

Table 64. Setting up asymmetric encryption

Goal	Where to find information
Create a new key database.	"Creating a new key database" on page 241

Table 64. Setting up asymmetric encryption (continued)

Goal	Where to find information
Create a request for a new public-private key pair and send that request to a trusted Certificate Authority.	"Creating a new public-private key pair and certificate request"
Optionally use a temporary, self-signed key pair while you wait for your CA-signed certificate.	"Using a temporary self-signed certificate" on page 242
Add the CA-signed digital certificate to your key database.	"Receiving the CA-signed certificate" on page 242
Enable components to access the certificate by saving the key database password to a stash file on your computer.	"Save the password to a stash file" on page 243

Important: If you do not use the recommended names for the key database, stash file, and certificate label as described below, you must change the following environment variables in the KFWSERVICES file on the portal server:

- KDEBE_KEYRING_FILE=C:\IBM\ITM\keyfiles\keyfile.kdb
- KDEBE_KEYRING_STASH=C:\IBM\ITM\keyfiles\keyfile.sth
- KDEBE_KEY_LABEL=IBM_Tivoli_Monitoring_Certificate

Creating a new key database

Use the following steps to create a new key database:

1. Start iKeyman:
   - On Windows, double-click the gsk7ikm.exe file, located in the c:\Program Files\IBM\gsk7\bin directory.
   - On UNIX, change to the GSKit directory and run one of the following commands:

     For 32-bit operating systems, run **gsk7ikm**.

     For 64-bit operating systems, run **gsk7ikm_64**.
2. Click **Key Database File → New**.
3. Select **CMS** in the **Key database type** field.
4. Type `keyfile.kdb` in the **File Name** field.
5. Type the following location in the **Location field**: `<itm_installdir>/keyfiles`.
6. Click **OK**. The Password Prompt window is displayed.
7. Enter a password in the **Password** field, and confirm it again in the **Confirm Password** field. Click **OK**.
8. A confirmation window is displayed. Click **OK**.

The IBM Key Management window is displayed. This window reflects the new CMS key database file and your signer digital certificates.

Creating a new public-private key pair and certificate request

Use the following steps to create a new public-private key pair and certificate request:

1. Start iKeyman.
2. Click **Key Database File → Open**.
3. Select the keyfile.kdb key database and click **Open**.
4. Type the password for the key database and click **OK**.

5. Select **Personal Certificate Requests** from the pull-down list and click **New**.
6. Click **New**.
7. Type `IBM_Tivoli_Monitoring_Certificate` in the **Key Label** field.
8. Type a **Common Name** and **Organization**, and select a **Country**. For the remaining fields, either accept the default values, or type or select new values.
9. At the bottom of the window, type a name for the file.
10. Click **OK**. A confirmation window is displayed, verifying that you have created a request for a new digital certificate.
11. Click **OK**.

The IBM Key Management window is displayed.

Send the file to a CA to request a new digital certificate, or cut and paste the request into the request forms on the CA's Web site.

Using a temporary self-signed certificate

It can take between two and three weeks to receive a CA-signed digital certificate. If you want to use a digital certificate other than the one provided with IBM Tivoli Monitoring and you have not yet received the CA-signed digital certificate, you can create a self-signed certificate on the portal server. A self-signed digital certificate is not as secure as a CA-signed certificate; this is strictly a temporary measure until the CA-signed certificate arrives.

Creating and using a self-signed certificate involves the following steps:

1. Create a CA key database.
2. Create the self-signed certificate.
3. Export the self-signed certificate.
4. Receive the self-signed certificate into the key databases on the portal server.

When you receive the CA-signed certificate, you need to delete the self-signed certificate.

For information on all of these steps, see the iKeyman documentation available at http://www-1.ibm.com/support/docview.wss?uid=pub1sc32136300.

Receiving the CA-signed certificate

After the CA returns your new digital certificate, save it on the computer where the portal server is running. Repeat for the client. If the CA returns the certificate as part of an e-mail message, copy and paste it from the e-mail into a text file.

Use the following steps to receive the digital certificate from the CA into key database on each computer.

1. Start iKeyman.
2. Click **Key Database File → Open**.
3. Select the keyfile.kdb database and click **Open**.
4. Type the password for the database and click **OK**.
5. Select **Personal Certificates** from the pull-down list.
6. Click **Receive**.
7. Click **Data type** and select the data type of the new digital certificate, such as **Base64-encoded ASCII data**.
8. Type `keyfile.sth` for the **Certificate file name** and `<itm_installdir>/keyfiles` as the **Location** for the new digital certificate.

9. Click **OK**.
10. Type `IBM_Tivoli_Monitoring_Certificate` for the new digital certificate and click **OK**.

Save the password to a stash file

Because many of the IBM Tivoli Monitoring components work without user intervention, you need to save the key database password to a stash file on your computer. This enables the components to use SSL without requiring any intervention from you. Use the following steps to save the password to a stash file:

1. Start iKeyman.
2. Select **Key Database File → Stash File**.

   An information window is displayed telling you that the password was saved to a stash file.
3. Click **OK**.

Disabling SSL

If you do not want to use Secure Socket Layer communication between IBM Tivoli Monitoring components and the Tivoli Enterprise Portal Server, use the following steps to disable it:

Note: Each interface independently enables or disables SSL. If you are using multiple interfaces, you must disable all of them.

1. In Manage Tivoli Monitoring Services, right-click **Tivoli Enterprise Portal Server**.
2. Click **Advanced → Edit ENV file**.
3. Find the following line:

   ```
   kfw_interface_cnps_ssl=Y
   ```
4. Change the `Y` to `N`.
5. Save the file and exit.
6. Click **Yes** when you are asked if you want to recycle the service.

Configuring an external Web server to work with Tivoli Enterprise Portal

If you want to use an external Web server to view the Tivoli Enterprise Portal, you need to configure that Web server. The following sections provide configuration information for Microsoft Internet Information Server versions 5.0 and 6.0.

- "Configuring Internet Information Server V5.0"
- "Configuring Internet Information Server V6.0" on page 244
- "Configuring IBM HTTP Server on Linux" on page 245

Configuring Internet Information Server V5.0

Use the following steps to configure Internet Information Server V5.0 to work as a Tivoli Enterprise Portal browser client.

1. Start the Internet Services Manager.
2. Right click the WWW service (the system host name).
3. Select **Master Properties** and click **Edit**.
4. Click the **Directory Security** tab.
5. Click **Edit**.

6. Ensure that **Anonymous access** and **Integrated Windows authentication** are selected and click **OK**.
7. Click the **Documents** tab.
8. Click **Add**.
9. Type `index.html` in the **Default Document Name** field.
10. Click **OK** and then click **OK** to close the Master Properties notebook.

Use the following steps to set up the Web site:

1. From the Internet Services Manager, right-click the WWW service.
2. Click **New → Web Site**.
3. Click **Next**.
4. Type a description for the Web site (for example, ″ITM″).

   Note: Refer to the documentation for Internet Information Server before changing any of the default values in the next steps.
5. If you have multiple IP addresses, select the one that is appropriate for this site.
6. If you want to use a separate port of this site, type the port number in the **TCP Port** field.
7. Type the path to the Tivoli Enterprise Portal browser client. The default path is C:\IBM\ITM\CNB.
8. Ensure that **Read** and **Run Scripts** are selected. Do *not* select **Execute**.
9. Click **Next** and then click **Finish**.

If the site does not start automatically, right-click it and click **Start**.

Configuring Internet Information Server V6.0

Use the following steps to configure Internet Information Server V6.0 on Windows 2003 to work as a Tivoli Enterprise Portal browser client:

1. Start IIS Manager.
2. Right-click **Web Sites** and click **New → Web Site**.
3. Click **Next**.
4. Type the name of a Web site (for example ″Tivoli″) and click **Next**.
5. Type the IP address for the Tivoli Enterprise Portal Server computer (this should be the same computer where IIS 6.0 is running) and click **Next**.
6. Type the path to the IBM Tivoli Monitoring home directory that is the root of the Web Content subdirectories. The default path is C:\IBM\ITM\CNB. Click **Next**.
7. Select **Read**, **Run scripts**, and **Execute**. Click **Next**.
8. Click **Finish**.
9. Right-click the new Web site and click **Properties**.
10. Click the **Documents** tab.
11. In the **Add Content Page** field, type `index.html`. This is the main page for the Tivoli Enterprise Portal.
12. Click the **Move Up** button to move **index.html** to the top of the list.
13. Click the **HTTP Headers** tab.
14. Click **MIME Types**.
15. Click **New** next to **MIME Types**.
16. Type `*.asp` in the **Extension** field.

17. Type `application/x-asp` in the **MIME Type** field.
18. Click **OK**.
19. Repeat Steps 15 on page 244 to 18 for each of the following:

Extension	MIME Type
.class	application/java-class
.ior	application/octet-stream
.jar	application/java-archive
.jks	application/octet-stream
.jnlp	application/x-java-jnlp-file
.js	application/x-javascript
.llser	application/octet-stream
.pl	application/x-perl
.ser	application/java-serialized-object
.txt	text/plain
.zip	application/zip

20. Click **OK**.
21. Click **Apply**.
22. Click **OK**.

Configuring IBM HTTP Server on Linux

Use the following steps to configure IBM HTTP Server to work on a Linux computer:

1. Install IBM HTTP Server with the default settings. See the product documentation (www-306.ibm.com/software/webservers/httpservers/library) for additional information.
2. Open the *IHS_install_dir*/conf/httpd.conf file in a text editor. The default installation directory is /opt/IBMIHS.
3. Find the line that begins with `DocumentRoot`. Change the value (between the double quotation marks [`""`]) to *`itm_installdir`*`/`*`linux_dir`*`/cw`, where *itm_installdir* is the directory where IBM Tivoli Monitoring is installed and *linux_dir* is li6243 (Red Hat systems), li6263 (SLES9 for Intel systems) or li3263 (SLES9 for z/Series systems). For example:

   ```
   DocumentRoot "/data/candle/li6243/cw"
   ```

4. Find the line that begins with `<Directory>/opt`. Change the path to the value used for DocumentRoot. (From our previous example, it would be *itm_installdir*/li6243/cw).
5. Save and close the file.
6. Open the *IHS_install_dir*/conf/mime.types file in a text editor.
7. Add the following lines:

   ```
   application/java-archive     jar
   application/java-serialized-object     ser
   image/icon     ico
   ```

8. Modify the line that begins with `application/octet-stream` to include `cab ior jks llrser jbf jnlp vbs` at the end. For example:

   ```
   application/octet-stream bin dms lha lzh exe class so dll cab ior jks llrser
   jbf jnlp vbs
   ```

9. Modify the line that beings with `text/plain` to include `bat ini inf ivl log lng lvl mf properties` at the end. For example:

   ```
   text/plain     asc txt bat ini inf ivl log lng lvl mf properties
   ```

10. Save and close the file.
11. Stop the IBM HTTP Server services, then start it again to enable the configuration changes.

Configuring a portal client connection to an external Web server

Use the following sections to configure your portal client to work with an external Web server:

- "Browser client"
- "Desktop client"

Browser client

During installation, the IBM Tivoli integral Web server is installed as a component of the Tivoli Enterprise Portal Server. You can also use an external Web server on your Tivoli Enterprise Portal Server computer, as shown in "Firewall scenarios for Tivoli Enterprise Portal" on page 249.

Currently, IBM supports an external Web server for browser client access only when installed on the same computer as the Tivoli Enterprise Portal Server.

Desktop client

Although the desktop client does not need a Web server to start Tivoli Enterprise Portal, it does use it for common files stored on the Tivoli Enterprise Portal Server, such as the graphic view icons and style sheets. If your Tivoli Enterprise Portal Server setup disables the integral Web server and uses only an external Web server, you need to specify the Interoperable Object Reference (IOR) for every desktop client.

Updating the IOR for Windows

Use the following steps to specify the IOR for the desktop client:

1. On the computer where Tivoli Enterprise Portal desktop client is installed, open Manage Tivoli Monitoring Services
2. Right-click **Tivoli Enterprise Portal – Desktop** and click **Reconfigure**.
3. Double-click **cnp.http.url.DataBus** in the parameters list. The Edit Tivoli Enterprise Portal Parm window is displayed.
4. In the **Value** field, type the Web server address where the cnps.ior can be found. For example, if the Web server name is xyz.myserver.com and the document root for the Web server is \ibm\itm\cnb, the value is http://xyz.myserver.com/cnps.ior.
5. Select **In Use** and click **OK**.
6. Click **OK** to close the window.

Updating the IOR for Linux

Use the following steps to specify the IOR for the desktop client:

1. On the computer where the Tivoli Enterprise Portal desktop client is installed, go to the *install_dir*/bin directory and edit the cnp.sh shell script.
2. Add the following parameter to the last line of the file specifying the Web server address where the cnps.ior can be found for the value. For example, if

the Web server name is xyz.myserver.com and the document root for the Web server is /candle/cnb, the value is http://xyz.myserver.com/cnps.ior.

```
-Dcnp.http.url.DataBus=http://xyz.myserver.com/cnps.ior
```

Note: The last line of cnp.sh is very long and has various options on it, including several other -D options to define other properties. It is very important to add the option in the correct place.

If the last line of your bin/cnp.sh originally looked like this:

```
${JAVA_HOME}/bin/java -showversion -noverify -classpath ${CLASSPATH}
-Dkjr.trace.mode=LOCAL -Dkjr.trace.file=/opt/IBM/ITM/logs/kcjras1.log
-Dkjr.trace.params=ERROR -DORBtcpNoDelay=true -Dcnp.http.url.host=
-Dvbroker.agent.enableLocator=false
-Dhttp.proxyHost=
-Dhttp.proxyPort=candle.fw.pres.CMWApplet 2>& 1 >> ${LOGFILENAME}.log
```

To specify the IOR, change the line to look like the following:

```
${JAVA_HOME}/bin/java -showversion -noverify -classpath ${CLASSPATH}
-Dcnp.http.url.DataBus=http://xyz.myserver.com/cnps.ior
-Dkjr.trace.mode=LOCAL -Dkjr.trace.file=/opt/IBM/ITM/logs/kcjras1.log
-Dkjr.trace.params=ERROR -DORBtcpNoDelay=true -Dcnp.http.url.host=
-Dvbroker.agent.enableLocator=false
-Dhttp.proxyHost=
-Dhttp.proxyPort=candle.fw.pres.CMWApplet 2>& 1 >> ${LOGFILENAME}.log
```

Firewall network address translation (NAT) or multiple network interface cards

The URL for starting Tivoli Enterprise Portal in browser mode includes the Tivoli Enterprise Portal Server host name or IP address. The address for starting Tivoli Enterprise Portal is set for the desktop client during installation or through Manage Tivoli Monitoring Services. If any of the following is true in your configuration, you need to define a Tivoli Enterprise Portal Server interface:

- A firewall with Network Address Translation (NAT) is used between the client and the Tivoli Enterprise Portal Server.
- The host of the Tivoli Enterprise Portal Server has more than one Network Interface Card (NIC).

On Windows you define an interface using Manage Tivoli Monitoring Services. On Linux and AIX, you edit the `lnxenv` file manually.

Defining a Tivoli Enterprise Portal Server interface on Windows

Use the following steps to define a Tivoli Enterprise Portal Server interface on Windows:

1. On the computer where the Tivoli Enterprise Portal Server is installed, click **Start → Programs → IBM Tivoli Monitoring → Manage Tivoli Monitoring Services**.
2. Right-click **Tivoli Enterprise Portal Server**.
3. Click **Advanced → Configure TEPS Interfaces**.

   Initially, the list has one definition named "cnps," using port 15001 for the Tivoli Enterprise Portal Server and the IBM Tivoli integrated Web server at http://*mysystem*:1920///cnp/client (where the variable *mysystem* is the host name). Port 80, for an external Web server, is assumed if the URL does not specify 1920 for the integrated Web server.

Note: If IIS is being used as the external Web server for Tivoli Enterprise Portal over a firewall, you may experience performance problems like slow download times. Socket pooling may also cause problems under certain conditions. If you encounter problems, try using a port other than the default port 80 on the IIS server.

4. Click **Add**.
5. Define the interface. Complete the following fields:

   Interface Name
   Type a one-word title for the interface.

   Host If you are defining an interface for a specific NIC or different IP address on this computer, type the TCP/IP host address. Otherwise, leave this field blank.

   Proxy Host
   If you are using address translation (NAT), type the TCP/IP address used outside the firewall. This is the NATed address.

   Port Type a new port number for the Tivoli Enterprise Portal Server. The default 15001 is for the server host address, so a second host IP address or a NATed address requires a different port number.

   Proxy Port
   If the port outside the firewall will be translated to something different than what is specified for **Port**, set that value here.

   Enable SSL for TEP clients
   Enable secure communications between clients and the portal server.
6. Click **OK** to add the new Tivoli Enterprise Portal Server interface definition to the list.

Defining a Tivoli Enterprise Portal Server interface on Linux or UNIX

To define an additional Tivoli Enterprise Portal interface on Linux or UNIX, edit the <install_dir>/<platform_dir>/cq/bin/lnxenv file as follows:

1. Locate the KFW_INTERFACES= variable and add the one-word name of the new interface, separating it from the preceding name by a space. For example:

   ```
   KFW_INTERFACES=cnps myinterface
   ```
2. Following the entries for the default cnps interface, add the following variables as needed, specifying the appropriate values:

   KFW_INTERFACE_<interface_name>_HOST=
   If you are defining an interface for a specific NIC or different IP address on this computer, specify the TCP/IP host address.

   KFW_INTERFACE_<interface_name>_PORT=
   Type a port number for the Tivoli Enterprise Portal Server. The default 15001 is for the server host address, so a second host IP address or a NATed address requires a different port number.

   KFW_INTERFACE_<interface_name>_PROXY_HOST=
   If you are using address translation (NAT), type the TCP/IP address used outside the firewall. This is the NATed address.

   KFW_INTERFACE_<interface_name>_PROXY_HOST=
   If the port outside the firewall will be translated to something different than what is specified for **Port**, set that value here.

KFW_INTERFACE_<interface_name>_SSL=Y
If you want clients to use Secure Socket Layers (SSL) to communicate with the Tivoli Enterprise Portal Server, add the following variable.

Firewall scenarios for Tivoli Enterprise Portal

The following diagrams illustrate several firewall scenarios using various combinations of the IBM Tivoli integral Web server, an external Web server (such as Apache or IBM HTTP Server), NAT, and a second NIC on the Tivoli Enterprise Portal Server computer. These scenarios can help you to define the Tivoli Enterprise Portal Server interface.

Note: You can download the IBM HTTP Server for free at http://www-306.ibm.com/software/webservers/httpservers/.

Figure 33 shows scenario with the following configuration:

- Has an intranet firewall
- Has no NAT
- Uses the integral Web server

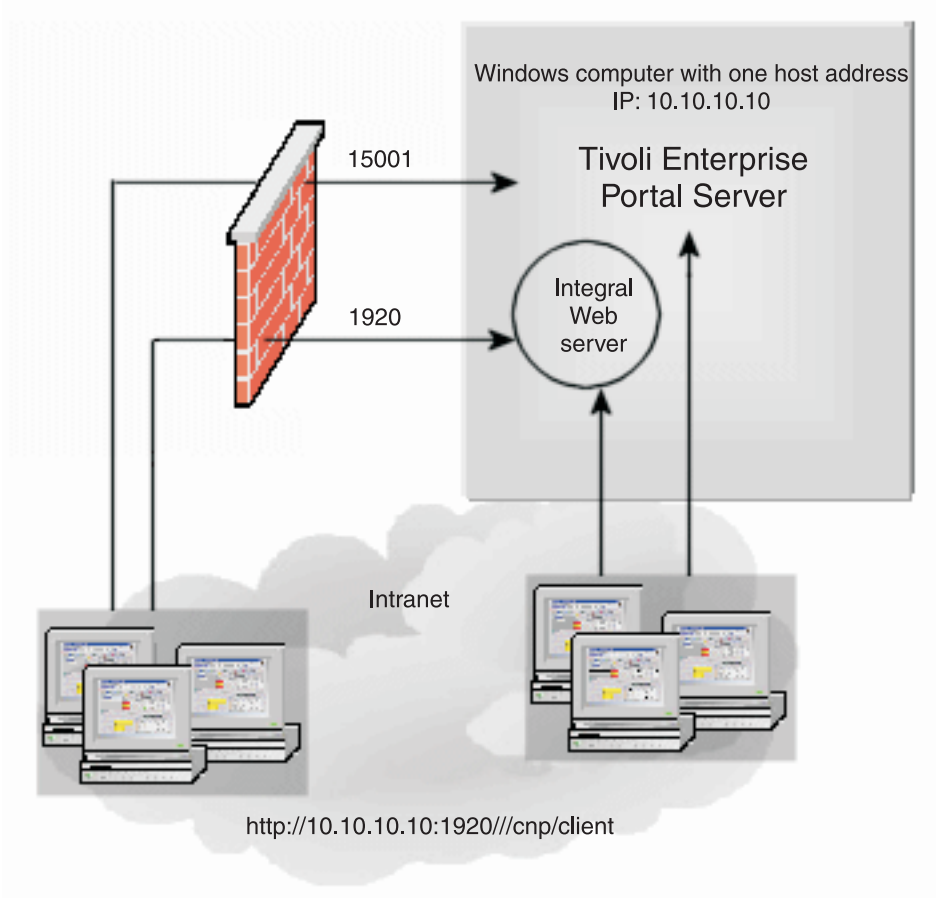


Figure 33. Intranet with integral Web server

The default Tivoli Enterprise Portal Server interface "cnps" is used. No additional interface definitions are needed. Browser mode users, whether going through the firewall or not, start Tivoli Enterprise Portal at:

```
http://10.10.10.10:1920///cnp/client
```

or substitute the host name for the IP address.

For configurations using the integrated Web server and these port numbers, use the default cnps interface definition.

In this scenario, the monitoring server and agents can be installed on the Tivoli Enterprise Portal Server computer.

Figure 34 shows a scenario that has the following configuration:

- Has an intranet firewall
- Has no NAT
- Uses an external Web server (such as IBM HTTP Server, Apache or IIS)

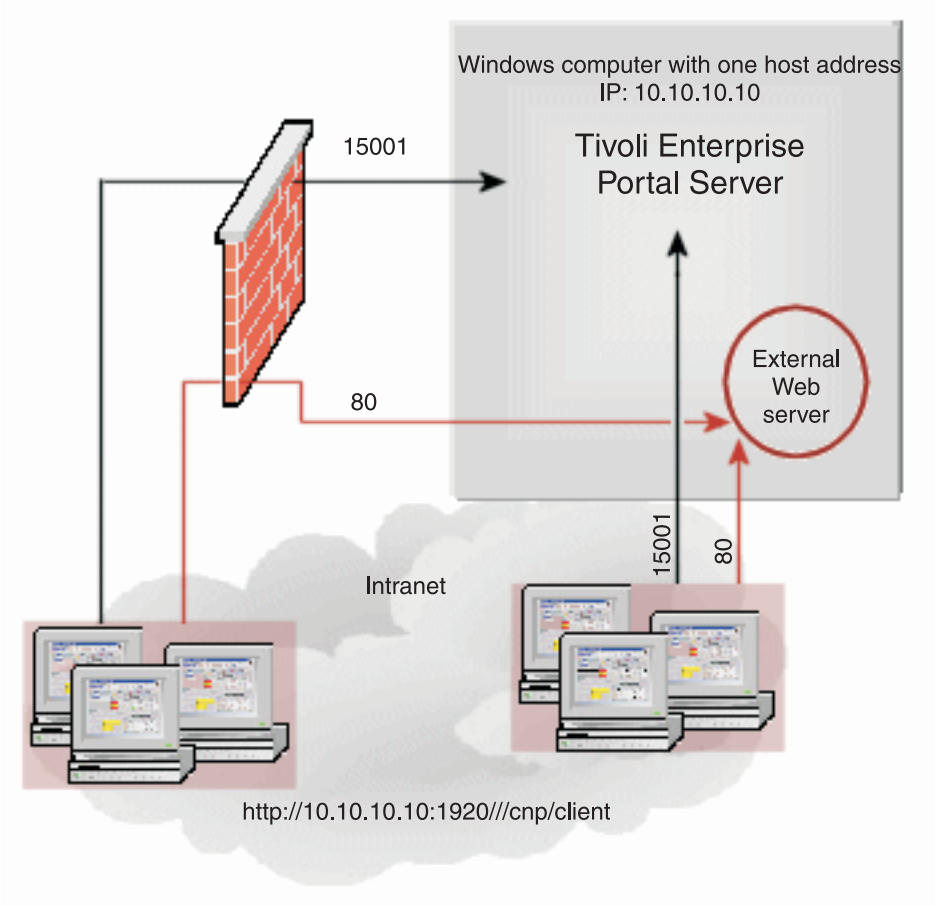


Figure 34. Intranet with external Web server

Browser mode users, whether going through the firewall or not, start Tivoli Enterprise Portal Server with

```
http://10.10.10.10 or http://10.10.10.10/mydirectory
```

(where mydirectory is the alias), or substitute the host name for the IP address.

For intranet configurations using an external Web server, with no NAT, you do not need to add a new interface definition. Web server port 80 is used automatically when none is specified in the URL.

In this scenario, the monitoring server and agents can be installed on the Tivoli Enterprise Portal Server computer.

Figure 35 shows the following two-part configuration:

- Intranet firewall without NAT and using the integral Web server
- Internet firewall with NAT and using an external Web server

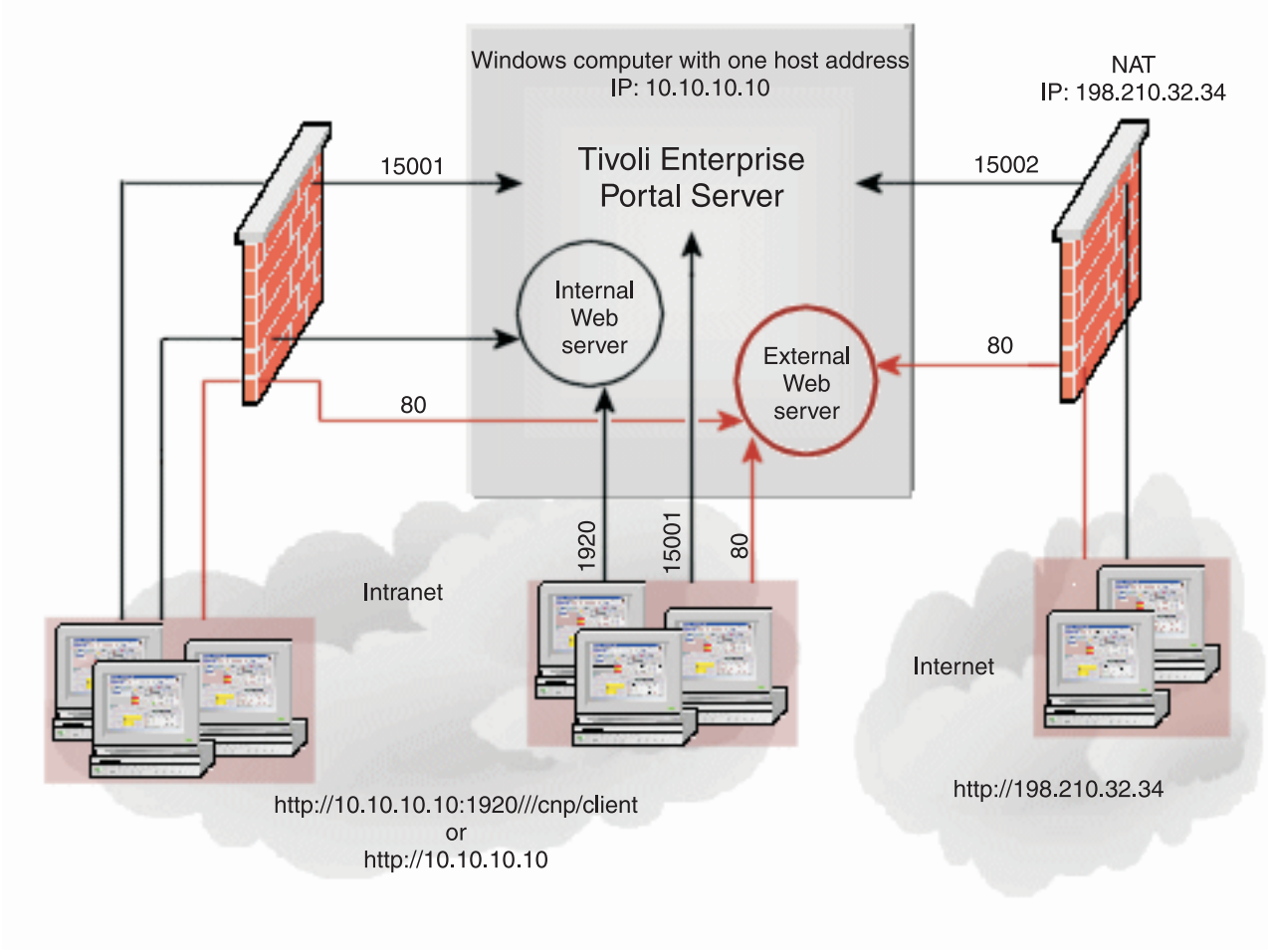


Figure 35. Intranet with integral Web server; Internet with external Web server

Intranet users can enter the URL for either the integral Web server or the external Web server:

```
http//10.10.10.10:1920///cnp/client or http://10.10.10.10
```

Internet users enter the URL for the NATed address:

```
http://198.210.32.34/?ior=internet.ior
```

(or substitute the host name for the IP address).

The Internet configuration requires a new Tivoli Enterprise Portal Server interface named "internet", with proxy host address 198.210.32.34 and port number 15002. The intranet firewall uses the "cnps" definition.

In this scenario, the monitoring server and agents cannot be installed on the Tivoli Enterprise Portal Server computer.

Figure 36 shows the following three-part configuration:

- Intranet firewall with NAT through the firewall to the external Web server
  `http://192.168.1.100/?ior=intranet.ior`
- Without NAT inside the DMZ to the integral Web server
  `http://10.10.10.10:1920///cnp/client`
- Internet firewall with NAT through the firewall to the external Web server
  `http://198.210.32.34/?ior=internet.ior`

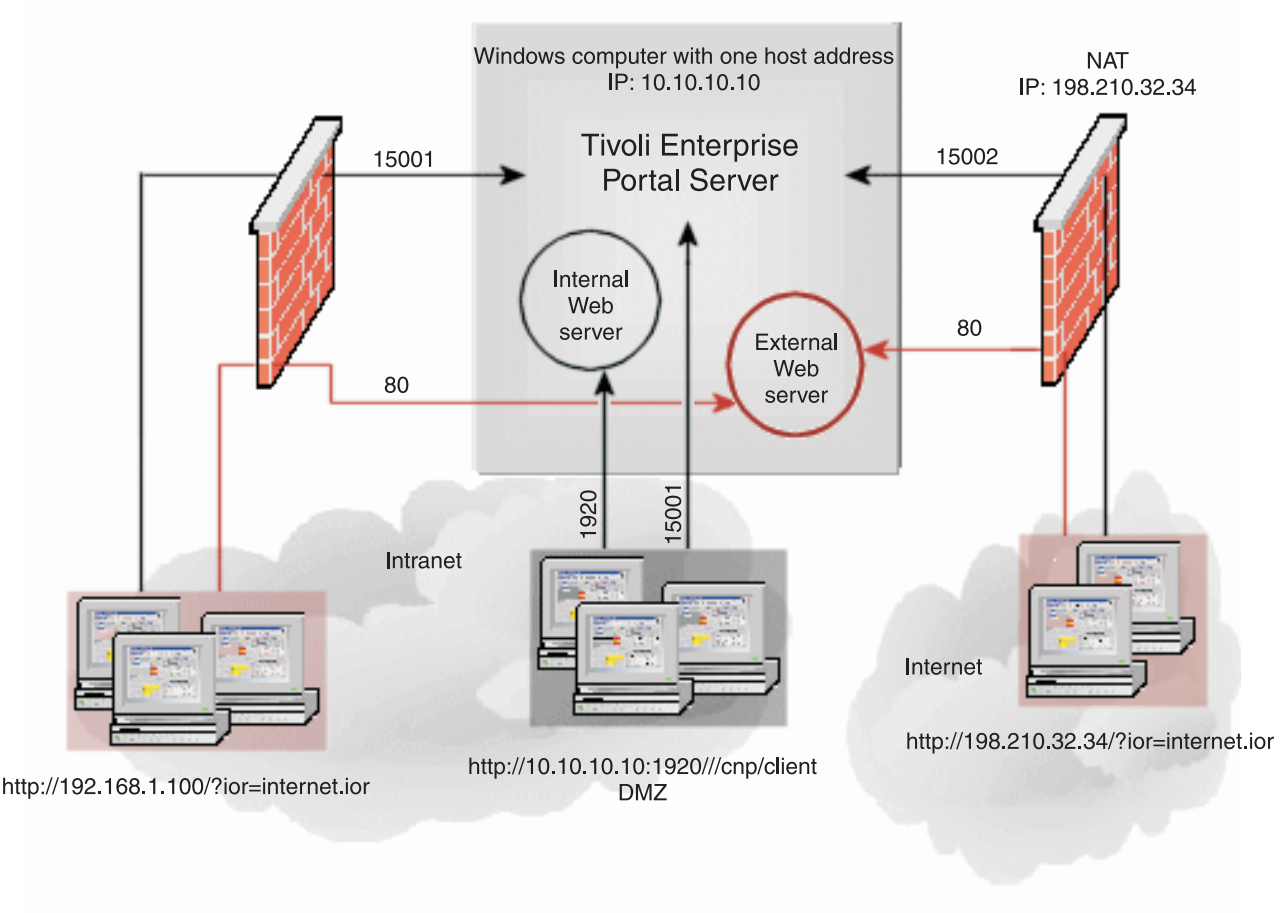


Figure 36. Intranet and Internet with integral and external Web servers

The intranet firewall configuration requires a new Tivoli Enterprise Portal Server interface named "intranet", which uses proxy host 192.168.1.100 and port 15003.

The Internet DMZ configuration requires a new Tivoli Enterprise Portal Server interface definition.

The Internet configuration uses the same Tivoli Enterprise Portal Server ″internet″ interface definition as the previous scenario: proxy host 198.210.32.34 and port 15002.

In this scenario, the monitoring server and agents cannot be installed on the Tivoli Enterprise Portal Server computer.

Figure 37 shows the following two-part configuration:

- Intranet firewall with NAT through the firewall to the external Web server using http://192.168.1.100, and without NAT inside the DMZ to the integral Web server uses http://10.10.10.10:1920///cnp/client
- Internet firewall with NAT through the firewall to the external Web server using http://198.210.32.34.

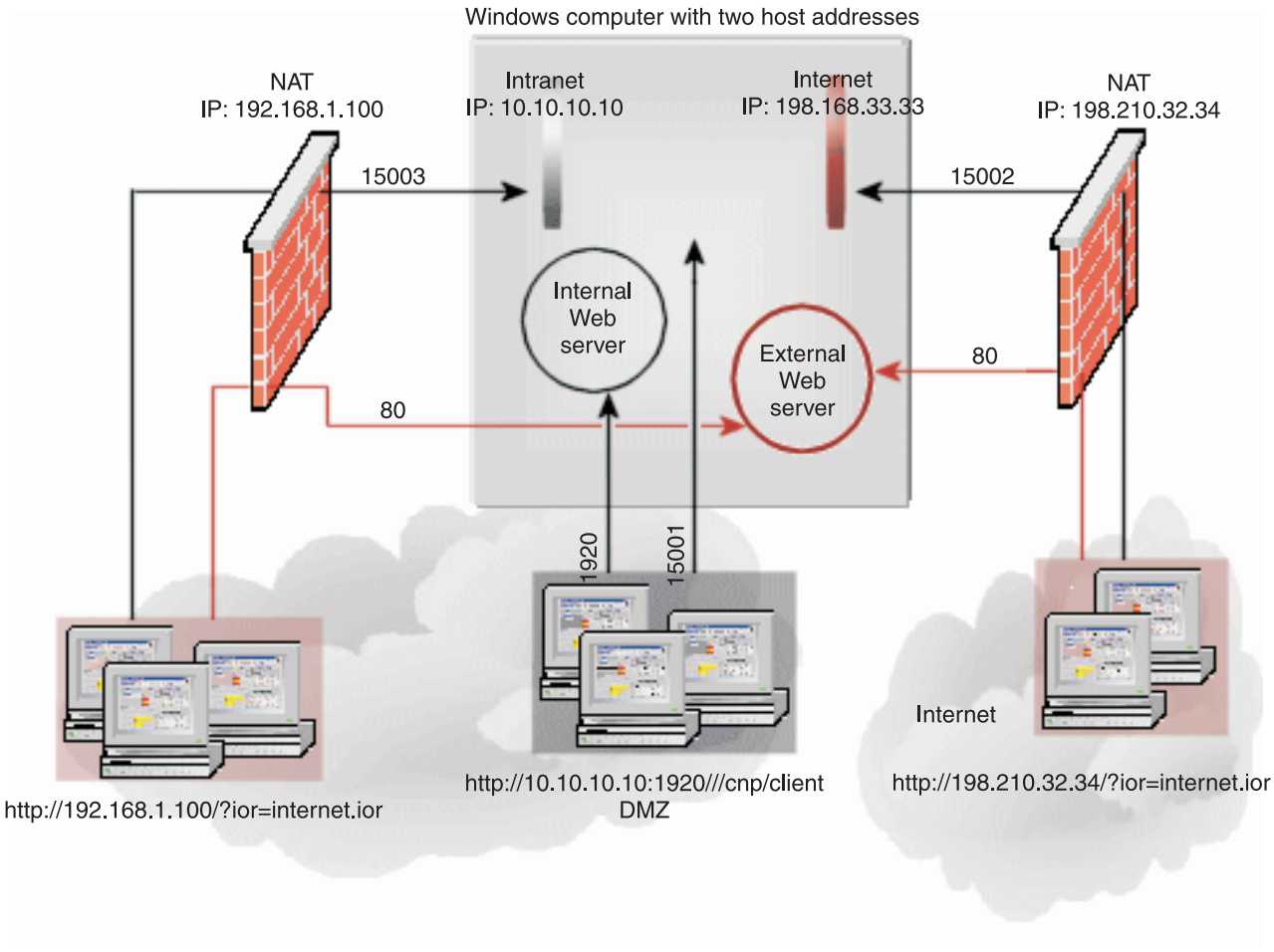


Figure 37. Two host addresses, intranet and Internet, with integral and external Web servers

The intranet firewall configuration uses the same Tivoli Enterprise Portal Server interface definition (named ″intranet″) as in the scenario shown in Figure 36 on page 252: http://10.10.10.10; proxy host 192.168.1.100; and port 15003.

The intranet DMZ configuration uses the default Tivoli Enterprise Portal Server interface definition: host 192.168.33.33; proxy host 198.210.32.34; port 15002; and proxy port 444.

In this scenario, the monitoring server and agents cannot be installed on the Tivoli Enterprise Portal Server computer.

Chapter 11. Configuring IBM Tivoli Monitoring Web Services (SOAP Server)

IBM Tivoli Monitoring Web Services provide an industry-standard open interface into products that use the Tivoli Management Services framework. This open interface provides easy access to performance and availability data, allowing you to use this information for advanced automation and integration capabilities. Web Services implements a client/server architecture. The client sends SOAP requests to the SOAP server. The server receives and processes the SOAP requests from the client. Predefined SOAP methods let you perform many functions within the monitored environment. Using Web Services requires a basic understanding of SOAP, XML and XML Namespaces, and the Web Services Description Language (WSDL).

By default, the SOAP server is enabled on all hub monitoring servers. This chapter describes how to configure security on a SOAP server, and how to configure communication between SOAP servers.

Note: You cannot make SOAP requests from IBM Tivoli Monitoring to earlier SOAP servers (such as those in OMEGAMON Platform V350/360).

For complete information about using Web Services and customizing the SOAP interface for your site, refer to the *IBM Tivoli Monitoring Administrator's Guide*.

Table 65 outlines the steps required to configure the SOAP server.

Table 65. Overview of SOAP Server configuration steps

Task	Where to find information
Define the hubs with which your SOAP Server communicates.	"Defining hubs"
Create users and grant them access.	"Adding users" on page 258
Verify that you have successfully configured SOAP.	"Verifying the configuration" on page 260

Defining hubs

In this step you activate a SOAP server and define hubs with which it communicates. You can use Manage Tivoli Monitoring Services to configure the SOAP server. On Linux and UNIX you can also use the **itmcmd config** command. After you configure the SOAP Server, you must restart the Tivoli Enterprise Monitoring Server.

- "Windows: Defining hubs"
- "UNIX and Linux: Defining hubs (GUI procedure)" on page 256
- "UNIX and Linux: Defining hubs (CLI procedure)" on page 257

Windows: Defining hubs

Use the following steps to define SOAP hubs on Windows:

1. Start Manage Tivoli Monitoring Services (select **Start → (All) Programs → IBM Tivoli Monitoring → Manage Tivoli Monitoring Services**).

© Copyright IBM Corp. 2005, 2007

2. In the Manage Tivoli Monitoring Services window, right-click **Tivoli Enterprise Monitoring Server**.
3. Click **Advanced → Configure SOAP Server Hubs**.

   The SOAP Server Hubs Configuration window is displayed. If the name of the local hub does not appear in the tree, define the local hub, including assigning user access, before defining the hubs with which it communicates.
4. Click **Add Hub**. The Hub Specification window is displayed.
5. Select the communications protocol to be used with the hub from the **Protocol** menu.
6. Specify an alias name in the **Alias** field.

   The alias for the local hub monitoring server must always be "SOAP". For hubs with which the local SOAP Server communicates, you may choose any alias (for example, `HUB2`). Alias names can be a minimum of 3 characters and a maximum of 8 characters.
7. Do one of the following:
   - If you are using TCP/IP or TCP/IP Pipe communications, complete the fields in Table 66:

Table 66. TCP/IP Fields in Hub Specification dialog

Field	Description
Hostname or IP Address	The host name or TCP/IP address of the host computer.
Port	The TCP/IP listening port for the host computer.

   - If you are using SNA communications, complete the fields in Table 67:

Table 67. SNA Fields in Hub Specification dialog

Field	Description
Network Name	Your site SNA network identifier.
LU Name	The LU name for the monitoring server. This LU name corresponds to the Local LU Alias in your SNA communications software.
LU6.2 LOGMODE	The name of the LU6.2 logmode. Default: CANCTDCS.
TP Name	The Transaction Program name for the monitoring server.

8. Click **OK**. The server tree is displayed, with the newly defined hub.

You can define any hubs with which the local SOAP Server will communicate by repeating steps 4 - 7, or you can specify which user IDs can access the SOAP Server you just defined and what access privileges they have. See “Adding users” on page 258.

UNIX and Linux: Defining hubs (GUI procedure)

Use the following steps to define SOAP hubs on UNIX or Linux using Manage Tivoli Monitoring Services:

1. Change to the *<itm_install_dir>*/bin directory and start Manage Tivoli Monitoring Services by entering the following command:

   ```
   ./itmcmd manage
   ```

The Manage Tivoli Monitoring Services Window is displayed.

2. Right-click **Tivoli Enterprise Monitoring Server** and select **Configure** from the popup menu.

   The Configure TEMS window is displayed.

3. Click **Save**.

   The SOAP Server Hubs Configuration window"UNIX and Linux: Defining hubs (GUI procedure)" on page 256 is displayed.

4. Confirm that the host name or IP address, port number, and protocol displayed for the hub monitoring server are correct. If not, correct them.

   If the name of the local hub does not appear in the tree, define the local hub before defining the hubs with which it communicates. The alias for the local hub must always be "SOAP".

5. To add another hub:

   a. Type the name or IP address and the port number of the host in the appropriate fields. The port should be match the hub's protocol port number. By default, this is 1918.

   b. Specify an alias name in the **Alias** field.

      Alias names can be a minimum of 3 characters and a maximum of 8 characters (for example, HUB2).

   c. Select the communications protocol to be used with the hub from the **Transport** menu.

6. Click **Add Host**.

   The server tree is displayed, with the newly defined hub.

You can now define any hubs with which the local SOAP Server will communicate by repeating step 5, or you can specify which user IDs can communicate with the local SOAP Server and what access privileges they have.

UNIX and Linux: Defining hubs (CLI procedure)

Complete the following steps to configure the SOAP server:

1. On the host of the hub monitoring server on which you want to configure Web Services, change to the <install_dir>/bin directory and enter the following command:

   ```
   ./itmcmd config -S -t <tems_name>
   ```

2. Accept the defaults, which should reflect the choices made during the last configuration, until you see the following prompt:

   ```
   *************************

   Editor for SOAP hubs list

   *************************

   Hubs
   ## CMS_Name
   1 ip.pipe:TEMS_NAME[port_#]

   1)Add, 2)Remove ##, 3)Modify Hub ##, 4)UserAccess ##, 4)Cancel, 5)Save/exit:
   ```

3. To add a hub with which the local hub can communicate:

   a. Type 1 and press Enter.

   b. Respond to the following prompts as shown in :

```
Network Protocol [ip, sna, ip.pipe, or ip.spipe] (Default is: ip):
CMS Name (Default is: local_host):
Port Number (Default is: 1918):
Alias (Default is: SOAP):
```

Table 68. SOAP hub configuration values

Network Protocol	The communications protocol configured for the hub monitoring server
CMS Name	The host name of the hub monitoring server. The host name must be fully
Port Number	The protocol port for the hub monitoring.
Alias	An alias for the hub. Alias names can be a minimum of 3 characters and a maximum of 8 characters. The alias for the local hub must always be SOAP, but you must create a new alias for additional hubs (for example, HUB2).

After you enter the alias, the list of hubs is displayed with the new hub added. For example,

```
Hubs
##      CMS_Name
1       ip.pipe:chihuahua[1918]
2       ip:maple[1918]

1)Add, 2)Remove ##, 3)Modify Hub ##, 4)UserAccess ##, 5)Cancel, 6)Save/exit:
```

You can continue to add hubs, or you can proceed to define user access for the hubs you have already defined.

Adding users

Access to SOAP server can be secured in one of two ways: by enabling **Security: Validate User** and creating user accounts on the host of the hub monitoring server, or by adding specific users to the server definition.

If **Security: Validate User** is *not* enabled and no users are added to the server definition, the SOAP server honors all requests regardless of the sender. If **Security: Validate User** *is* enabled on the hub monitoring server, the SOAP server honors requests only from users defined to the operating system or security authorization facility of the host of the monitoring server.

However, if any users are added to the SOAP server definition, only those users have access to the server, regardless of whether or not **Security: Validate User** is enabled.

In this step you define users to a SOAP Server and specify the access privileges for each user: Query or Update. The access privileges control what methods the user is allowed to use. Update access includes Query access. Table 69 lists the methods associated with each access. For information on using these methods, see *IBM Tivoli Monitoring: Administrator's Guide*.

Table 69. SOAP methods associated with access privileges

Method	Update	Query
CT_Acknowledge	x	
CT_Activate	x	
CT_Alert	x	

Table 69. SOAP methods associated with access privileges (continued)

Method	Update	Query
CT_Deactivate	x	
CT_Email	x	x
CT_Execute	x	x
CT_Export	x	x
CT_Get	x	x
CT_Redirect	x	x
CT_Reset	x	
CT_Resurface	x	
CT_Threshold	x	
WTO	x	x

After you configure the SOAP Server, you must restart the Tivoli Enterprise Monitoring Server.

Windows: Adding users

Use the following steps to define users to a SOAP server:

1. In the SOAP Server Hubs Configuration window, select the server (click anywhere within the server tree displayed).
2. Under Add User Data, type the user name.

   If **Security: Validate User** is enabled, user IDs 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.
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.
5. To delete a user: Select the user name from the tree and click **Delete Item**.
6. To delete a hub: Click anywhere within the hub's tree and click **Clear Tree**.

UNIX or Linux: Adding users (GUI)

Complete the following steps to define which users can make requests to a hub and assign access privileges to those users, using a graphical user interface:

1. If you are not already in the SOAP Server Hubs Configuration window, perform steps 1 - 3 in "UNIX and Linux: Defining hubs (GUI procedure)" on page 256.
2. In the hub tree, select the **Access** node for the hub to which you want to define users.

   The values for that hub are displayed in the section above the tree.
3. Type the user ID you want to add in the **User** field.

   If the **Security: Validate User** option is enabled on the hub, the user ID must be a valid user ID on the hub system.
4. Use the radio buttons in the **Access** field to select the type of access you want to grant to the user.

   See Table 69 on page 258 for a list of the method each type of access includes.
5. Click **Add User**.

The user ID appears under the appropriate subnode of the Access node of the selected hub.

6. To add additional users, repeat steps 2 through 5.
7. Click **OK** to close the window and save the changes.

UNIX or Linux: Adding users (CLI)

Complete the following steps to define users to a hub and assign access privileges using the command line interface:

1. If you are not already at the following prompt, perform steps 1 and 2 in "UNIX and Linux: Defining hubs (CLI procedure)" on page 257:

```
************************

Editor for SOAP hubs list

************************

Hubs
## CMS_Name
1 ip.pipe:TEMS_NAME[port_#]

1)Add, 2)Remove ##, 3)Modify Hub ##, 4)UserAccess ##, 4)Cancel, 5)Save/exit:
```

2. To define users and assign access privileges, enter 4 followed by a space, and then the number (in the list) of the hub you want to configure. For example:

```
1)Add, 2)Remove ##, 3)Modify Hub ##, 4)UserAccess ##, 5)Cancel, 6)Save/exit:4 1
```

   The following prompt is displayed:

```
=> Query Access:

=> Update Access:

1)QueryAdd <user>, 2)UpdateAdd <user>, 3)Remove ##, 4)Exit :
```

   Any users already defined are listed under the corresponding access.

3. To define a user with Query access, enter 1 followed by a space and the user ID. To define a user with Update access, enter 2 followed by a space and the user ID. See Table 69 on page 258 for a list of the methods associated with each type of access.

   Note: If the **Security: Validate User** option is enabled, the user ID must be a valid user on the hub system.

   The prompt appears again with the new user added to the appropriate access list. You can continue to add users by repeating step 3 or complete the configuration by typing 4 and pressing Enter.

Verifying the configuration

In this step you verify that SOAP has been correctly configured by starting the SOAP client and making a request using the command line utility kshsoap.

Use the following steps:

1. Verify that the monitoring server that you used to enable SOAP is running. If not, start it.
2. Open a command window.
3. Change to the <install_dir>\cms directory (on Windows) or the <install_dir>/TBD (on UNIX and Linux operating systems).

4. In the current directory, create an ASCII text file named SOAPREQ.txt that contains the following SOAP request:

   ```
   <CT_Get><object>ManagedSystem</object></CT_Get>
   ```

   Or if security has been enabled:

   ```
   <CT_Get><userid>logonid</userid><password>password</password> \
   <object>ManagedSystem</object></CT_Get>
   ```

5. Create another ASCII text file named URLS.txt that contains URLs that will receive the SOAP request. For example: http://hostname:1920///cms/soap
6. Run the following command:

   ```
   kshsoap SOAPREQ.txt URLS.txt
   ```

   SOAPREQ.txt is the name of the file that contains the SOAP request and URLS.txt is the name of the file that contains the URLs.

The kshsoap utility processes the SOAPREQ.txt file and displays the output of the SOAP request in the command window. The SOAP request is sent to each URL listed in URLS.txt, and the SOAP response from each URL displays in the DOS window.

Part 4. Setting up data warehousing

The chapters in this section provide instructions for installing and configuring the components that collect and manage historical data in the Tivoli Data Warehouse.

Chapter 12, "Tivoli Data Warehouse solutions," on page 265 introduces and summarizes your options for database platforms, operating systems, and communications between warehousing components.

Chapter 13, "Tivoli Data Warehouse solution using DB2," on page 273 provides information and instructions for implementing a Tivoli Data Warehouse solution using DB2 for the warehouse database.

Chapter 14, "Tivoli Data Warehouse solution using Microsoft SQL Server," on page 299 provides information and instructions for implementing a Tivoli Data Warehouse solution using Microsoft SQL Server for the warehouse database.

Chapter 15, "Tivoli Data Warehouse solution using Oracle," on page 315 provides information and instructions for implementing a Tivoli Data Warehouse solution using Oracle for the warehouse database.

Chapter 16, "Tivoli Data Warehouse solutions: common procedures," on page 337 contains information and procedures common to the Tivoli Data Warehouse solutions that use any of the supported database platform. You should read the chapter that pertains to the database platform you are using for the warehouse before you read this chapter.

© Copyright IBM Corp. 2005, 2007

Chapter 12. Tivoli Data Warehouse solutions

The term *Tivoli Data Warehouse solution* refers to the set of IBM Tivoli Monitoring components, successfully installed and configured, that interact to collect and manage historical data. These *warehousing components* include the Tivoli Enterprise Portal server, Tivoli Data Warehouse database, the Warehouse Proxy agent, and the Summarization and Pruning agent.

While all Tivoli Data Warehouse solutions include these four components, the details of any particular solution vary according to the size of the environment, which database management systems are used, and which operating systems are involved. This chapter introduces and summarizes your options for database platforms, operating systems, and communications between warehousing components.

- "New in V6.2"
- "Planning assumptions" on page 266
- "Firewall considerations for the Tivoli Data Warehouse" on page 267
- "Summary of supported operating systems" on page 268

Each of the next three chapters describes how to implement solutions for a variety of configurations using one of the supported database platforms: IBM DB2, Microsoft SQL Server, and Oracle.

New in V6.2

The following features are new in V6.2:

- Use of variable length character columns

  Starting with V6.2, character columns in raw data and summary tables larger than 16 characters are now created as variable length columns (VARCHAR in DB2, VARCHAR2 in Oracle, VARCHAR or NVARCHAR in SQL Server) rather than fixed length CHAR or NCHAR columns. This significantly reduces disk space requirements for tables and improves the performance and scalability of the warehouse.
- Most key columns in summary tables defined as NOT NULL

  Many columns in summary tables can never have a NULL value. Defining these columns as NOT NULL reduces disk space requirements. This is particularly true for DB2 since these columns are indexed. Index disk space requirements are significantly reduced when using DB2.
- Improved indexing on summary tables

  Indexes on summary tables now include all of the key columns needed for SNP processing. This significantly improves SNP performance since many tablespace scans have been eliminated.

These improvements are available only on tables or indexes created by the 6.2 version of the Warehouse Proxy and Summarization and Pruning agents. Currently there is no migration utility to convert tables and indexes that were created in 6.1 versions of these agents, but those tables and indexes can be used by all of the V6.2 components.

© Copyright IBM Corp. 2005, 2007

Planning assumptions

The information in this and the next three chapters is based on the following assumptions:

- You have completed the preliminary planning required to determine the size and topology of your environment and your warehousing needs. You may have already installed a monitoring server, a portal server, and some monitoring agents, but you have not yet created the Tivoli Data Warehouse.
- You are not installing IBM Tivoli Monitoring on one computer.
- You will create the Tivoli Data Warehouse database on a different computer from the Tivoli Enterprise Portal Server.
- If you are upgrading from IBM Tivoli Monitoring V6.1, you have performed the necessary agent warehouse database upgrade steps.

The following sections discuss these assumptions in more detail.

Preliminary planning is complete

For guidance on planning the size of your environment and determining the warehousing capacity you need, see "Scenarios for small, medium, and large environments" on page 27 and "Planning considerations for the Tivoli Data Warehouse" on page 19. The deployment scenarios illustrate your options for where to locate the warehousing components, whether to have multiple Warehouse Proxy agents reporting to the same hub monitoring server, and whether to deploy single or multiple hub installations.

This is not a single computer installation

The information in the current chapter and the next three chapters assume an environment with more than one computer.

In environments where monitoring and warehousing needs are minimal, such as a test environment, you can install all IBM Tivoli Monitoring components on one computer: a monitoring server, portal server, data warehouse, Warehouse Proxy agent, and Summarization and Pruning agent. (See Figure 3 on page 28 for an illustration of a single computer deployment with one backup server.)

If you install all components on a Windows system with either DB2 or Microsoft SQL Server, many of the warehouse configuration tasks are automated. If you want to deploy IBM Tivoli Monitoring on one Windows computer with either of these database platforms, follow the instructions in Chapter 5, "Installing IBM Tivoli Monitoring on one computer," on page 105.

The data warehouse is remote from the portal server

There are two databases involved in IBM Tivoli Monitoring:

- The *Tivoli Enterprise Portal Server database* (or *portal server database*) stores user data and information required for graphical presentation on the user interface. The portal server database is created automatically during configuration of the portal server. It is always located on the same computer as the portal server.
- The *Tivoli Data Warehouse database* (also called the *warehouse database* or *data warehouse*) stores historical data for presentation in historical data views. While it is possible for the warehouse database to be located on the portal server (as in the single computer deployment), it is best to create the database on a remote computer to handle the warehousing needs of most production environments.

The procedures described in the next three chapters are based on the assumption that you will install the Tivoli Data Warehouse database remotely from the portal server.

No assumption is made about where you will install the Warehouse Proxy agents and Summarization and Pruning agent. Either of these agents may be installed on the same computer as the Tivoli Data Warehouse or on a different computer:

- Installing the Warehouse Proxy agent and Summarization and Pruning agent on the same computer as the data warehouse minimizes server deployments, simplifies configuration, and eliminates network transmission overhead.
- If you install these components are different computers, ensure that you have a high-speed network connection for best performance.
- In environments with more than one Warehouse Proxy agent reporting to the same hub monitoring server, install each Warehouse Proxy on a separate computer.

Agent warehouse database upgrade

Some of the monitoring agents have made changes to the warehouse tables that require performing upgrade procedures before running the V6.2 Warehouse Proxy and Summarization and Pruning agents. See "Upgrading the warehouse" on page 95 for more information.

Firewall considerations for the Tivoli Data Warehouse

Firewalls can be a significant factor in most Tivoli Data Warehouse implementations. At a minimum:

- The Warehouse Proxy agent must be able to communicate with:
  - The database
  - The hub monitoring server
  - The agents that are exporting data
- The Summarization and Pruning agent must be able to communicate with:
  - The database
  - The monitoring server it is configured to communicate with (not necessarily the hub)
  - The Tivoli Enterprise Portal Server
- The agents exporting data to the Warehouse Proxy agent must be able to communicate with the Warehouse Proxy agent.

Appendix C, "Firewalls," on page 427 contains information on the firewall options available. The IBM Redbook, *Tivoli Management Services Warehouse and Reporting*, available from www.redbooks.ibm.com discusses firewall considerations specific to the Tivoli Data Warehouse in detail.

Next steps

After you have completed your preliminary planning, you are ready to implement your Tivoli Data Warehouse solution:

- Review the *Summary of supported operating systems* section in this chapter to understand your options for operating system platforms, database platforms, and communications between warehousing components, all summarized in a single composite graphic. This section also describes the relationships between warehousing components.

- The next three chapters are organized by database platform. Follow the instructions in the chapter that pertains to the database platform you are using for the Tivoli Data Warehouse database: IBM DB2, Microsoft SQL Server, or Oracle.

Summary of supported operating systems

Figure 38 summarizes the supported operating system platforms for the various warehousing components, the supported database products, and the connections between components. For more specific information about supported operating systems and database products, including product names and versions, see "Hardware and software requirements" on page 70. In this diagram, UNIX refers to any UNIX platform supported by the RDBMS.

Note: The diagram is not meant to suggest that each warehousing component must be installed on a separate computer. Multiple components can exist on the same computer provided there is operating system support for all installed components. Connections between components must be configured whether or not they exist on the same computer. (Although the diagram makes no assumptions about where components are installed, the procedures described in the next three chapters assume a Tivoli Data Warehouse that is remote from the portal server.)

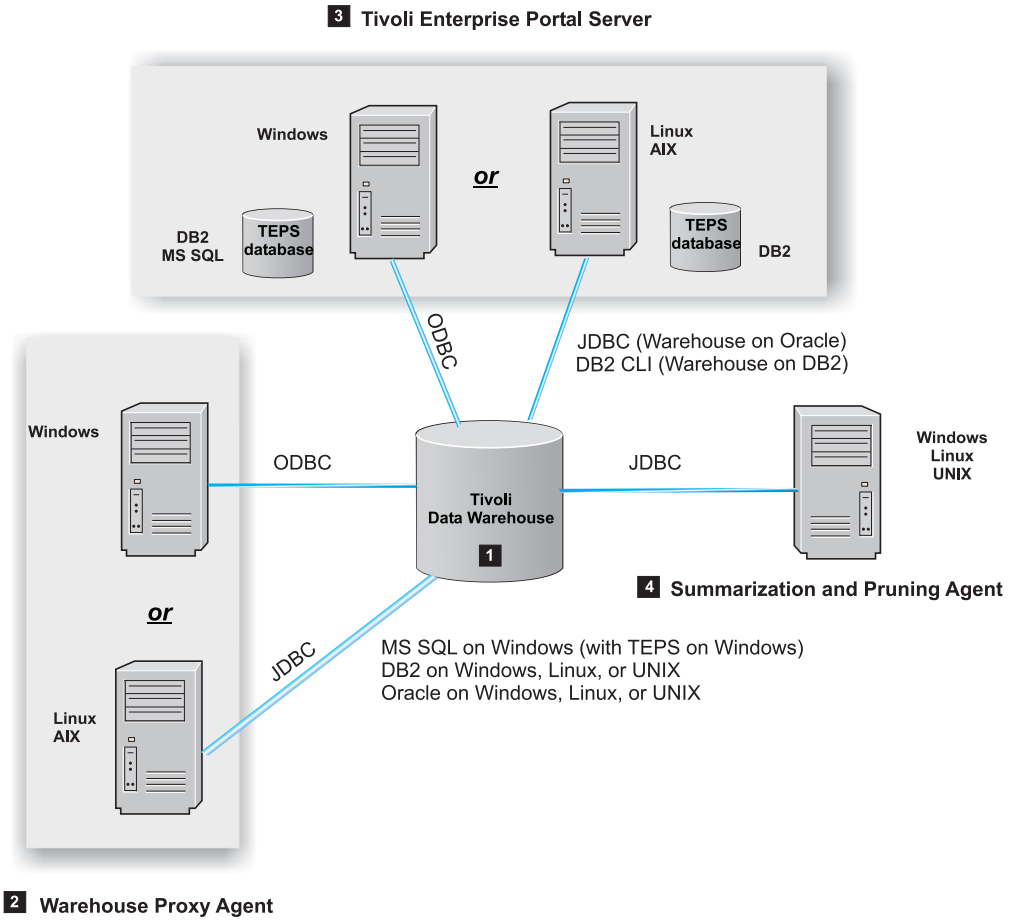


Figure 38. Summary of support for the Tivoli Data Warehouse

In the following discussion, numbered product components correspond to the numbers on the diagram.

1 Tivoli Data Warehouse database

Data collected by monitoring agents is stored at intervals in binary files. The data in the binary files is referred to as *historical data*. The binary files is located either at the agents or at the monitoring server (hub or remote) to which the agents report. (An administrator can determine where the data is stored. The monitoring agents and monitoring server are not shown in the diagram.)

The historical data is sent from its temporary storage location (at the monitoring agents or monitoring server) to the Warehouse Proxy agent at a preset interval (either every hour or every 24 hours). The Warehouse Proxy agent sends the data it receives to the Tivoli Data Warehouse.

Long-term historical data in binary files (data that is older than 24 hours) is pruned when the monitoring agent or monitoring server receives an acknowledgment that the data has been successfully inserted into the Tivoli Data Warehouse (an operation that may take some time). (The pruning of binary files is not the pruning performed by the Summarization and Pruning agent. The Summarization and Pruning agent prunes data in the Tivoli Data Warehouse.) The result of these operations is that at any given time the binary files contain primarily *short-term historical data* (data less than 24 hours old) and the Tivoli Data Warehouse contains primarily *long-term historical data* (data older than 24 hours).

The Tivoli Data Warehouse database can be created using Microsoft SQL Server, IBM DB2, or Oracle, on the indicated operating system platforms. Note that the warehouse database is supported on Microsoft SQL Server only if the Tivoli Enterprise Portal Server (TEPS) is installed on Windows. This condition applies even if the warehouse database and portal server are installed on separate computers. For example, a portal server on Linux does not support a warehouse database on Microsoft SQL Server.

2 Warehouse Proxy agent

A Warehouse Proxy agent on Windows uses an ODBC connection to send the collected data to the warehouse database. A Warehouse Proxy agent on Linux or AIX uses a JDBC connection.

The Warehouse Proxy agent will do the following as needed:

- Create new tables and indexes.
- Alter existing tables.

  For example, add a new column to a table. This can occur if the table was created for an older version of an agent but data is being exported for the first time from a newer version of the agent that has more attributes.

Firewall considerations:

- The Warehouse Proxy agent must be able to communicate with the hub monitoring server.
- The Warehouse Proxy agent must be able to communicate with the RDBMS.

- The agents exporting data must be able to communicate with the Warehouse Proxy *and* the Warehouse Proxy agent must be able to communicate with the agents (there must be two-way communication between agents and the Warehouse Proxy agent).

Appropriate ports must be open to support these communication channels (see Appendix C, "Firewalls," on page 427).

3 Tivoli Enterprise Portal Server

The Tivoli Enterprise Portal Server retrieves historical data for display in historical data views in the Tivoli Enterprise Portal. It retrieves short-term historical data from the binary files on the monitoring agents or monitoring server. It retrieves long-term historical data from the Tivoli Data Warehouse.

In Figure 38 on page 268, the Tivoli Enterprise Portal Server is shown with the *portal server database* (designated as *TEPS database* in the diagram). The portal server database stores user data and information required for graphical presentation on the user interface. Before you install and configure the portal server, you must install the database platform (RDBMS) to be used for the portal server database (DB2 or Microsoft SQL Server) on the same computer. The portal server database is created automatically during configuration of the portal server.

Although the portal server database is not considered a warehousing component, it is included in the diagrams in this and the following chapters because it can affect the installation and configuration tasks required for the Tivoli Data Warehouse database. For example, the database client already installed for the portal server database can connect to a remote warehouse database, provided both databases use the same database platform. There is no need to manually install another client.

If the portal server is installed on Windows, it uses an ODBC connection to request and retrieve historical data from the warehouse database. If the portal server is installed on Linux or AIX, it communicates with the warehouse database through a JDBC connection, if the warehouse is installed on Oracle, or through a proprietary DB2 CLI connection if the warehouse is installed on DB2.

4 Summarization and Pruning agent

The Summarization and Pruning agent retrieves detailed data from the warehouse database, aggregates or prunes the data, and returns the processed data to the warehouse. Communication takes place through a JDBC connection, regardless of the operating system on which the Summarization and Pruning agent is installed.

The Summarization and Pruning agent will create tables, indexes, and views as needed. This could happen in either of the following situations:

- Summarization is enabled for the first time for an attribute group.
- Additional summarizations are enabled for an attribute group.

In addition, the Summarization and Pruning agent, like the Warehouse Proxy agent, may alter existing tables by adding new columns.

Firewall considerations:

- The Summarization and Pruning agent must be able to communicate with the RDBMS.

- The Summarization and Pruning agent must be able to communicate with the Tivoli Enterprise Portal Server.
- The Summarization and Pruning agent must be able to communicate with the Tivoli Enterprise Monitoring Server it is configured to use.

Chapter 13. Tivoli Data Warehouse solution using DB2

Use the information and instructions in this chapter to implement a Tivoli Data Warehouse solution using DB2 for the warehouse database. The following table lists the goals for creating a DB2 solution.

Table 70. Goals for creating a Tivoli Data Warehouse solution using DB2

Goal	Where to find information
Review your options, specific to a DB2 solution, for operating system platforms and communications between warehousing components.	"Supported components"
Install prerequisite software before implementing your Tivoli Data Warehouse solution.	"Prerequisite installation" on page 275
Understand how to use the instructions for implementing your Tivoli Data Warehouse solution.	"Implementing a Tivoli Data Warehouse solution using DB2" on page 276
Complete the steps for implementing your Tivoli Data Warehouse solution using DB2 for the data warehouse.	"Step 1: Create the Tivoli Data Warehouse database" on page 278 "Step 2: Install and configure communications for the Warehouse Proxy agent" on page 283 "Step 3: Configure communications between the Tivoli Enterprise Portal Server and the data warehouse" on page 292 "Step 4: Install and configure communications for the Summarization and Pruning agent" on page 297

Supported components

Figure 39 on page 274 presents the options for a Tivoli Data Warehouse solution using DB2 for the warehouse database. The diagram summarizes the supported operating system platforms for the various warehousing components, the supported database products, and the connections between components. For more specific information about supported operating systems and database products, including product names and versions, see "Hardware and software requirements" on page 70.

© Copyright IBM Corp. 2005, 2007

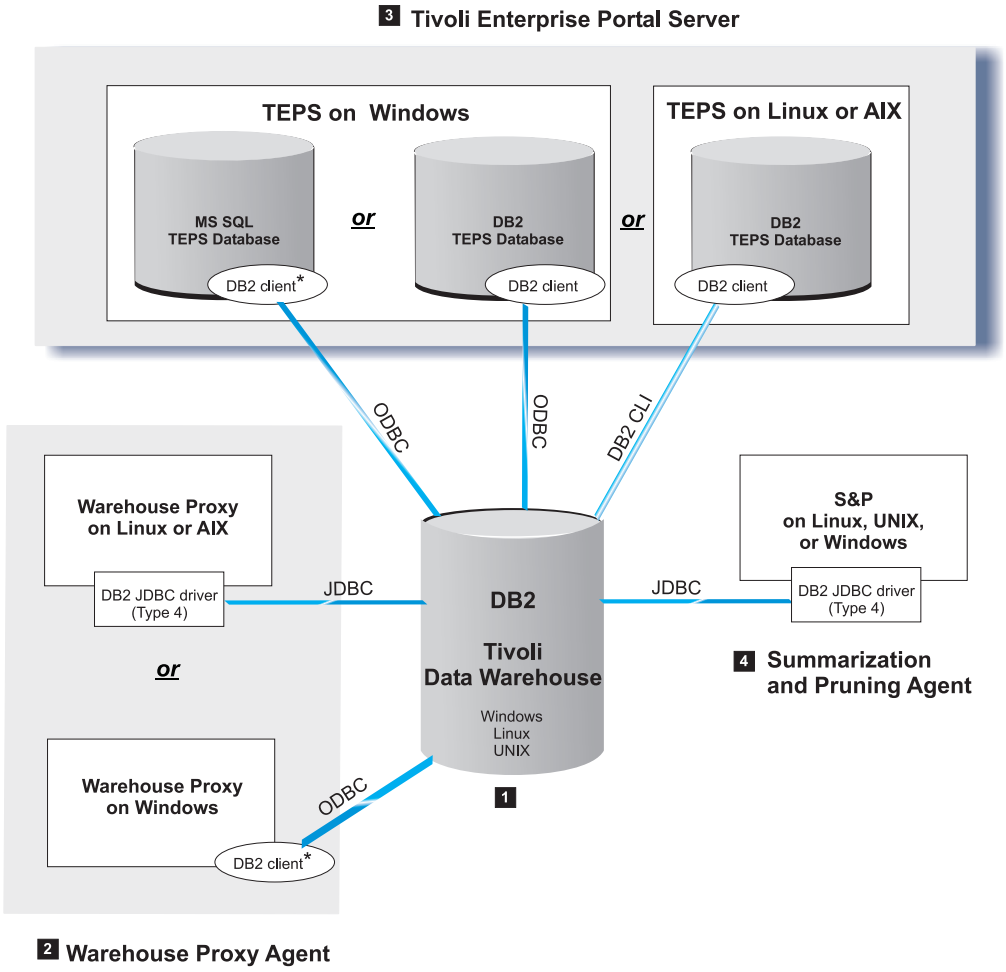


Figure 39. Tivoli Data Warehouse solution using DB2

Note: An asterisk (*) next to a database client indicates that you must manually install the client if it does not already exist.

In the following discussion, numbered product components correspond to the numbers on the diagram.

1 Tivoli Data Warehouse on DB2

A Tivoli Data Warehouse database on DB2 can be installed on supported Windows, Linux, or any UNIX platform that is supported by DB2. Ensure that the DB2 TCP/IP listeners are active in order to accept connections from a DB2 client or JDBC driver.

2 Warehouse Proxy Agent

A Warehouse Proxy agent on Linux or AIX communicates with the warehouse database through a JDBC connection. Install a Type 4 driver (DB2 UDB JDBC Universal Driver) on the computer where the Warehouse Proxy agent is located.

A Warehouse Proxy agent on Windows communicates with the warehouse database through an ODBC connection. The ODBC driver is included with the DB2 client. If the Tivoli Data Warehouse is located on a remote computer, install a DB2

client on the local computer where the Warehouse Proxy agent is located. Also, catalog the remote node and database on the local computer.

3 Tivoli Enterprise Portal Server

A Tivoli Enterprise Portal Server on Windows, Linux, or AIX can connect to a DB2 data warehouse through a DB2 client installed on the portal server. If the *portal server database* (designated as *TEPS database* in the diagram) uses DB2, the DB2 client already exists. *Manually* install a DB2 client on the portal server only if the portal server database uses Microsoft SQL Server.

A portal server on Windows communicates with the warehouse database through an ODBC connection. The ODBC driver is included with the DB2 client. Catalog the remote warehouse node and database on the portal server.

A portal server on Linux or AIX uses the DB2 CLI interface, a proprietary connection, to communicate with the warehouse database. If the warehouse database is installed on a different computer from the portal server, catalog the remote database and remote node on the portal server.

4 Summarization and Pruning Agent

The Summarization and Pruning agent communicates with the warehouse database through a JDBC connection from any supported operating system. Install a DB2 Type 4 JDBC driver (*DB2 UDB JDBC Universal Driver*) on the computer where the Summarization and Pruning agent is located.

Prerequisite installation

Before you implement your Tivoli Data Warehouse solution, complete one or more hub installations, *excluding the warehousing components*. Include the following components in each hub installation:

- The hub Tivoli Enterprise Monitoring Server
- *(Optional)* One or more remote monitoring servers
- The Tivoli Enterprise Portal Server, including the prerequisite RDBMS for the portal server database (DB2 or Microsoft SQL Server)
- An IBM DB2 server on the computer where you will create the Tivoli Data Warehouse database. (The Tivoli Data Warehouse database can be shared in a multi-hub installation or dedicated to a single hub.)
- *(Optional)* A portal desktop client
- *(Optional)* Monitoring agents, and the application support for the monitoring agents

  Note: The term *monitoring agent*, as used here, refers to agents that collect data directly from managed systems, not the Warehouse Proxy agent or Summarization and Pruning agent.
- *(Optional)* Language packs for all languages other than English

Refer to Table 71 for related information:

Table 71. Information topics related to installation of prerequisite software for a Tivoli Data Warehouse solution

Topic	Where to find information
Single and multiple hub installations	To understand the terminology related to single and multiple hub installations, see "Scenarios for small, medium, and large environments" on page 27.
Installation procedures for prerequisite components	The detailed instructions for installing the prerequisite components are described in Chapter 6, "Installing IBM Tivoli Monitoring," on page 113. Refer to your database documentations for instructions on how to install a supported database server.
Supported RDBMS versions	For specific information about the supported database platforms for the portal server database and the Tivoli Data Warehouse, see "Hardware and software requirements" on page 70.

Implementing a Tivoli Data Warehouse solution using DB2

Use the instructions in the remainder of this chapter to implement a Tivoli Data Warehouse solution using DB2 for the data warehouse.

Assumptions

The implementation instructions are based on the following assumptions:

- You will create the Tivoli Data Warehouse database on a different computer from the Tivoli Enterprise Portal Server.
- You will create a single Tivoli Data Warehouse database, to be used either within a single hub installation or to be shared in a multi-hub installation. If you have multiple independent hub installations, repeat the implementation steps for each hub installation. (See "Scenarios for small, medium, and large environments" on page 27 for information about hub installations.)
- No assumption is made about where you will install the Warehouse Proxy agent and Summarization and Pruning agent. Either of these agents may be installed on the same computer as the Tivoli Data Warehouse or on a different computer.

Note: Each instance of the restricted-use version of DB2 UDB Enterprise Edition V9.1 provided for use with the portal server and the Tivoli Data Warehouse must be registered. See "Registering the DB2 product license key using the db2licm command" on page 79.

Solution steps

To implement your Tivoli Data Warehouse solution using DB2, complete the four major steps described in the remaining sections of this chapter, in the order listed:

1. Create the Tivoli Data Warehouse database.
2. Install and configure communications for the Warehouse Proxy agent.
3. Configure communications between the Tivoli Enterprise Portal Server and the data warehouse.
4. Install and configure communications for the Summarization and Pruning agent.

Each major step consists of a series of installation and configuration tasks, listed and described in a table. Use the step tables as a road map for implementing your solution. The step tables describe the tasks at a high level, account for variations among configuration options (such as which operating system is used for a component), and reference the appropriate sections for detailed implementation procedures. To implement your solution successfully:

- Perform the tasks in the order listed in the table.
- Do not skip a table to the procedures that follow it.

  Be aware that some of the implementation procedures referenced in a table are included in this chapter and some are documented elsewhere. In some cases, the task is described in the table, without referencing a separate procedure. Read and follow all instructions in the tables.

Step 1: Create the Tivoli Data Warehouse database

Complete the tasks described in the following table to create a Tivoli Data Warehouse database using DB2 and to make it accessible to clients.

Table 72. Tasks for creating the Tivoli Data Warehouse database

Task	Procedure
Create the Tivoli Data Warehouse database on one of the supported Windows, Linux, or UNIX operating systems. To comply with the assumptions described in the introduction to this chapter, create the warehouse database on a different computer from the Tivoli Enterprise Portal Server.	For guidance on planning the size and disk requirements for the warehouse database, see "Planning considerations for the Tivoli Data Warehouse" on page 19. For information about creating the warehouse database using DB2, see "Creating the warehouse database on DB2."
Create an operating system (OS) user account (user name and password) with administrator authority on the computer where the warehouse database is located. The warehousing components (portal server, Warehouse Proxy agents, and Summarization and Pruning agent) will use this OS user account to access the database. Create only one user account for all warehousing components to use. This user is referred to in this chapter as the *warehouse user*.	"Creating a warehouse user on Windows" on page 279 "Creating a warehouse user on Linux or UNIX" on page 279
(*Optional*) Restrict the authority of the warehouse user. Initially, the warehouse user is created with OS administrative authority. Use the referenced procedure if you want to limit the authority of the warehouse user to just those privileges required to access and use the data warehouse.	"Limiting the authority of the warehouse user" on page 280
(*Tivoli Data Warehouse on Linux or AIX only*) Activate the DB2 TCP/IP listeners on the DB2 server where the Tivoli Data Warehouse is installed. The TCP/IP listener processes on the DB2 server must be active in order to accept connections from a DB2 client or JDBC driver. The DB2 listeners are automatically activated on Windows systems. Perform the referenced procedure to activate the DB2 listeners if the warehouse database is located on a Linux or AIX system.	"Activating the DB2 listeners on a UNIX DB2 server" on page 282

Creating the warehouse database on DB2

This section provides guidelines for creating the Tivoli Data Warehouse database on DB2. For specific instructions on how to create a DB2 database, refer to the DB2 documentation or have a database administrator create the database for you.

When you create the warehouse database using DB2, follow these guidelines:

- Create the database with UTF-8 encoding.
- Create a name for the warehouse database, and an operating system (OS) user account (user name and password) that the warehousing components (portal server, Warehouse Proxy agent, and Summarization and Pruning agent) can use to access the data warehouse. In these instructions, this user account is referred to as the *warehouse user*.

- Consider using the default values shown in Table 73 for the warehouse name and warehouse user. The default values are used in the configuration procedures for connecting the warehousing components to the warehouse database. (For example, see the entries in Figure 40 on page 287.)

Table 73. Default values for Tivoli Data Warehouse parameters

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

- Give the warehouse user administrative authority to the database initially. After that, you can optionally limit the authority of the warehouse user to just the privileges required for interacting with the data warehouse. See the following sections for information about creating and limiting the authority of the warehouse user.
  - "Creating a warehouse user on Windows"
  - "Creating a warehouse user on Linux or UNIX"
  - "Limiting the authority of the warehouse user" on page 280
- For a Tivoli Data Warehouse on Linux or AIX, ensure that the DB2 server is configured for TCP/IP communications. See "Activating the DB2 listeners on a UNIX DB2 server" on page 282.

Creating a warehouse user on Windows

Complete the following steps on the computer where the warehouse database is installed to create a Windows OS user with Administrator authority:

1. Right-click the **My Computers** icon on the Windows desktop and click **Manage**.
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 a user name and password in the **User Name** and **Password** fields. Confirm the password by typing it again in the **Confirm password** field.
5. Clear **User must change password at next logon**.
6. Click **Close**.
7. Click the **Groups** folder.
8. Double-click **Administrators** in the right pane of the window.
9. Click **Add** in the Administrator Properties window.
10. Locate the new user you created and select it.
11. Click **Add**.
12. Click **OK** and then **OK** again to close the Administrator Properties window.
13. Close the Computer Management window.

Creating a warehouse user on Linux or UNIX

Complete the following procedure on the computer where the warehouse database is installed to create a Linux or UNIX OS user with administrative authority to the warehouse:

- To create the user, follow the instructions in the documentation for the specific Linux or UNIX product and version that is installed on the computer where the warehouse database is located.
- To give this user administrative authority to the data warehouse, add the user to the DB2 SYSADM group. Run the following command to find the name of the DB2 SYSADM group:

  db2 get dbm cfg | grep SYSADM

  For example:

  ```
  db2 get dbm cfg | grep SYSADM
  SYSADM group name          (SYSADM_GROUP) = DB2GRP1
  ```

  In this example, the name of the DB2 SYSADM group is DB2GRP1. If you created an OS user named ITMUSER, add ITMUSER to DB2GRP1.

Limiting the authority of the warehouse user

If you do not want the warehouse user to have broad administrative authority, you can limit the authority of the warehouse user to just those privileges required for accessing and using the data warehouse. These more limited privileges include the authority to create and update tables, to insert information into the tables, to create indexes for the tables, and to grant public authority to the tables.

Before you begin

The Tivoli Data Warehouse requires one bufferpool and three tablespaces to begin its operation. The bufferpool and tablespaces are created by the warehouse user before the Warehouse Proxy agent starts, provided the warehouse user has administrative authority to the database. A warehouse user with limited authority cannot create the required bufferpool and tablespaces. Therefore, this procedure to limit the authority of the warehouse user includes steps to create the bufferpool and tablespaces in advance. Be sure to perform this procedure before the Warehouse Proxy agent starts.

Use the script shown in Table 74 on page 281 to create the required bufferpool and tablespaces. Create the script on a computer from which you can connect to the Tivoli Data Warehouse database server. The name of the script is KHD_DB2_crt_BP_TBSP.sql.

Table 74. Script for creating required bufferpool and tablespaces for the Tivoli Data Warehouse

```
-- CREATE a Bufferpool of page size 8K
CREATE BUFFERPOOL ITMBUF8K IMMEDIATE  SIZE 250[1] PAGESIZE 8 K;

-- CREATE a Regular Tablespace using the 8K Bufferpool
CREATE REGULAR TABLESPACE ITMREG8K PAGESIZE 8 K
    MANAGED BY SYSTEM
    USING ('itmreg8k')[2] BUFFERPOOL ITMBUF8k;

-- CREATE a System tablespace using the 8K Bufferpool
CREATE SYSTEM TEMPORARY TABLESPACE ITMSYS8K PAGESIZE 8 K
    MANAGED BY SYSTEM
    USING ('itmsys8k')[2] BUFFERPOOL ITMBUF8k;

-- CREATE a User tablespace using the 8K Bufferpool

CREATE USER TEMPORARY  TABLESPACE ITMUSER8K PAGESIZE 8 K
    MANAGED BY SYSTEM
    USING ('itmuser8k')[2] BUFFERPOOL ITMBUF8k;
```

Notes:

1. SIZE is is the number of 8K pages to allocate for the bufferpool. If there is sufficient memory, performance can be improved by increasing this number.
2. A fully qualified path can be specified here. As shown this will be created in a default directory.

Procedure

To limit the authority of the warehouse user, complete the following steps:

1. Connect to the data warehouse with db2admin privileges:

   ```
   db2 connect to warehouse user db2admin using password
   ```

   where *warehouse* is the name of the Warehouse database, *db2admin* is the DB2 administrator ID, and *password* is the password of the *db2admin* user ID. The user ID must be a DB2 user with SYSADM authority
2. Change to the directory where the KHD_DB2_crt_BP_TBSP.sql script is located.
3. Run the script to create the required bufferpool and tablespaces:

   ```
   db2 -stvf KHD_DB2_crt_BP_TBSP.sql
   ```
4. Remove administrative privileges from the warehouse user (OS user) that you created when you created the warehouse database:
   - On Windows, remove the warehouse user from the Administrator group.
   - On Linux or UNIX, remove the warehouse user from the SYSADM group to which it was assigned (for example, DB2GRP1). (See "Creating a warehouse user on Linux or UNIX" on page 279.)
5. Grant CONNECT and CREATETAB authorities to the warehouse user.

   CONNECT authority grants the user access to the database. CREATETAB authority allows the user to create and drop tables, to alter tables, to create and drop indexes for the tables, and to insert, delete, or update data in the tables.

   To grant these authorities, you can either use the DB2 Control Center (Database Authorities window) or the command line interface. If you use the command line interface, run commands similar to the following. In this example, the name of the warehouse user is `itmuser`.

```
db2 "GRANT CONNECT ON DATABASE TO USER itmuser"
db2 "GRANT CREATETAB ON DATABASE TO USER itmuser"
```

Setting database and instance configuration values

The default values for many of the configuration values for the DB2 database and the DB2 instance may not be acceptable for a production environment. Following are a few of the values you should consider adjusting. Consult the DB2 documentation or your DB2 database administrator for other adjustments that can improve performance.

LOGPRIMARY
Number of primary transaction logs. In a production environment, this value should be larger than the default.

LOGSECOND
Number of secondary log files. In a production environment, this value should be larger than the default.

NEWLOGPATH
Location of transaction logs. To improve performance, the logs should be placed on a separate physical disk from the tables and indexes.

LOGFILSIZ
Size of transaction log files. In a production environment, this value should be larger than the default.

LOCKTIMEOUT
Defaults to infinite wait, which can cause Warehouse Proxy and Summarization and Pruning processing to appear to be locked up. This should be set to a reasonable value such as 120 seconds.

Activating the DB2 listeners on a UNIX DB2 server

The TCP/IP listener processes on the DB2 server where the Tivoli Data Warehouse database is installed must be active in order to accept connections from a DB2 client or a JDBC Type 4 driver (*DB2 UDB JDBC Universal Driver*). On a Windows system, the DB2 listeners are automatically activated. Run the following commands on a UNIX system where the Tivoli Data Warehouse database is installed to activate the DB2 listeners:

```
db2set -i instance_name DB2COMM=tcpip
db2 update dbm cfg using SVCENAME port_number
db2stop
db2start
```

where *instance_name* is the name of the instance in which you created the warehouse database and *port_number* is the listening port for the instance. (The port number is specified in the file /etc/services.) For example:

```
db2set -i db2inst1 DB2COMM=tcpip
db2 update dbm cfg using SVCENAME 60000
db2stop
db2start
```

Step 2: Install and configure communications for the Warehouse Proxy agent

You can install one or more Warehouse Proxy agents to collect and send historical data to the Tivoli Data Warehouse database. Complete the tasks described in the following table, in the order listed, to install and configure each Warehouse Proxy agent.

Table 75. Tasks for installing and configuring communications for the Warehouse Proxy agent

Task	Procedure
Install one or more Warehouse Proxy agents. If you want to install a Summarization and Pruning agent on the same computer as one of the Warehouse Proxy agents, use the referenced procedures to install both agents at the same time. If you are installing more than one Warehouse Proxy agent, each agent must be installed on a separate computer. The installation procedure for Windows includes steps for configuring the connection between the agent and the hub Tivoli Enterprise Monitoring server. On Linux or AIX, this step is performed in a separate configuration procedure (*Configuring the monitoring agent*) and an X11 GUI is required to configure the agent. Alternatively, you can run the following command to utilize an X terminal emulation program (such as Cygwin) that is running on another computer: `export DISPLAY=`*`my_windows_pc_IP_addr`*`:0.0` where *my_windows_pc_IP_addr* is the IP address of a computer that is running an X terminal emulation program. See the information at right. Be sure to perform all referenced installation and configuration procedures.	To install a Warehouse Proxy agent on Windows, complete the procedure "Windows: Installing a monitoring agent" on page 149. To install a Warehouse Proxy agent on Linux or AIX, complete the procedure "Linux or UNIX: Installing a monitoring agent" on page 152, including the following subsections: • *Installing the monitoring agent* • *Configuring the monitoring agent* • *Changing the file permissions for agents* (if you used a non-root user to install the Warehouse Proxy) *Do not complete the procedure for starting the agent*.
(*Warehouse Proxy agent on Windows only*) • Install a DB2 client on the computer where the Warehouse Proxy agent is installed if *both* of the following statements are true: – The Warehouse Proxy is installed on Windows, and – The Warehouse Proxy needs to connect to a remote data warehouse. • Catalog the remote data warehouse on the Windows computer where you installed the DB2 client. You must perform this step before configuring an ODBC data source. (See the next row.) • Set the following system variable on the computer where the Warehouse Proxy agent is installed. Reboot the computer after setting the variable. DB2CODEPAGE=1208 Set the environment variable whether or not the warehouse database is local or remote.	Refer to the DB2 documentation for instructions on how to install a DB2 client. To catalog a remote data warehouse, see "Cataloging a remote data warehouse" on page 284.
(*Warehouse Proxy agent on Windows only*) On the computer where the Warehouse Proxy agent is installed, configure an ODBC data source for the data warehouse. Perform this procedure whether or not the Warehouse Proxy agent and the warehouse database are installed on the same computer.	"Configuring an ODBC data source for a DB2 data warehouse" on page 285

Table 75. Tasks for installing and configuring communications for the Warehouse Proxy agent (continued)

Task	Procedure
(*Warehouse Proxy agent on Linux or AIX only*) If the data warehouse is located on a remote computer, copy the *DB2 UDB JDBC Universal Driver* (Type 4 driver) JAR files, included with the DB2 product installation, to the local computer where the Warehouse Proxy agent is installed. You can copy the files to any directory on the local computer.	The Type 4 driver file names and locations are as follows: <*db2installdir*>/java/db2jcc.jar <*db2installdir*>/java/db2jcc_license_cu.jar where <*db2installdir*> is the directory where DB2 was installed. The default DB2 Version 9 installation directory is as follows: • On AIX: /usr/opt/db2_09_01 • On Linux: /opt/IBM/db2/V9.1
Configure the Warehouse Proxy agent to connect to the data warehouse. Perform this procedure whether or not the Warehouse Proxy agent and the warehouse database are installed on the same computer.	For a Warehouse Proxy agent on Windows, see "Configuring a Warehouse Proxy agent on Windows (ODBC connection)" on page 286. For a Warehouse Proxy agent on Linux or AIX, see "Configuring a Warehouse Proxy agent on Linux or AIX (JDBC connection)" on page 288.
If you are installing more than one Warehouse Proxy agent within the same hub monitoring server installation, associate each Warehouse Proxy agent with a subset of monitoring servers (hub or remote) within the installation. Each Warehouse Proxy agent receives data from the monitoring agents that report to the monitoring servers on the list. Use the environment variable KHD_WAREHOUSE_TEMS_LIST to specify a list of monitoring servers to associate with a Warehouse Proxy agent.	For an example topology of multiple Warehouse Proxy agents within the same hub monitoring server installation, see Figure 5 on page 31 and the related discussion. For instructions about installing and configuring multiple Warehouse Proxy agents within a single hub monitoring server installation, see "Installing and configuring multiple Warehouse Proxy agents" on page 347.
(*Optional*) Customize the configuration of the Warehouse Proxy agent for tuning performance.	"Tuning the performance of the Warehouse Proxy" on page 354
Start the Warehouse Proxy agent.	"Starting the Warehouse Proxy" on page 290

Cataloging a remote data warehouse

Perform this procedure on a computer where a DB2 client is installed to enable communication between the client and a *remote* DB2 server where the data warehouse is installed. For example, use this procedure to set up communication to a remote DB2 data warehouse server from:

- The DB2 client on the computer where the Tivoli Enterprise Portal Server is installed (on any platform)
- The DB2 client on a Windows computer where a Warehouse Proxy agent installed

Do *not* perform this procedure on the computer where the data warehouse (DB2 server) is installed or on a computer where there is no DB2 client (for example, on a computer where a Type 4 DB2 JDBC driver is used to communicate with the remote DB2 server).

Complete the following steps on the computer where the DB2 client is installed (the *local* computer):

1. Catalog the remote TCP/IP node where the warehouse database is installed:

   ```
   db2 catalog tcpip node <node_name> remote <host_name> server <port>
   db2 terminate
   ```

   where the indicated variables identify the location and port of the remote DB2 server. For *host_name*, specify the host name or IP address. The default port for a DB2 server is 60000. For example:

   ```
   db2 catalog tcpip node amsc2424 remote 8.53.36.240 server 60000
   db2 terminate
   ```

2. Catalog the remote Tivoli Data Warehouse database:

   ```
   db2 catalog db <db_name> as <db_alias> at node <node_name>
   db2 terminate
   ```

   where

   <*db_name*> is the name of the remote warehouse database.

   <*db_alias*> is the nickname or alias used to identify the remote warehouse database on the local computer. The local alias for the warehouse database must match the name that you specify in the configuration procedure for the portal server, Warehouse Proxy agent, or Summarization and Pruning agent.

   <*node_name*> is the name of the node where the warehouse database is located.

   Example:

   ```
   db2 catalog db WAREHOUS as WAREHOUS at node amsc2424
   db2 terminate
   ```

3. Test the connection to the remote warehouse database:

   ```
   db2 connect to <db_alias> user <user_name> using <user_password>
   ```

   where:

   <*db_alias*> is the nickname or alias used to identify the remote warehouse database on the local computer.

   <*user_name*> and <*user_password*> are the user ID and password that the local DB2 client uses to access the warehouse database.

   These values must match the values that you specify in the configuration procedures for the portal server, Warehouse Proxy agent, or Summarization and Pruning agent.

   Example:

   ```
   db2 connect to WAREHOUS user itmuser using itmpswd1
   ```

Configuring an ODBC data source for a DB2 data warehouse

A DB2 client on Windows requires an ODBC connection to the data warehouse. For the Warehouse Proxy agent, you must configure the ODBC connection manually.

Before you begin

- If the warehouse database is remote from the Warehouse Proxy agent, catalog the remote database before you configure the ODBC data source. See "Cataloging a remote data warehouse" on page 284. The ODBC connection does not work if the remote database has not been cataloged prior to performing this procedure.

- This procedure uses default values for the data source name, warehouse alias, and warehouse user ID. (Default values are used in configuration procedures for warehousing components.) Substitute different values if you do not want to use the default values.

Procedure

Complete the following procedure to set up an ODBC connection for a Warehouse Proxy agent on Windows to a local or remote Tivoli Data Warehouse.

1. On the computer where the Warehouse Proxy agent is installed, open the Control Panel.
2. Click **Administrative Tools → Data Sources (ODBC)**
3. Click **Add** in the **System DSN** tab in the ODBC Data Source Administrator window.
4. Select **IBM DB2 ODBC DRIVER** from the list.
5. Click **Finish**.
6. In the ODBC DB2 Driver - Add window, perform the following steps:
   a. Enter `ITM Warehouse` in **Data source name**.
   b. Enter `Warehous` in **Database Alias**.

      If the Tivoli Data Warehouse is located on a remote computer, ensure that the database alias matches the alias that you used when cataloging the remote data warehouse. See "Cataloging a remote data warehouse" on page 284.

      If local, ensure that the database alias matches the name used for the warehouse database.
   c. Click **OK**.
7. Test the ODBC database connection before continuing:
   a. In the ODBC Data Source Administrator window, select **ITM Warehouse**.
   b. Click **Configure**.
   c. In the CLI/ODBC Settings - ITM Warehouse window, you see the data source name, **ITM Warehouse**.
   d. Enter `ITMUser` for the **User ID**.
   e. Type a password for the user in the **Password** field. The default password is `itmpswd1`.
   f. Click **Connect**.
   g. A **Connection test successful** message is displayed.
   h. Click **OK**.
   i. Click **OK** to close the window.

Configuring a Warehouse Proxy agent on Windows (ODBC connection)

Use this procedure to configure a Warehouse Proxy agent on Windows to connect to a DB2 data warehouse:

1. Log on to the Windows system where the Warehouse Proxy agent is installed and begin the configuration:
   a. Click **Start → Programs → IBM Tivoli Monitoring → Manage Tivoli Monitoring Services**.

      The Manage Tivoli Enterprise Monitoring Services window is displayed.
   b. Right-click **Warehouse Proxy** and click **Configure Using Defaults**.

Click **Reconfigure** if the Warehouse Proxy is installed on the same computer as the portal server.

c. Click **OK** on the message regarding connection to a hub monitoring server.

2. The next two windows (entitled Warehouse Proxy: Agent Advanced Configuration) contain the settings for the connection between the Warehouse Proxy agent and the hub monitoring server. These settings were specified when the Warehouse Proxy agent was installed. Click **OK** on each window to accept the settings.
3. Click **Yes** on the message asking if you want to configure the ODBC data source.
4. Select **DB2** from the list of databases and click **OK**.

   The following configuration window is displayed.

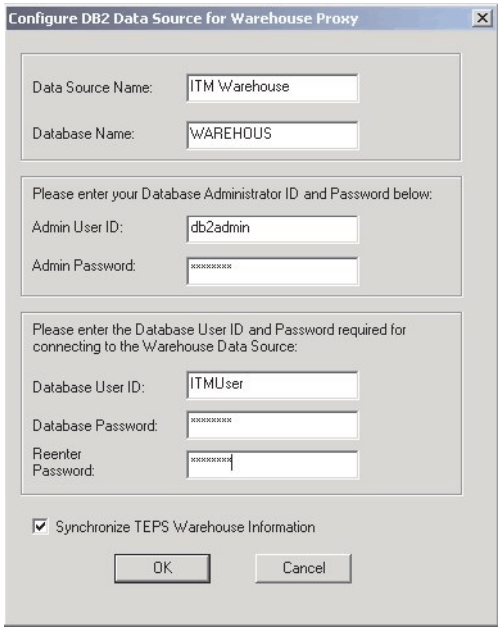


Figure 40. Configure DB2 Data Source for Warehouse Proxy window

5. Click **OK** to accept all default information on this window, or change one or more default values and then click **OK**. The fields on this window are described in Table 76.

   Note: The values for the data source name, database name, and database user ID and password must match the values that you used when configuring an ODBC connection for the Warehouse Proxy agent. (See "Configuring an ODBC data source for a DB2 data warehouse" on page 285.)

Table 76. Configuration information for the Tivoli Data Warehouse database on DB2

Field	Default value	Description
Data Source Name	ITM Warehouse	The name of the data source.

Table 76. Configuration information for the Tivoli Data Warehouse database on DB2 (continued)

Field	Default value	Description
Database Name	WAREHOUS	The name of the database. If the Warehouse Proxy agent is not installed on the same computer as the Tivoli Data Warehouse, this value must match the name of the database alias you used when cataloging the remote data warehouse. (See "Cataloging a remote data warehouse" on page 284.)
Admin User ID	db2admin	The database administrator ID.
Admin Password	(no default)	The password for the database administrator.
Database User ID	ITMUser	The name of the Windows OS user that the Warehouse Proxy agent will use to access the Tivoli Data Warehouse database.
Database Password	itmpswd1	The password for the Windows OS user. If your environment requires complex passwords (passwords that require both alpha and numeric characters), specify a password that complies with these requirements.
Reenter Password	itmpswd1	Confirm the password by entering it again.
Synchronize TEPS Warehouse Information	yes	This check box is used only if you are re-configuring a Warehouse Proxy agent that is installed on the same Windows computer as the portal server. If this check box is selected, any change that you make to the connection information on this window for the Warehouse Proxy is automatically applied to the portal server.

6. Click **OK**.

Configuring a Warehouse Proxy agent on Linux or AIX (JDBC connection)

Use this procedure to configure a Warehouse Proxy agent on Linux or AIX to connect to a DB2 Tivoli Data Warehouse on any operating system:

1. Log on to the computer where the Warehouse Proxy agent is installed and begin the configuration.
   a. Change to the *install_dir*/bin directory and run the following command:
      ```
      ./itmcmd manage [-h install_dir]
      ```
      where *install_dir* is the installation directory for IBM Tivoli Monitoring. The default installation directory is /opt/IBM/ITM.
      The Manage Tivoli Enterprise Monitoring Services window is displayed.
   b. Right-click **Warehouse Proxy** and click **Configure**.
      The Configure Warehouse Proxy window is displayed.

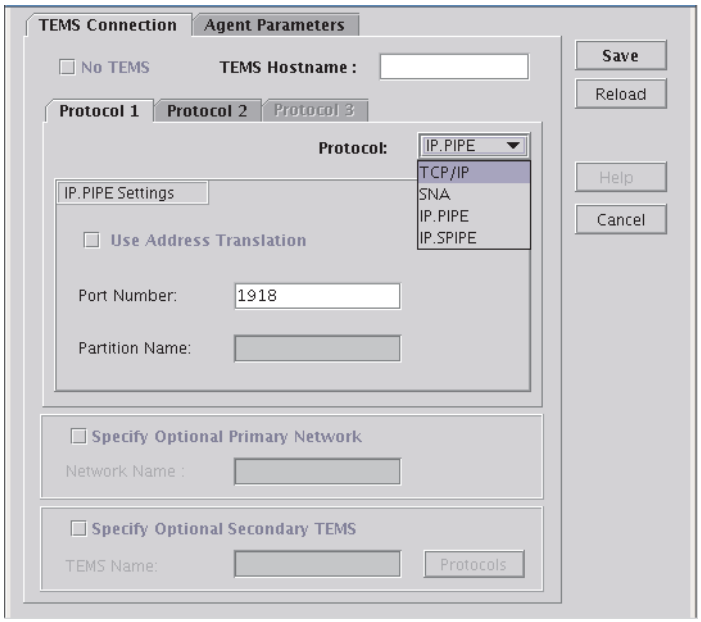


Figure 41. Configure Warehouse Proxy window (TEMS Connection tab)

2. On the **TEMS Connection** tab, review the settings for the connection between the Warehouse Proxy agent and the hub monitoring server. Correct the settings if necessary.

   The Warehouse Proxy agent must use the same protocols used by the application agents and by the hub monitoring. If the proxy agent does not have the same protocol as the hub monitoring server, it cannot register with the hub. If the proxy does not have the same protocol as the application agents, then the application agents cannot communicate with the proxy when they to try create a route to it.
3. Click the **Agent Parameters** tab.

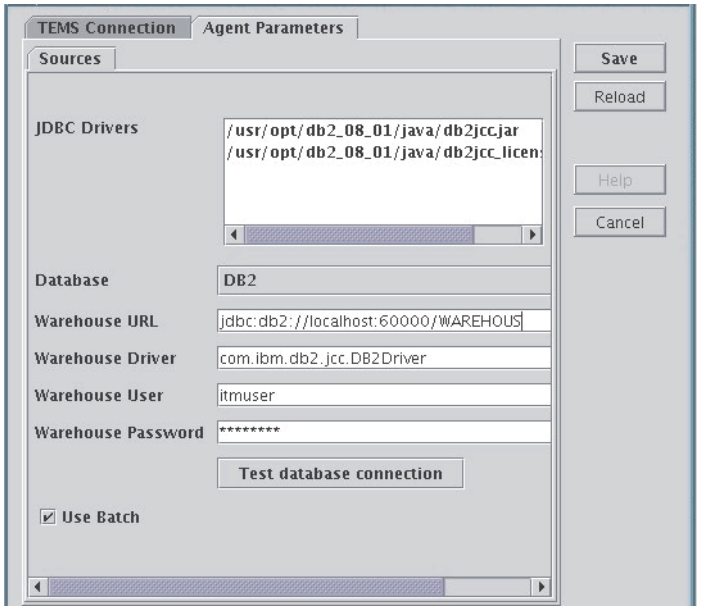


Figure 42. Configure Warehouse Proxy window (Agent Parameters tab)

4. In the **Database** drop-down list, select **DB2**.
5. Add the names and directory locations of the JDBC driver JAR files to the **JDBC Drivers** list box:
   a. Use the scroll bar at the bottom of the window to display the **Add** and **Delete** buttons, which are located to the right of the **JDBC Drivers** list box.
   b. Click **Add** to display the file browser window. Navigate to the location of the driver files on this computer and select the following driver files:

      db2jcc.jar
      db2jcc_license_cu.jar
   c. Click **OK** to close the browser window and add the JDBC driver files to the list.

   If you need to delete an entry from the list, select the entry and click **Delete**.
6. Change the default value displayed in the **Warehouse URL** field if it is not correct. The default Tivoli Data Warehouse URL for IBM DB2 is as follows:

   jdbc:db2://localhost:60000/WAREHOUS
   - If the Tivoli Data Warehouse is installed on a remote computer, specify the host name of the remote computer instead of `localhost`.
   - Change the port number if it is different.
   - If the name of the Tivoli Data Warehouse database is not WAREHOUS, replace WAREHOUS with the actual name. (See "Creating the warehouse database on DB2" on page 278.)
7. Verify the JDBC driver name, which is displayed in the **Warehouse Driver** field. (Note that the **Warehouse Driver** field displays the *driver name*, in contrast to the *driver JAR files* that are listed in the **JDBC Drivers** field.)

   The DB2 JDBC driver name is as follows:

   com.ibm.db2.jcc.DB2Driver
8. If necessary, change the entries in the **Warehouse User** and **Warehouse Password** fields to match the user name and password that were created for the Tivoli Data Warehouse. (See "Creating the warehouse database on DB2" on page 278.) The default user name is `itmuser` and the default password is `itmpswd1`.
9. Check the **Use Batch** check box if you want the Warehouse Proxy agent to submit multiple execute statements to the Tivoli Data Warehouse database for processing as a batch.

   In some situations, such as crossing a network, sending multiple statements as a unit is more efficient than sending each statement separately. Batch processing is one of the features provided with the JDBC 2.0 API.
10. Click **Test database connection** to ensure you can communicate with the Tivoli Data Warehouse database.
11. Click **Save** to save your settings and close the window.

Starting the Warehouse Proxy

- To start the Warehouse Proxy agent from the Manage Tivoli Enterprise Services window, right-click **Warehouse Proxy** and select **Start**.
- (*Linux or AIX only*) To start the Warehouse Proxy agent from the command line, run the following command from the bin directory of the IBM Tivoli Monitoring installation directory. The default installation directory is /opt/IBM/ITM.

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

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

Step 3: Configure communications between the Tivoli Enterprise Portal Server and the data warehouse

Complete the tasks described in the following table, in the order listed, to configure communications between the portal server and the data warehouse.

Table 77. Tasks for configuring communications between the portal server and a DB2 data warehouse

Task	Procedure
(*Portal server on Windows only*) If the *portal server database* was created on Microsoft SQL Server, install a DB2 database client on the portal server. If the portal server database was created on DB2, the DB2 client already exists on the portal server.	Refer to the DB2 documentation for instructions on how to install a DB2 client.
On the computer where the portal server is installed, catalog the remote data warehouse. You must perform this step before configuring the portal server to connect to the data warehouse. (See the next row.) Cataloging the remote data warehouse enables communications between the DB2 client on the portal server and the remote DB2 server where the data warehouse is located. Complete this task regardless of which platforms are used by the portal server or the data warehouse.	"Cataloging a remote data warehouse" on page 284
Configure the portal server to connect to the data warehouse. The configuration procedure on Windows automatically configures an ODBC connection to the data warehouse.	For a portal server on Windows, see "Configuring a Windows portal server (ODBC connection)." For a portal server on Linux or AIX, see "Configuring a Linux or AIX portal server (DB2 CLI connection)" on page 294.
Restart the portal server.	"Starting the portal server" on page 295
Test the connection between the portal server and the Tivoli Data Warehouse by creating a customized query in the Tivoli Enterprise Portal.	"Testing the connection between the portal server and the Tivoli Data Warehouse" on page 351

Configuring a Windows portal server (ODBC connection)

The procedure described in this section uses the Manage Tivoli Enterprise Services window to configure an ODBC connection between a Windows portal server and the data warehouse. You do not need to configure the ODBC data source through the Control Panel in Windows.

Before you begin

Catalog the remote warehouse database before you configure the Windows portal server to connect to the database. See "Cataloging a remote data warehouse" on page 284. The ODBC connection does not work if the remote database has not been cataloged prior to performing this procedure.

Procedure

Complete the following procedure to configure a portal server on Windows to connect to a DB2 data warehouse:

1. Log on to the Windows system where the portal server is installed and begin the configuration:
   a. Click **Start → Programs → IBM Tivoli Monitoring → Manage Tivoli Monitoring Services**.

The Manage Tivoli Enterprise Monitoring Services window is displayed.

b. Right-click **Tivoli Enterprise Portal Server** and click **Reconfigure**.

2. The next two windows (entitled TEP Server Configuration) contain the settings for the connection between the portal server and the hub monitoring server. These settings were specified when the portal server was installed. Click **OK** on each window to accept the settings.
3. Click **Yes** on the message asking if you want to reconfigure the warehouse information for the Tivoli Enterprise Portal Server.
4. Select **DB2** from the list of databases and click **OK**.

   The following configuration window is displayed.

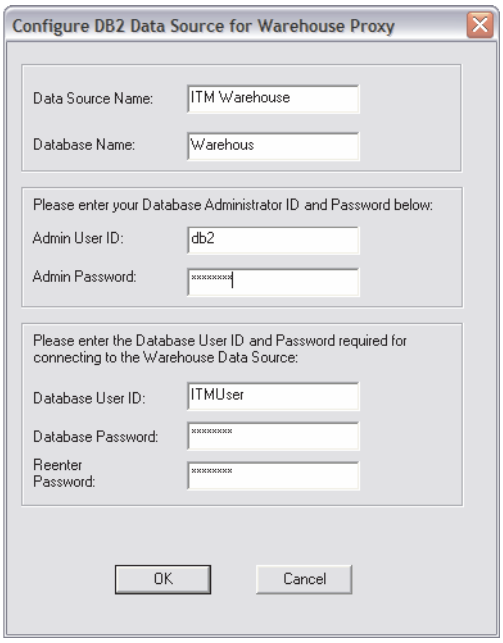


Figure 43. Configure DB2 Data Source for Warehouse Proxy window

5. Click **OK** to accept all default information on this window, or change one or more default values and then click **OK**. The fields on this window are described in the following table.

Table 78. Configuration information for the Tivoli Data Warehouse database on DB2

Field	Default value	Description
Data Source Name	ITM Warehouse	The name of the data source.
Database Name	WAREHOUS	The name of the database. This value must match the name of the database alias you used when cataloging the remote Tivoli Data Warehouse on the portal server. (See "Cataloging a remote data warehouse" on page 284.)
Admin User ID	db2admin	The database administrator ID.
Admin Password	(no default)	The password for the database administrator.

Table 78. Configuration information for the Tivoli Data Warehouse database on DB2 (continued)

Field	Default value	Description
Database User ID	ITMUser	The name of the Windows OS user that the portal server will use to access the Tivoli Data Warehouse database.
Database Password	itmpswd1	The password for the Windows user. If your environment requires complex passwords (passwords that require both alpha and numeric characters), specify a password that complies with these requirements.
Reenter Password	itmpswd1	Confirm the password by entering it again.

6. Click **OK**.

Configuring a Linux or AIX portal server (DB2 CLI connection)

Use this procedure to configure a portal server on Linux or AIX to connect to a DB2 Tivoli Data Warehouse on any operating system.

1. Log on to the computer where the Tivoli Enterprise Portal Server is installed and begin the configuration.
   a. Change to the *install_dir*/bin directory and run the following command:
      ```
      ./itmcmd manage [-h install_dir]
      ```
      where *install_dir* is the installation directory for IBM Tivoli Monitoring. The default installation directory is /opt/IBM/ITM.

      The Manage Tivoli Enterprise Monitoring Services window is displayed.
   b. Right-click **Tivoli Enterprise Portal Server** and click **Configure**.

      The Configure Tivoli Enterprise Portal Server window is displayed.
2. On the **TEMS Connection** tab, review the settings for the connection between the portal server and the hub monitoring server. These settings were specified when the portal server was installed.
3. Click the **Agent Parameters** tab.
4. Select the **DB2** radio button.

   The fields for configuring the connection to a DB2 data warehouse are displayed at the bottom of the window.

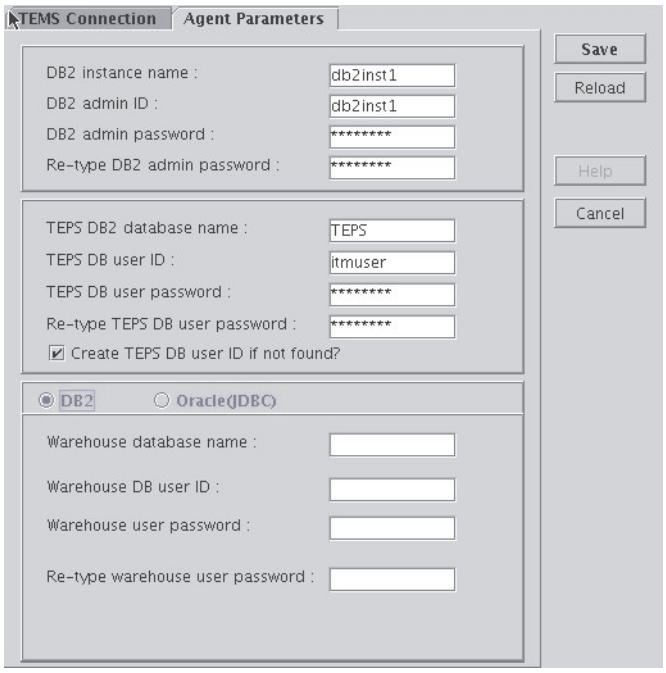


Figure 44. Configuring the connection to a DB2 data warehouse

5. Enter information in the fields described in the following table:

Table 79. Configuration information for the Tivoli Data Warehouse database on DB2

Field	Default value	Description
Warehouse database name	WAREHOUS	The name of the Tivoli Data Warehouse database.
Warehouse database user ID	itmuser	The login name of the database user that the portal server will use to access the Tivoli Data Warehouse database.
Warehouse user password	itmpswd1	The password for the database login user. If your environment requires complex passwords (passwords that require both alpha and numeric characters), specify a password that complies with these requirements.
Re-type warehouse user password	itmpswd1	Confirm the password by entering it again.

6. Click **Save** to save your settings and close the window.

Starting the portal server

Use the following steps to start the portal server:

- To start the portal server from the Manage Tivoli Enterprise Services window, right-click **Tivoli Enterprise Portal Server** and select **Start**.
- (*Linux or AIX only*) To start the portal server from the command line, run the following command from the bin directory of the IBM Tivoli Monitoring installation directory. The default installation directory is /opt/IBM/ITM.

  ```
  ./itmcmd agent start cq
  ```

where cq is the product code for the portal server.

Step 4: Install and configure communications for the Summarization and Pruning agent

Complete the tasks described in the following table, in the order listed, to install and configure the Summarization and Pruning agent.

Table 80. Tasks for installing and configuring communications for the Summarization and Pruning agent

Task	Procedure
Install the Summarization and Pruning agent if you have not already installed it. For best performance, install the Summarization and Pruning agent on the same computer as the data warehouse. The installation procedure for Windows includes steps for configuring the connection between the agent and the hub Tivoli Enterprise Monitoring server. On Linux or AIX, this step is performed in a separate configuration procedure (*Configuring the monitoring agent*). See the information at right. Be sure to perform all referenced installation and configuration procedures. **Note**: The Summarization and Pruning agent is not automatically started after installation. Do not complete any step or procedure for starting the agent at this point.	To install a Summarization and Pruning agent on Windows, complete the procedure "Windows: Installing a monitoring agent" on page 149. To install a Summarization and Pruning agent on Linux or UNIX, complete the procedure "Linux or UNIX: Installing a monitoring agent" on page 152, including the following subsections: • *Installing the monitoring agent* • *Configuring the monitoring agent* • *Changing the file permissions for agents* (if you used a non-root user to install the Warehouse Proxy) *Do not complete the procedure for starting the agent*.
If the data warehouse is located on a remote computer, copy the *DB2 UDB JDBC Universal Driver* (Type 4 driver) JAR files, included with the DB2 product installation, to the local computer where the Summarization and Pruning agent is installed. You can copy the files to any directory that the user that the Summarization and Pruning agent process runs as has access to.	The Type 4 driver file names and locations are as follows: <*db2installdir*>/java/db2jcc.jar <*db2installdir*>/java/db2jcc_license_cu.jar where <*db2installdir*> is the directory where DB2 was installed. The default DB2 Version 9 installation directory is as follows: • On Windows: C:\Program Files\IBM\SQLLIB • On AIX: /usr/opt/db2_09_01 • On Linux or Solaris: /opt/IBM/db2/V9.1
Configure the Summarization and Pruning agent. When you configure the Summarization and Pruning agent, you configure the connection to the Tivoli Data Warehouse and you specify settings that control the operation of the Summarization and Pruning agent. Perform this procedure whether or not the Summarization and Pruning agent and the warehouse database are installed on the same computer.	"Configuring the Summarization and Pruning agent (JDBC connection)" on page 337
Configure history collection. When you configure history collection, you specify settings for how often to collect, aggregate, and prune data for individual monitoring agents and attribute groups. Configure history collection from the Tivoli Enterprise Portal.	See the *IBM Tivoli Monitoring Administrator's Guide* for instructions on how to configure history collection.

Table 80. Tasks for installing and configuring communications for the Summarization and Pruning agent (continued)

Task	Procedure
Start the Summarization and Pruning agent.	"Starting the Summarization and Pruning agent" on page 347

Chapter 14. Tivoli Data Warehouse solution using Microsoft SQL Server

Use the information and instructions in this chapter to implement a Tivoli Data Warehouse solution using Microsoft SQL Server for the warehouse database. The following table lists the goals for achieving a Microsoft SQL solution.

Table 81. Goals for achieving a Tivoli Data Warehouse solution using Microsoft SQL Server

Goal	Where to find information
Review your options, specific to a Microsoft SQL solution, for operating system platforms and communications between warehousing components.	"Supported components"
Install prerequisite software before implementing your Tivoli Data Warehouse solution.	"Prerequisite installation" on page 301
Understand how to use the instructions for implementing your Tivoli Data Warehouse solution.	"Implementing a Tivoli Data Warehouse solution using Microsoft SQL Server" on page 302
Complete the steps for implementing your Tivoli Data Warehouse solution using Microsoft SQL Server for the data warehouse.	"Step 1: Create the Tivoli Data Warehouse database" on page 304 "Step 2: Install and configure communications for the Warehouse Proxy agent" on page 305 "Step 3: Configure communications between the Tivoli Enterprise Portal Server and the data warehouse" on page 312 "Step 4: Install and configure communications for the Summarization and Pruning agent" on page 314

Supported components

Figure 45 on page 300 presents the options for a Tivoli Data Warehouse solution using Microsoft SQL Server for the warehouse database. The diagram summarizes the supported operating system platforms for the various warehousing components, the supported database products, and the connections between components. For more specific information about supported operating systems and database products, including product names and versions, see "Hardware and software requirements" on page 70.

© Copyright IBM Corp. 2005, 2007

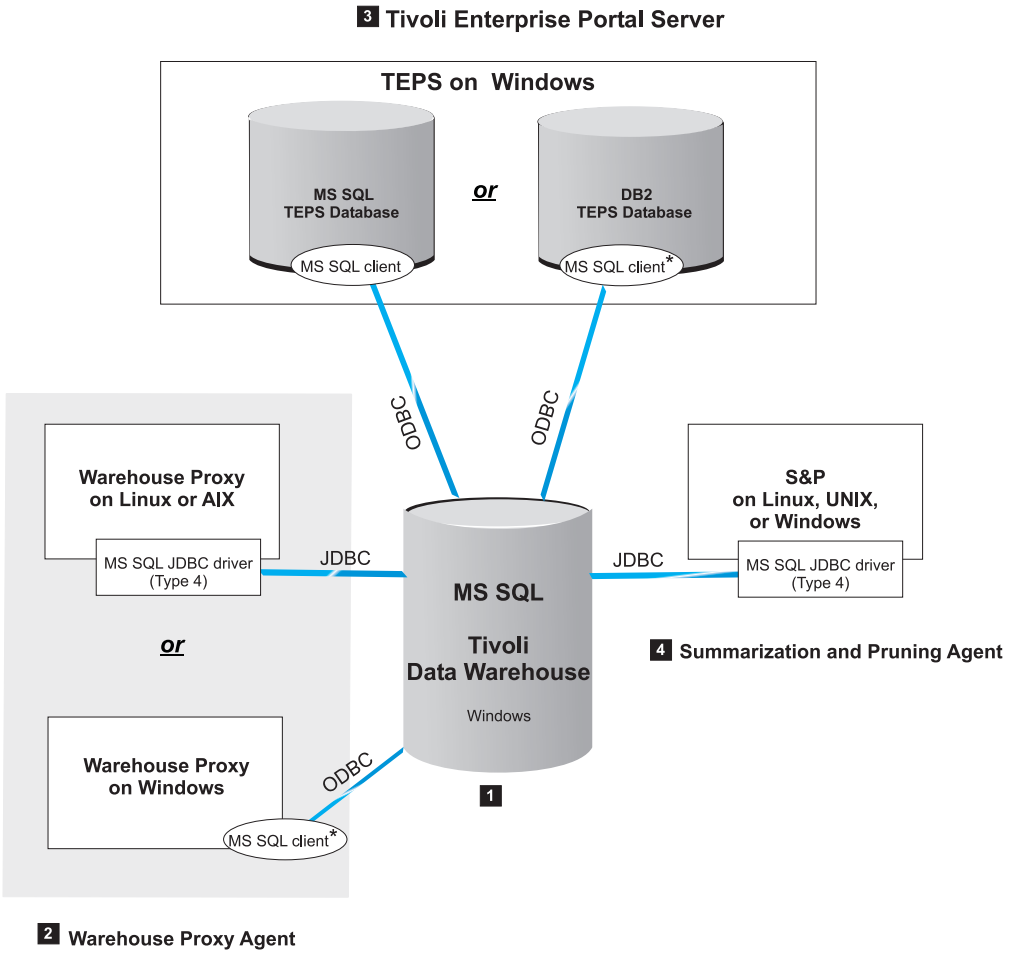


Figure 45. Tivoli Data Warehouse solution using Microsoft SQL Server

Note: An asterisk (*) next to a database client indicates that you must manually install the client if it does not already exist.

In the following discussion, numbered product components correspond to the numbers on the diagram.

1 Tivoli Data Warehouse on Microsoft SQL Server

A Tivoli Data Warehouse database on Microsoft SQL Server can be installed on supported Windows platforms.

2 Warehouse Proxy Agent

A Warehouse Proxy agent on Linux or AIX communicates with the warehouse database through a JDBC connection. Install a Microsoft SQL Type 4 driver on the computer where the Warehouse Proxy is located.

Important: Use the 2005 SQL driver even if you are connecting to a warehouse database that was created in Microsoft SQL Server 2000.

A Warehouse Proxy agent on Windows communicates with the warehouse database through an ODBC connection. The ODBC driver is included with the Microsoft SQL Server client. If the Tivoli Data Warehouse is located on a remote

computer, install a Microsoft SQL Server client on the local computer where the Warehouse Proxy agent is located. Also, configure a remote client connection to the Tivoli Data Warehouse.

3 Tivoli Enterprise Portal Server

A Tivoli Enterprise Portal Server on Windows can connect to a Microsoft SQL Server data warehouse through a Microsoft SQL Server client installed on the portal server. If the *portal server database* (designated as *TEPS database* in the diagram) uses Microsoft SQL Server, the client already exists. *Manually* install a Microsoft SQL Server client on the portal server only if the portal server database uses DB2.

The portal server communicates with the warehouse database through an ODBC connection. The ODBC driver is included with the Microsoft SQL Server client. Configure a remote client connection to the Tivoli Data Warehouse.

4 Summarization and Pruning Agent

The Summarization and Pruning agent communicates with the warehouse database through a JDBC connection from any supported operating system. Install a Microsoft SQL Type 4 JDBC driver on the computer where the Summarization and Pruning agent is located.

Important: Use the 2005 SQL driver even if you are connecting to a warehouse database that was created in Microsoft SQL Server 2000.

Prerequisite installation

Before you implement your Tivoli Data Warehouse solution, complete one or more hub installations, *excluding the warehousing components*. Include the following components in each hub installation:

- The hub Tivoli Enterprise Monitoring Server
- *(Optional)* One or more remote monitoring servers
- The Tivoli Enterprise Portal Server, including the prerequisite RDBMS for the portal server database (DB2 or Microsoft SQL Server)
- A Microsoft SQL server instance on the computer where you will create the Tivoli Data Warehouse database. (The Tivoli Data Warehouse database can be shared in a multi-hub installation or dedicated to a single hub.) The SQL Server instance must be patched to the current service pack level.
- *(Optional)* A portal desktop client
- *(Optional)* Monitoring agents, and the application support for the monitoring agents

  Note: The term *monitoring agent*, as used here, refers to agents that collect data directly from managed systems, not the Warehouse Proxy agent or Summarization and Pruning agent.
- *(Optional)* Language packs for all languages other than English

Refer to the following table for related information:

Table 82. Information topics related to installation of prerequisite software for a Tivoli Data Warehouse solution

Topic	Where to find information
Single and multiple hub installations	To understand the terminology related to single and multiple hub installations, see "Scenarios for small, medium, and large environments" on page 27.
Installation procedures for prerequisite components	The detailed instructions for installing the prerequisite components are described in Chapter 6, "Installing IBM Tivoli Monitoring," on page 113. Refer to your database documentations for instructions on how to install a supported database server.
Supported RDBMS versions	For specific information about the supported database platforms for the portal server database and the Tivoli Data Warehouse, see "Hardware and software requirements" on page 70.

Implementing a Tivoli Data Warehouse solution using Microsoft SQL Server

Use the instructions in the remainder of this chapter to implement a Tivoli Data Warehouse solution using Microsoft SQL Server for the data warehouse.

Assumptions

The implementation instructions are based on the following assumptions:

- You will create the Tivoli Data Warehouse database on a different computer from the Tivoli Enterprise Portal Server.
- You will create a single Tivoli Data Warehouse database, to be used either within a single hub installation or to be shared in a multi-hub installation. If you have multiple independent hub installations, repeat the implementation steps for each hub installation. (See "Scenarios for small, medium, and large environments" on page 27 for information about hub installations.)
- No assumption is made about where you will install the Warehouse Proxy agent and Summarization and Pruning agent. Either of these agents may be installed on the same computer as the Tivoli Data Warehouse or on a different computer.

Solution steps

To implement your Tivoli Data Warehouse solution using Microsoft SQL Server, complete the four major steps described in the remaining sections of this chapter, in the order listed:

1. Create the Tivoli Data Warehouse database.
2. Install and configure communications for the Warehouse Proxy agent.
3. Configure communications between the Tivoli Enterprise Portal Server and the data warehouse.
4. Install and configure communications for the Summarization and Pruning agent.

Except for Step 1, each major step consists of a series of installation and configuration tasks, listed and described in a table. Use the step tables as a road map for implementing your solution. The step tables describe the tasks at a high

level, account for variations among configuration options (such as which operating system is used for a component), and reference the appropriate sections for detailed implementation procedures. To implement your solution successfully:

- Perform the tasks in the order listed in the table.
- Do not skip a table to the procedures that follow it.

  Be aware that some of the implementation procedures referenced in a table are included in this chapter and some are documented elsewhere. In some cases, the task is described in the table, without referencing a separate procedure. Read and follow all instructions in the tables.

Step 1: Create the Tivoli Data Warehouse database

This section provides guidelines for creating the Tivoli Data Warehouse database using Microsoft SQL Server 2000 and 2005. For specific instructions on how to create a Microsoft SQL Server database, refer to the Microsoft SQL Server documentation or have a database administrator create the database for you.

When you create the warehouse database using Microsoft SQL Server, follow these guidelines:

- Connect to the Microsoft SQL database server and create the Tivoli Data Warehouse database using the system administrator (sa) user.
- Create a database user login name and password that the warehousing components (portal server, Warehouse Proxy agent, and Summarization and Pruning agent) can use to access the data warehouse. In these instructions, this user account is referred to as the *warehouse user*.

  You can create the warehouse user with either Windows authentication or SQL Server authentication. If you choose Windows authentication, the user must not belong to the Administrators group.

  Note: The warehousing components must *not* use the system administrator (sa) user to connect to the data warehouse.
- Consider using the default values shown in the following table for the warehouse name and warehouse user. The default values are used in the configuration procedures for connecting the warehousing components to the warehouse database.

Table 83. Default values for Tivoli Data Warehouse parameters

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

- Give the warehouse user public and db_owner privileges to the Tivoli Data Warehouse database.
- For Microsoft SQL Server 2005, do the following:
  - Create a schema with the same name (and owner) as the database user login name (for example, `ITMUser`) and change the default schema for the user from `dbo` to this login name. (This step is not necessary if you are using Microsoft SQL Server 2000.)
  - Make sure the database is set up to support inbound network TCP/IP connections.

Step 2: Install and configure communications for the Warehouse Proxy agent

You can install one or more Warehouse Proxy agents to collect and send historical data to the Tivoli Data Warehouse database. Complete the tasks described in the following table, in the order listed, to install and configure each Warehouse Proxy agent.

Table 84. Tasks for installing and configuring communications for the Warehouse Proxy agent

Task	Procedure
Install one or more Warehouse Proxy agents. If you want to install a Summarization and Pruning agent on the same computer as one of the Warehouse Proxy agents, use the referenced procedures to install both agents at the same time. If you are installing more than one Warehouse Proxy agent, each agent must be installed on a separate computer. The installation procedure for Windows includes steps for configuring the connection between the Warehouse Proxy and the hub Tivoli Enterprise Monitoring server. On Linux or AIX, this step is performed in a separate configuration procedure (*Configuring the monitoring agent*). See the information at right. Be sure to perform all of the referenced installation and configuration procedures.	To install a Warehouse Proxy agent on Windows, complete the procedure "Windows: Installing a monitoring agent" on page 149. To install a Warehouse Proxy agent on Linux or AIX, complete the procedure "Linux or UNIX: Installing a monitoring agent" on page 152, including the following subsections: • *Installing the monitoring agent* • *Configuring the monitoring agent* • *Changing the file permissions for agents* (if you used a non-root user to install the Warehouse Proxy) *Do not complete the procedure for starting the agent*.
(*Warehouse Proxy agent on Windows only*) • Install a Microsoft SQL Server client on the computer where the Warehouse Proxy agent is installed if *both* of the following statements are true: – The Warehouse Proxy is installed on Windows, and – The Warehouse Proxy needs to connect to a remote data warehouse. • Configure a remote client connection to the data warehouse server using Microsoft SQL Server tools.	Refer to the Microsoft SQL Server documentation for instructions on how to install a Microsoft SQL client and configure a remote client connection.
(*Warehouse Proxy agent on Windows only*) On the computer where the Warehouse Proxy agent is installed, configure an ODBC data source for the data warehouse. Perform this procedure whether or not the Warehouse Proxy agent and the warehouse database are installed on the same computer.	"Configuring an ODBC data source for a Microsoft SQL data warehouse" on page 306
(*Warehouse Proxy agent on Linux or AIX only*) Install the Microsoft SQL Server 2005 JDBC Driver (Type 4 driver) on the computer where the Warehouse Proxy agent is installed. Use the 2005 SQL JDBC driver even if you are connecting to a Microsoft SQL Server 2000 data warehouse.	Obtain the 2005 JDBC driver from the following Microsoft Web page: http://msdn.microsoft.com/data/jdbc/default.aspx Follow the instructions on the Microsoft download page for installing the driver. After you install the driver, the JAR file name and location are as follows: <*mssql2005installdir*>/sqljdbc_1.0/enu/sqljdbc.jar

Table 84. Tasks for installing and configuring communications for the Warehouse Proxy agent (continued)

Task	Procedure
Configure the Warehouse Proxy agent to connect to the data warehouse. Perform this procedure whether or not the Warehouse Proxy agent and the warehouse database are installed on the same computer.	For a Warehouse Proxy agent on Windows, see "Configuring a Warehouse Proxy agent on Windows (ODBC connection)" on page 307. For a Warehouse Proxy agent on Linux or AIX, see "Configuring a Warehouse Proxy agent on Linux or AIX (JDBC connection)" on page 309.
If you are installing more than one Warehouse Proxy agent within the same hub monitoring server installation, associate each Warehouse Proxy agent with a subset of monitoring servers (hub or remote) within the installation. Each Warehouse Proxy agent receives data from the monitoring agents that report to the monitoring servers on the list. Use the environment variable KHD_WAREHOUSE_TEMS_LIST to specify a list of monitoring servers to associate with a Warehouse Proxy agent.	For an example topology of multiple Warehouse Proxy agents within the same hub monitoring server installation, see Figure 5 on page 31 and the related discussion. For instructions about installing and configuring multiple Warehouse Proxy agents within a single hub monitoring server installation, see "Installing and configuring multiple Warehouse Proxy agents" on page 347.
(*Optional*) Customize the configuration of the Warehouse Proxy agent for tuning performance.	"Tuning the performance of the Warehouse Proxy" on page 354
Start the Warehouse Proxy agent.	"Starting the Warehouse Proxy agent" on page 311

Configuring an ODBC data source for a Microsoft SQL data warehouse

A Microsoft SQL client on Windows requires an ODBC connection to the data warehouse. For the Warehouse Proxy agent, you must configure the ODBC connection manually.

Complete the following procedure to set up an ODBC connection for a Warehouse Proxy agent on Windows to a local or remote Tivoli Data Warehouse.

Note: This procedure uses default values for the data source name and warehouse user ID. (Default values are used in configuration procedures for warehousing components.) Substitute different values if you do not want to use the default values.

1. Open the Control Panel.
2. Click **Administrative Tools → Data Sources (ODBC)**
3. Click **Add** in the **System DSN** tab in the ODBC Data Source Administrator window.
4. Select **SQL Server** and click **Finish**.
5. Enter `ITM Warehouse` in the **Name** field.
6. Select the Microsoft SQL server where the Tivoli Data Warehouse is located from the drop down list and click **Next**.
7. Select **With SQL Server authentication using a login ID and password entered by the user**.
8. Enter `ITMUser` for the **Login ID**.

The user ID must match exactly, including case, what was created in the SQL Server database if using database authentication or the ID that was created in the Windows OS. Mixing the case will cause tables to be created with dbo as the owner rather than ITMUser. This will cause many warehousing components to not work properly.

9. Type a password for the user in the **Password** field. The default password is `itmpswd1`.
10. Click **Next**.
11. Click **Next** again.
12. Click **Finish**.
13. Click **Test Data Source** to test the connection to the database.
14. Click **OK**.

Configuring a Warehouse Proxy agent on Windows (ODBC connection)

Use this procedure to configure a Warehouse Proxy agent on Windows to connect to a Tivoli Data Warehouse in Microsoft SQL Server:

1. Log on to the Windows system where the Warehouse Proxy agent is installed and begin the configuration:
   a. Click **Start** → **Programs** → **IBM Tivoli Monitoring** → **Manage Tivoli Monitoring Services**.

      The Manage Tivoli Enterprise Monitoring Services window is displayed.
   b. Right-click **Warehouse Proxy** and click **Configure Using Defaults**.

      Click **Reconfigure** if the Warehouse Proxy is installed on the same computer as the portal server.
   c. Click **OK** on the message regarding connection to a hub monitoring server.
2. The next two windows (entitled Warehouse Proxy: Agent Advanced Configuration) contain the settings for the connection between the Warehouse Proxy agent and the hub monitoring server. These settings were specified when the Warehouse Proxy agent was installed. Click **OK** on each window to accept the settings.
3. Click **Yes** on the message asking if you want to configure the ODBC data source.
4. Select **SQL Server** from the list of databases and click **OK**.

   The following configuration window is displayed.

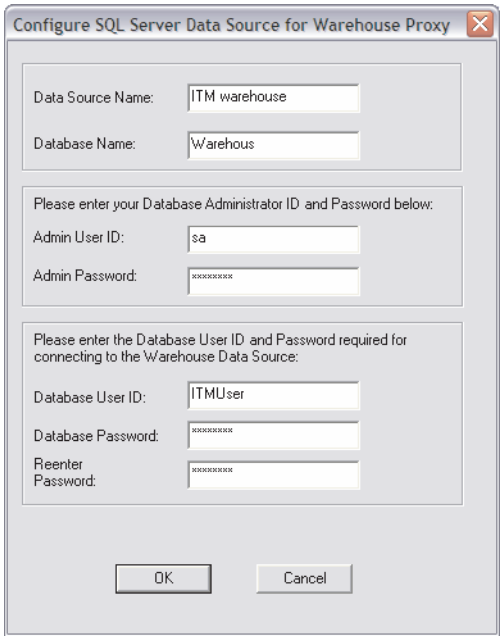


Figure 46. Configure SQL Data Source for Warehouse Proxy window

5. Click **OK** to accept all default information on this window, or change one or more default values and then click **OK**. The fields on this window are described in Table 85.

   Note: The values for the data source name, and database user ID and password must match the values that you used when configuring an ODBC connection for the Warehouse Proxy agent. (See "Configuring an ODBC data source for a Microsoft SQL data warehouse" on page 306.)

Table 85. Configuration information for the Tivoli Data Warehouse database on Microsoft SQL Server

Field	Default value	Description
Data Source Name	ITM Warehouse	The name of the data source.
Database Name	WAREHOUS	The name of the database.
Admin User ID	sa	The database administrator ID.
Admin Password	(no default)	The password for the database administrator.
Database User ID	ITMUser	The login name of the database user that the portal server will use to access the Tivoli Data Warehouse database. The user ID must match exactly, including case, what was created in the SQL Server database if using database authentication or the ID that was created in the Windows OS.
Database Password	itmpswd1	The password for the database login user. If your environment requires complex passwords (passwords that require both alpha and numeric characters), specify a password that complies with these requirements.

Table 85. Configuration information for the Tivoli Data Warehouse database on Microsoft SQL Server (continued)

Field	Default value	Description
Reenter Password	itmpswd1	Confirm the password by entering it again.
Synchronize TEPS Warehouse Information	yes	This check box is used only if you are re-configuring a Warehouse Proxy agent that is installed on the same Windows computer as the portal server. If this check box is selected, any change that you make to the connection information on this window for the Warehouse Proxy is automatically applied to the portal server.

6. Click **OK**.

Configuring a Warehouse Proxy agent on Linux or AIX (JDBC connection)

Use this procedure to configure a Warehouse Proxy agent on Linux or AIX to connect to a Microsoft SQL Server data warehouse:

1. Log on to the computer where the Warehouse Proxy agent is installed and begin the configuration.
   a. Change to the *install_dir*/bin directory and run the following command:
      `./itmcmd manage [-h install_dir]`

      where *install_dir* is the installation directory for IBM Tivoli Monitoring. The default installation directory is /opt/IBM/ITM.

      The Manage Tivoli Enterprise Monitoring Services window is displayed.
   b. Right-click **Warehouse Proxy** and click **Configure**.

      The Configure Warehouse Proxy window is displayed.

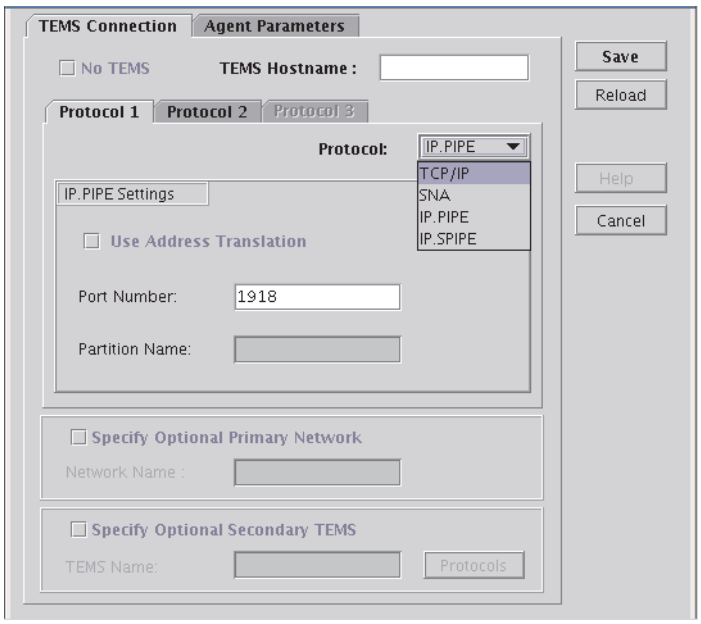


Figure 47. Configure Warehouse Proxy window (TEMS Connection tab)

2. On the **TEMS Connection** tab, review the settings for the connection between the Warehouse Proxy agent and the hub monitoring server.

   The Warehouse Proxy agent must use the same protocols used by the application agents and by the hub monitoring. If the proxy agent does not have the same protocol as the hub monitoring server, it cannot register with the hub. If the proxy does not have the same protocol as the application agents, then the application agents cannot communicate with the proxy when they to create a route to it.
3. Click the **Agent Parameters** tab.

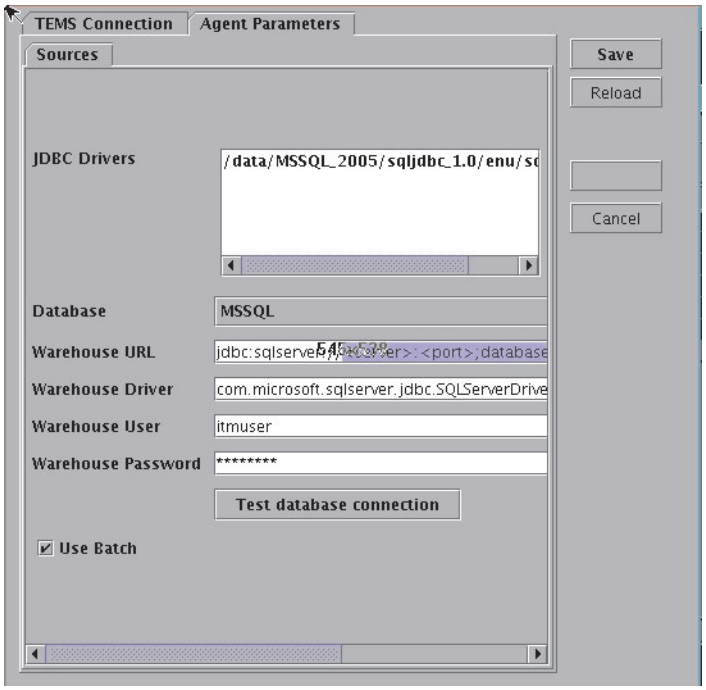


Figure 48. Configure Warehouse Proxy window (Agent Parameters tab)

4. In the **Database** drop-down list, select **MSSQL**.
5. Add the name and directory location of the JDBC driver JAR file to the **JDBC Drivers** list box:
   a. Use the scroll bar at the bottom of the window to display the **Add** and **Delete** buttons, which are located to the right of the **JDBC Drivers** list box.
   b. Click **Add** to display the file browser window. Navigate to the location of the JDBC driver JAR file on this computer and select the file. The Microsoft SQL Server 2005 driver JAR file name and default location after downloading from the Web are as follows:

      <mssql2005installdir>/sqljdbc_1.0/enu/sqljdbc.jar

      Important: Use the Microsoft SQL Server 2005 Driver even if you are connecting to a Microsoft SQL Server 2000 data warehouse.
   c. Click **OK** to close the browser window and add the driver file to the list.

   If you need to delete an entry from the list, select the entry and click **Delete**.
6. Change the default value displayed in the **Warehouse URL** field if it is not correct. The Warehouse URL for Microsoft SQL Server 2005 is as follows:

jdbc:sqlserver://localhost:1433;databaseName=WAREHOUS

- If the Tivoli Data Warehouse is installed on a remote computer, specify the host name of the remote computer instead of `localhost`.
- Change the port number if it is different.
- If the name of the Tivoli Data Warehouse database is not WAREHOUS, replace WAREHOUS with the actual name. (See Table 83 on page 304.)

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

   The Microsoft SQL Server 2005 Driver name is as follows:

   com.microsoft.sqlserver.jdbc.SQLServerDriver
8. If necessary, change the entries in the **Warehouse User** and **Warehouse Password** fields to match the user name and password that were created for the Tivoli Data Warehouse. (See "Step 1: Create the Tivoli Data Warehouse database" on page 304.) The default user name is `ITMUser` and the default password is `itmpswd1`.
9. Check the **Use Batch** check box if you want the Warehouse Proxy agent to submit multiple execute statements to the Tivoli Data Warehouse database for processing as a batch.

   In some situations, such as crossing a network, sending multiple statements as a unit is more efficient than sending each statement separately. Batch processing is one of the features provided with the JDBC 2.0 API.
10. Click **Test database connection** to ensure you can communicate with the Tivoli Data Warehouse database.
11. Click **Save** to save your settings and close the window.

Starting the Warehouse Proxy agent

Use the following steps to start the Warehouse Proxy agent:

- To start the Warehouse Proxy agent from the Manage Tivoli Enterprise Services window, right-click **Warehouse Proxy** and select **Start**.
- (*Linux or AIX only*) To start the Warehouse Proxy agent from the command line, run the following command from the bin directory of the IBM Tivoli Monitoring installation directory. The default installation directory is /opt/IBM/ITM.

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

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

Step 3: Configure communications between the Tivoli Enterprise Portal Server and the data warehouse

Complete the tasks described in the following table, in the order listed, to configure communications between the portal server and the data warehouse.

Table 86. Tasks for configuring communications between the portal server and a Microsoft SQL Server data warehouse

Task	Procedure
If the *portal server database* was created using DB2, install a Microsoft SQL Server database client on the portal server. If the portal server database was created using Microsoft SQL Server, the Microsoft SQL Server database client already exists on the portal server.	Refer to the Microsoft SQL Server documentation for instructions on how to install a Microsoft SQL Server database client.
Configure a remote client connection to the data warehouse server using Microsoft SQL Server tools.	Refer to the Microsoft SQL Server documentation for instructions on how to configure a remote client connection.
Configure the portal server to connect to the data warehouse. The configuration procedure automatically configures an ODBC connection to the data warehouse.	"Configuring the portal server (ODBC connection)"
Restart the portal server.	On the Manage Tivoli Enterprise Services window, right-click **Tivoli Enterprise Portal Server** and select **Start**.
Test the connection between the portal server and the Tivoli Data Warehouse by creating a customized query in the Tivoli Enterprise Portal.	"Testing the connection between the portal server and the Tivoli Data Warehouse" on page 351

Configuring the portal server (ODBC connection)

Use this procedure to configure the portal server to connect to a Tivoli Data Warehouse in Microsoft SQL Server:

1. Log on to the Windows system where the portal server is installed and begin the configuration:
   a. Click **Start** → **Programs** → **IBM Tivoli Monitoring** → **Manage Tivoli Monitoring Services**.

      The Manage Tivoli Enterprise Monitoring Services window is displayed.
   b. Right-click **Tivoli Enterprise Portal Server** and click **Reconfigure**.
2. The next two windows (entitled TEP Server Configuration) contain the settings for the connection between the portal server and the hub monitoring server. These settings were specified when the portal server was installed. Click **OK** on each window to accept the settings.
3. Click **Yes** on the message asking if you want to reconfigure the warehouse information for the Tivoli Enterprise Portal Server.
4. Select **SQL Server** from the list of databases and click **OK**.

   The following configuration window is displayed.

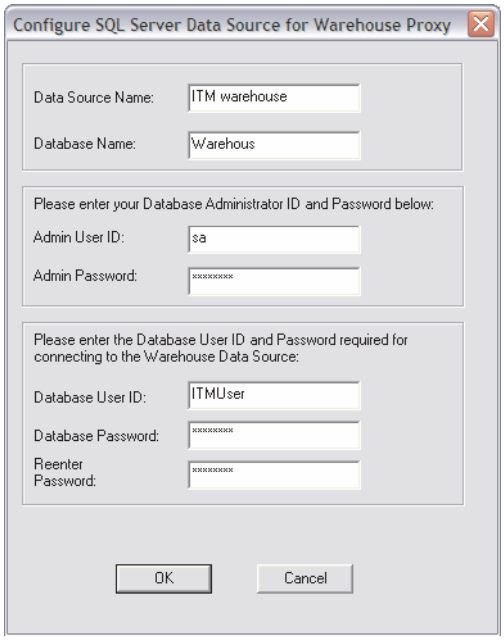


Figure 49. Configure SQL Data Source for Warehouse Proxy window

5. Click **OK** to accept all default information on this window, or change one or more default values and then click **OK**. The fields on this window are described in the following table:

Table 87. Configuration information for the Tivoli Data Warehouse database on Microsoft SQL Server

Field	Default value	Description
Data Source Name	ITM Warehouse	The name of the data source.
Database Name	WAREHOUS	The name of the database.
Admin User ID	sa	The database administrator ID.
Admin Password	(no default)	The password for the database administrator.
Database User ID	ITMUser	The login name of the database user that the portal server will use to access the Tivoli Data Warehouse database.
Database Password	(no default)	The password for the database login user. If your environment requires complex passwords (passwords that require both alpha and numeric characters), specify a password that complies with these requirements.
Reenter Password	(no default)	Confirm the password by entering it again.

6. Click **OK**.

Step 4: Install and configure communications for the Summarization and Pruning agent

Complete the tasks described in the following table, in the order listed, to install and configure the Summarization and Pruning agent.

Table 88. Tasks for installing and configuring communications for the Summarization and Pruning agent

Task	Procedure
Install the Summarization and Pruning agent if you have not already installed it. For best performance, install the Summarization and Pruning agent on the same computer as the data warehouse. The installation procedure for Windows includes steps for configuring the connection between the agent and the hub Tivoli Enterprise Monitoring server. On Linux or AIX, this step is performed in a separate configuration procedure (*Configuring the monitoring agent*). See the information at right. Be sure to perform all referenced installation and configuration procedures. **Note**: The Summarization and Pruning agent is not automatically started after installation. Do not complete any step or procedure for starting the agent at this point.	To install a Summarization and Pruning agent on Windows, complete the procedure "Windows: Installing a monitoring agent" on page 149. To install a Summarization and Pruning agent on Linux or UNIX, complete the procedure "Linux or UNIX: Installing a monitoring agent" on page 152, including the following subsections: • *Installing the monitoring agent* • *Configuring the monitoring agent* • *Changing the file permissions for agents* (if you used a non-root user to install the Warehouse Proxy) *Do not complete the procedure for starting the agent*.
Install the Microsoft SQL Server 2005 JDBC Driver (Type 4 driver) on the computer where the Summarization and Pruning agent is installed. Use the 2005 SQL JDBC driver even if you are connecting to a Microsoft SQL Server 2000 data warehouse.	Obtain the 2005 JDBC driver from the following Microsoft Web page: http://msdn.microsoft.com/data/jdbc/default.aspx Follow the instructions on the Microsoft download page for installing the driver. After you install the driver, the JAR file name and location are as follows: <*mssql2005installdir*>/sqljdbc_1.0/enu/sqljdbc.jar
Configure the Summarization and Pruning agent. When you configure the Summarization and Pruning agent, you configure the connection to the Tivoli Data Warehouse and you specify settings that control the operation of the Summarization and Pruning agent. Perform this procedure whether or not the Summarization and Pruning agent and the warehouse database are installed on the same computer.	"Configuring the Summarization and Pruning agent (JDBC connection)" on page 337
Configure history collection. When you configure history collection, you specify settings for how often to collect, aggregate, and prune data for individual monitoring agents and attribute groups. Configure history collection from the Tivoli Enterprise Portal.	See the *IBM Tivoli Monitoring Administrator's Guide* for instructions on how to configure history collection.
Start the Summarization and Pruning agent.	"Starting the Summarization and Pruning agent" on page 347

Chapter 15. Tivoli Data Warehouse solution using Oracle

Use the information and instructions in this chapter to implement a Tivoli Data Warehouse solution using Oracle for the warehouse database. The following table lists the goals for achieving an Oracle solution.

Table 89. Goals for achieving a Tivoli Data Warehouse solution using Oracle

Goal	Where to find information
Review your options, specific to an Oracle solution, for operating system platforms and communications between warehousing components.	"Supported components"
Install prerequisite software before implementing your Tivoli Data Warehouse solution.	"Prerequisite installation" on page 317
Understand how to use the instructions for implementing your Tivoli Data Warehouse solution.	"Implementing a Tivoli Data Warehouse solution using Oracle" on page 318
Complete the steps for implementing your Tivoli Data Warehouse solution using Oracle for the data warehouse.	"Step 1: Create the Tivoli Data Warehouse database" on page 320 "Step 2: Install and configure communications for the Warehouse Proxy agent" on page 322 "Step 3: Configure communications between the Tivoli Enterprise Portal Server and the data warehouse" on page 330 "Step 4: Install and configure communications for the Summarization and Pruning agent" on page 334

Supported components

Figure 50 on page 316 presents the options for a Tivoli Data Warehouse solution using Oracle for the warehouse database. The diagram summarizes the supported operating system platforms for the various warehousing components, the supported database products, and the connections between components. For more specific information about supported operating systems and database products, including product names and versions, see "Hardware and software requirements" on page 70.

© Copyright IBM Corp. 2005, 2007

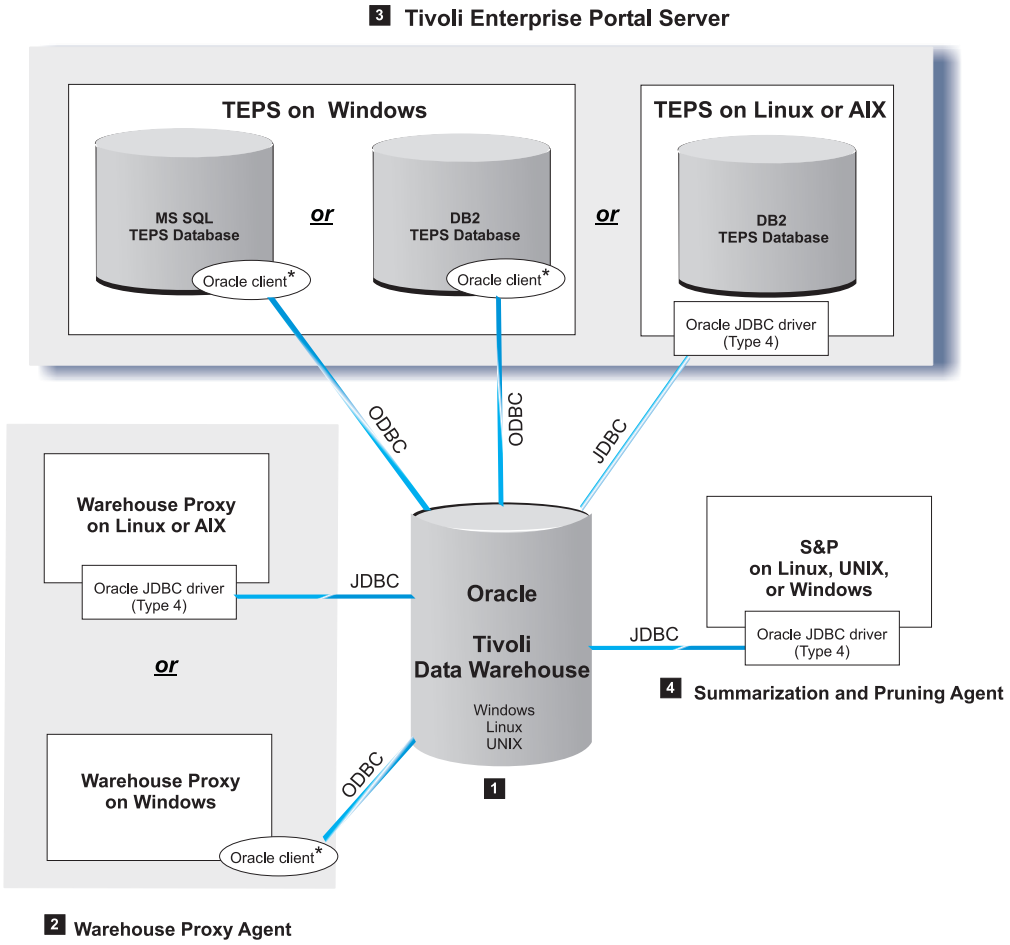


Figure 50. Tivoli Data Warehouse solution using Oracle

Note: An asterisk (*) next to a database client indicates that you must manually install the client if it does not already exist.

In the following discussion, numbered product components correspond to the numbers on the diagram.

1 Tivoli Data Warehouse on Oracle

A Tivoli Data Warehouse database on Oracle can be installed on supported Windows, Linux, or any UNIX platform support by Oracle. Ensure that the Oracle listener is active in order to accept connections from an Oracle client or JDBC driver.

2 Warehouse Proxy Agent

A Warehouse Proxy agent on Linux or AIX communicates with the warehouse database through a JDBC connection. Install an Oracle Type 4 JDBC driver on the computer where the Warehouse Proxy agent is located. If the Tivoli Data Warehouse is located on a remote computer, create a TNS (Transparent Network Substrate) Service Name on the local computer where the Warehouse Proxy agent is located.

A Warehouse Proxy agent on Windows communicates with the warehouse database through an ODBC connection. The ODBC driver is included with the Oracle client. If the Tivoli Data Warehouse is located on a remote computer, install an Oracle client on the local computer where the Warehouse Proxy agent is located. Also, create a TNS Service Name on the local computer.

3 Tivoli Enterprise Portal Server

A Tivoli Enterprise Portal Server on Windows communicates with an Oracle data warehouse through an Oracle database client using an ODBC connection. You must manually install the Oracle client on the portal server. The ODBC driver is included with the Oracle client.

A portal server on Linux or AIX communicates with the warehouse database through a JDBC connection. Install an Oracle Type 4 JDBC driver on the portal server.

4 Summarization and Pruning Agent

The Summarization and Pruning agent communicates with the warehouse database through a JDBC connection from any supported operating system. Install an Oracle Type 4 JDBC driver on the computer where the Summarization and Pruning agent is located.

Prerequisite installation

Before you implement your Tivoli Data Warehouse solution, complete one or more hub installations, *excluding the warehousing components*. Include the following components in each hub installation:

- The hub Tivoli Enterprise Monitoring Server
- *(Optional)* One or more remote monitoring servers
- The Tivoli Enterprise Portal Server, including the prerequisite RDBMS for the portal server database (DB2 or Microsoft SQL Server)
- An Oracle database server on the computer where you will create the Tivoli Data Warehouse database. (The Tivoli Data Warehouse database can be shared in a multi-hub installation or dedicated to a single hub.)
- *(Optional)* A portal desktop client
- *(Optional)* Monitoring agents, and the application support for the monitoring agents

  Note: The term *monitoring agent*, as used here, refers to agents that collect data directly from managed systems, not the Warehouse Proxy agent or Summarization and Pruning agent.
- *(Optional)* Language packs for all languages other than English

Refer to the following table for related information:

Table 90. Information topics related to installation of prerequisite software for a Tivoli Data Warehouse solution

Topic	Where to find information
Single and multiple hub installations	To understand the terminology related to single and multiple hub installations, see “Scenarios for small, medium, and large environments” on page 27.

Table 90. Information topics related to installation of prerequisite software for a Tivoli Data Warehouse solution (continued)

Topic	Where to find information
Installation procedures for prerequisite components	The detailed instructions for installing the prerequisite components are described in Chapter 6, "Installing IBM Tivoli Monitoring," on page 113. Refer to your database documentations for instructions on how to install a supported database server.
Supported RDBMS versions	For specific information about the supported database platforms for the portal server database and the Tivoli Data Warehouse, see "Hardware and software requirements" on page 70.

Implementing a Tivoli Data Warehouse solution using Oracle

Use the instructions in the remainder of this chapter to implement a Tivoli Data Warehouse solution using Oracle for the data warehouse.

Assumptions

The implementation instructions are based on the following assumptions:

- You will create the Tivoli Data Warehouse database on a different computer from the Tivoli Enterprise Portal Server.
- You will create a single Tivoli Data Warehouse database, to be used either within a single hub installation or to be shared in a multi-hub installation. If you have multiple independent hub installations, repeat the implementation steps for each hub installation. (See "Scenarios for small, medium, and large environments" on page 27 for information about hub installations.)
- No assumption is made about where you will install the Warehouse Proxy agent and Summarization and Pruning agent. Either of these agents may be installed on the same computer as the Tivoli Data Warehouse or on a different computer.

Solution steps

To implement your Tivoli Data Warehouse solution using Oracle, complete the four major steps described in the remaining sections of this chapter, in the order listed:

1. Create the Tivoli Data Warehouse database.
2. Install and configure communications for the Warehouse Proxy agent.
3. Configure communications between the Tivoli Enterprise Portal Server and the data warehouse.
4. Install and configure communications for the Summarization and Pruning agent.

Each major step consists of a series of installation and configuration tasks, listed and described in a table. Use the step tables as a road map for implementing your solution. The step tables describe the tasks at a high level, account for variations among configuration options (such as which operating system is used for a component), and reference the appropriate sections for detailed implementation procedures. To implement your solution successfully:

- Perform the tasks in the order listed in the table.
- Do not skip a table to the procedures that follow it.

Be aware that some of the implementation procedures referenced in a table are included in this chapter and some are documented elsewhere. In some cases, the task is described in the table, without referencing a separate procedure. Read and follow all instructions in the tables.

Step 1: Create the Tivoli Data Warehouse database

Complete the tasks described in the following table to create a Tivoli Data Warehouse database using Oracle and to make it accessible to clients.

Table 91. Tasks for creating the Tivoli Data Warehouse database

Task	Procedure
Create the Tivoli Data Warehouse database on one of the supported Windows, Linux, or UNIX operating systems. To comply with the assumptions described in the introduction to this chapter, create the database on a different computer from the Tivoli Enterprise Portal Server.	For guidance on planning the size and disk requirements for the warehouse database, see "Planning considerations for the Tivoli Data Warehouse" on page 19. For information about creating the warehouse database using Oracle, see "Creating the warehouse database on Oracle."
Activate the Oracle listener on the Oracle server where the Tivoli Data Warehouse is installed. To activate the Oracle listener: • Use the Oracle Listener Service on Windows. • Use the **lsnrctl start** command on Linux and UNIX.	Refer to the Oracle documentation for instructions on how to activate the Oracle listener.

Creating the warehouse database on Oracle

This section provides guidelines for creating the Tivoli Data Warehouse database on Oracle. For specific instructions on how to create an Oracle database, refer to the Oracle documentation or have a database administrator create the database for you.

When you create the warehouse database using Oracle, follow these guidelines:

- The character set should be the Unicode (AL32UTF8) when creating the database.
- Create a database user login name and password that the warehousing components (portal server, Warehouse Proxy agent, and Summarization and Pruning agent) can use to access the data warehouse. In these instructions, this user account is referred to as the *warehouse user*.
- Consider using the default values shown in the following table for the warehouse name and warehouse user. The default values are used in the configuration procedures for connecting the warehousing components to the warehouse database.

Table 92. Default values for Tivoli Data Warehouse parameters

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

- Create an ″ITM_DW″ role and give this role the following permissions:

  GRANT CREATE CONNECT TO ″ITM_DW″
  ALTER SESSION TO ″ITM_DW″
  CREATE SESSION TO ″ITM_DW″
  CREATE TABLE TO ″ITM_DW″
  CREATE ANY INDEX TO ″ITM_DW″
  CREATE ANY PROCEDURE TO ″ITM_DW″

CREATE VIEW TO ″ITM_DW″

After you create the warehouse user ID that will be used by the Warehouse Proxy and the Summarization and Pruning agents to connect to the Tivoli Data Warehouse database, give this user ID the role you just created. As all the Tivoli Data Warehouse tables are created in the user's default tablespace, you need to allocate enough space quota on the default tablespace to this user to create all the tables, or you can simplify it by allowing unlimited tablespace to this user.

- Activate the Oracle listener using the Oracle Listener Service on Windows or the **lsnrctl start** command on Linux and UNIX.

Step 2: Install and configure communications for the Warehouse Proxy agent

You can install one or more Warehouse Proxy agents to collect and send historical data to the Tivoli Data Warehouse database. Complete the tasks described in the following table, in the order listed, to install and configure each Warehouse Proxy agent.

Table 93. Tasks for installing and configuring communications for the Warehouse Proxy agent

Task	Procedure
Install one or more Warehouse Proxy agents. If you want to install a Summarization and Pruning agent on the same computer as one of the Warehouse Proxy agents, use the referenced procedures to install both agents at the same time. If you are installing more than one Warehouse Proxy agent, each agent must be installed on a separate computer. The installation procedure for Windows includes steps for configuring the connection between the agent and the hub Tivoli Enterprise Monitoring server. On Linux or AIX, this step is performed in a separate configuration procedure (*Configuring the monitoring agent*). See the information at right. Be sure to perform all referenced installation and configuration procedures.	To install a Warehouse Proxy agent on Windows, complete the procedure "Windows: Installing a monitoring agent" on page 149. To install a Warehouse Proxy agent on Linux or AIX, complete the procedure "Linux or UNIX: Installing a monitoring agent" on page 152, including the following subsections: • *Installing the monitoring agent* • *Configuring the monitoring agent* • *Changing the file permissions for agents* (if you used a non-root user to install the Warehouse Proxy) *Do not complete the procedure for starting the agent*.
(*Warehouse Proxy agent on Windows only*) • Install an Oracle client on the computer where the Warehouse Proxy agent is installed if *both* of the following statements are true: – The Warehouse Proxy is installed on Windows, and – The Warehouse Proxy needs to connect to a remote data warehouse. • Ensure that the the latest Oracle patches are installed. • Set the following system variable on the computer where the Warehouse Proxy agent is installed. Reboot the computer after setting the variable. The format of the NLS_LANG environment variable is: `NLS_LANG=`*`language_territory`*`.charset` The language and territory should be set to appropriate variables. For the United States this would be `NLS_LANG=AMERICAN_AMERICA.AL32UTF8`. Perform the last two tasks whether or not the warehouse database is local or remote.	Refer to the Oracle documentation for instructions on how to install an Oracle client. Obtain Oracle ODBC drivers from the following Web site: http://www.oracle.com/technology/software/tech/windows/odbc/htdocs/utilsoft.html
(*Warehouse Proxy agent on Windows only*) If the Tivoli Data Warehouse is located on a remote computer, create a TNS (Transparent Network Substrate) Service Name on the local computer where the Warehouse Proxy agent is located.	"Creating a TNS Service Name" on page 323

Table 93. Tasks for installing and configuring communications for the Warehouse Proxy agent (continued)

Task	Procedure
(*Warehouse Proxy agent on Windows only*) On the computer where the Warehouse Proxy agent is installed, configure an ODBC data source for the data warehouse, using the TNS Service Name that you created in the preceding step. Perform this procedure whether or not the Warehouse Proxy agent and the warehouse database are installed on the same computer.	"Configuring an ODBC data source for an Oracle data warehouse" on page 324
(*Warehouse Proxy agent on Linux or AIX only*) Install an Oracle Type 4 JDBC driver on the computer where the Warehouse Proxy agent is installed.	Obtain the Oracle JDBC Driver from the following Web site: http://www.oracle.com/technology/software/tech/java/sqlj_jdbc/index.html The Oracle JDBC driver JAR file name and location after installation is as follows: `<oracleinstalldir>/jdbc/lib/ojdbc14.jar` The ojdbc14.jar file supports JRE 1.5 or higher, the required Java Runtime Environment for IBM Tivoli Monitoring.
Configure the Warehouse Proxy agent to connect to the data warehouse. Perform this procedure whether or not the Warehouse Proxy agent and the warehouse database are installed on the same computer.	For a Warehouse Proxy agent on Windows, see "Configuring a Warehouse Proxy agent on Windows (ODBC connection)" on page 325. For a Warehouse Proxy agent on Linux or AIX, see "Configuring a Warehouse Proxy agent on Linux or AIX (JDBC connection)" on page 326.
If you are installing more than one Warehouse Proxy agent within the same hub monitoring server installation, associate each Warehouse Proxy agent with a subset of monitoring servers (hub or remote) within the installation. Each Warehouse Proxy agent receives data from the monitoring agents that report to the monitoring servers on the list. Use the environment variable KHD_WAREHOUSE_TEMS_LIST to specify a list of monitoring servers to associate with a Warehouse Proxy agent.	For an example topology of multiple Warehouse Proxy agents within the same hub monitoring server installation, see Figure 5 on page 31 and the related discussion. For instructions about installing and configuring multiple Warehouse Proxy agents within a single hub monitoring server installation, see "Installing and configuring multiple Warehouse Proxy agents" on page 347.
(*Optional*) Customize the configuration of the Warehouse Proxy agent for tuning performance.	"Tuning the performance of the Warehouse Proxy" on page 354
Start the Warehouse Proxy agent.	"Starting the Warehouse Proxy" on page 329

Creating a TNS Service Name

Create a TNS (Transparent Network Substrate) Service Name (also called a Net Service Name) on a computer where an Oracle client is installed if the Tivoli Data Warehouse exists on a *remote* Oracle server. The TNS Service name is needed to create an ODBC connection between the client and the server. Use this procedure to create a TNS Service name:

- On a Windows computer where a Warehouse Proxy agent installed.
- On a Windows computer where the Tivoli Enterprise Portal Server is installed.

Do *not* perform this procedure on the computer where the data warehouse (Oracle server) is installed or on a computer where there is no Oracle client (for example, on a computer where a Type 4 Oracle JDBC driver is used to communicate with the remote data warehouse).

Note: This procedure uses the default value for the warehouse name (`WAREHOUS`). Substitute a different value if you do not want to use the default name.

Complete the following steps to create the TNS Service Name. Click **Next** after each step.

1. Enter `dbca` at the Oracle command line to start the Oracle Net Configuration Assistant tool.
2. On the Welcome window, select **Local Net Service Name configuration**.
3. Select **Add**.
4. Enter `WAREHOUS` in the **Service Name** field. (This is the remote name for the Tivoli Data Warehouse.)
5. Select **TCP** as the network protocol to communicate with the Tivoli Data Warehouse database.
6. Specify the fully qualified host name and port number of the computer where the warehouse database is installed.
7. Perform the connection test to verify the connection to the warehouse database.
8. Optionally change the default name in the **Net Service Name** field.

   This is the TNS Service Name. The default name matches the name that you entered in Step 4. You can change this to a different name. The TNS Service Name can be considered a local alias for the remote Tivoli Data Warehouse name.
9. When prompted to configure another net service name, click **No** to return to the Welcome window.
10. Click **Finish**.

Configuring an ODBC data source for an Oracle data warehouse

An Oracle client on Windows requires an ODBC connection to the data warehouse. For the Warehouse Proxy agent, you must configure the ODBC connection manually.

Complete the following procedure to set up an ODBC connection for a Warehouse Proxy agent on Windows to a local or remote Tivoli Data Warehouse.

Note: This procedure uses default values for the data source name (`ITM Warehouse`) and warehouse user ID (`ITMUser`). (Default values are used in configuration procedures for warehousing components.) Substitute different values if you do not want to use the default values.

1. On the computer where the Warehouse Proxy agent is installed, open the Control Panel.
2. Click **Administrative Tools → Data Sources (ODBC)**
3. Click **Add** in the **System DSN** tab in the ODBC Data Source Administrator window.

4. Select the Oracle ODBC driver:
   - For Oracle 9, the ODBC driver name is **Oracle in Ora9ias_home**.
   - For Oracle 10, the ODBC driver name is **Oracle in OraDb10g_home1**.
5. Enter `ITM Warehouse` in the **Data Source Name** field.
6. Enter the TNS Service Name in the **TNS Service Name** field. This is the name that you specified in Step 8 on page 324 (for example, `WAREHOUS`).
7. Enter `ITMUser` in the **User ID** field.
8. Click **Test Connection**.
9. In the Oracle ODBC Driver Connect window, enter the TNS Service Name, and the user ID and password of the warehouse user.
10. Click **OK** on the **Connection successful** message.

Configuring a Warehouse Proxy agent on Windows (ODBC connection)

Use this procedure to configure a Warehouse Proxy agent on Windows to connect to an Oracle Tivoli Data Warehouse:

1. Log on to the Windows system where the Warehouse Proxy agent is installed and begin the configuration:
   a. Click **Start → Programs → IBM Tivoli Monitoring → Manage Tivoli Monitoring Services**.

      The Manage Tivoli Enterprise Monitoring Services window is displayed.
   b. Right-click **Warehouse Proxy** and click **Configure Using Defaults**.

      Click **Reconfigure** if the Warehouse Proxy is installed on the same computer as the portal server.
   c. Click **OK** on the message regarding connection to a hub monitoring server.
2. The next two windows (entitled Warehouse Proxy: Agent Advanced Configuration) contain the settings for the connection between the Warehouse Proxy agent and the hub monitoring server. Click **OK** on each window to accept the settings.
3. Click **Yes** on the message asking if you want to configure the ODBC data source.
4. Select **Oracle** from the list of databases and click **OK**.

   The following configuration window is displayed.

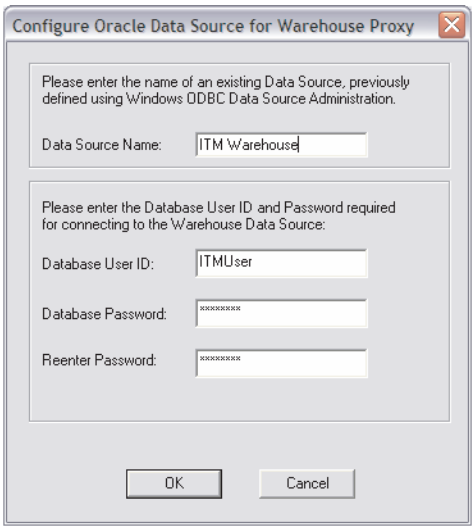


Figure 51. Configure Oracle Data Source for Warehouse Proxy window

5. Click **OK** to accept all default information on this window, or change one or more default values and then click **OK**. The fields on this window are described in Table 94.

   Note: The values for the data source name, database name, and database user ID and password must match the values that you used when configuring an ODBC connection for the Warehouse Proxy agent. (See "Configuring an ODBC data source for an Oracle data warehouse" on page 324.)

Table 94. Configuration information for the Tivoli Data Warehouse database on Oracle

Field	Default value	Description
Data Source Name	ITM Warehouse	The name of the data source.
Database User ID	ITMUser	The login name of the database user that the portal server will use to access the Tivoli Data Warehouse database.
Database Password	itmpswd1	The password for the database login user. If your environment requires complex passwords (passwords that require both alpha and numeric characters), specify a password that complies with these requirements.
Reenter Password	itmpswd1	Confirm the password by entering it again.

6. Click **OK**.

Configuring a Warehouse Proxy agent on Linux or AIX (JDBC connection)

Use this procedure to configure a Warehouse Proxy agent on Linux or AIX to connect to an Oracle data warehouse:

1. Log on to the computer where the Warehouse Proxy agent is installed.
2. Log on to the computer where the Warehouse Proxy agent is installed and begin the configuration.

a. Change to the *install_dir*/bin directory and run the following command:
   `./itmcmd manage [-h install_dir]`

   where *install_dir* is the installation directory for IBM Tivoli Monitoring. The default installation directory is /opt/IBM/ITM.

   The Manage Tivoli Enterprise Monitoring Services window is displayed.
b. Right-click **Warehouse Proxy** and click **Configure**.

   The Configure Warehouse Proxy window is displayed.

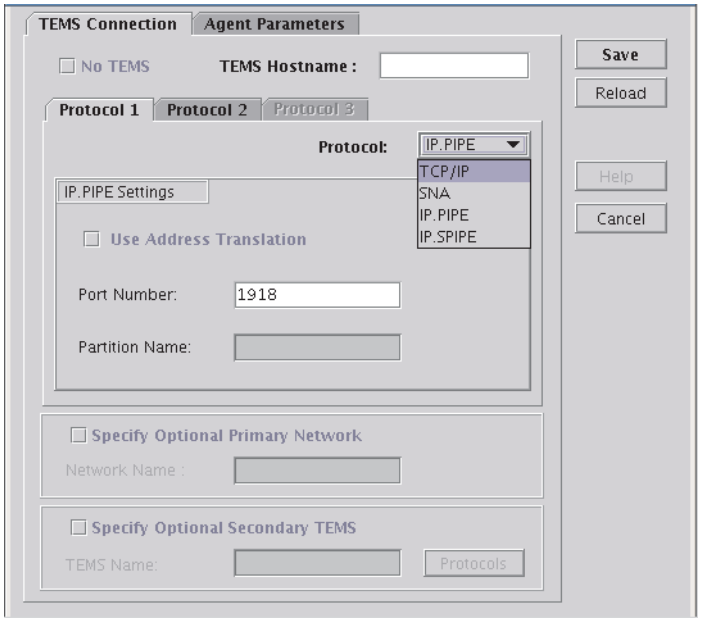


Figure 52. Configure Warehouse Proxy window (TEMS Connection tab)

3. On the **TEMS Connection** tab, review the settings for the connection between the Warehouse Proxy agent and the hub monitoring server.

   The Warehouse Proxy agent must use the same protocols used by the application agents and by the hub monitoring. If the proxy agent does not have the same protocol as the hub monitoring server, it cannot register with the hub. If the proxy does not have the same protocol as the application agents, then the application agents cannot communicate with the proxy when they to create a route to it.
4. Click the **Agent Parameters** tab.

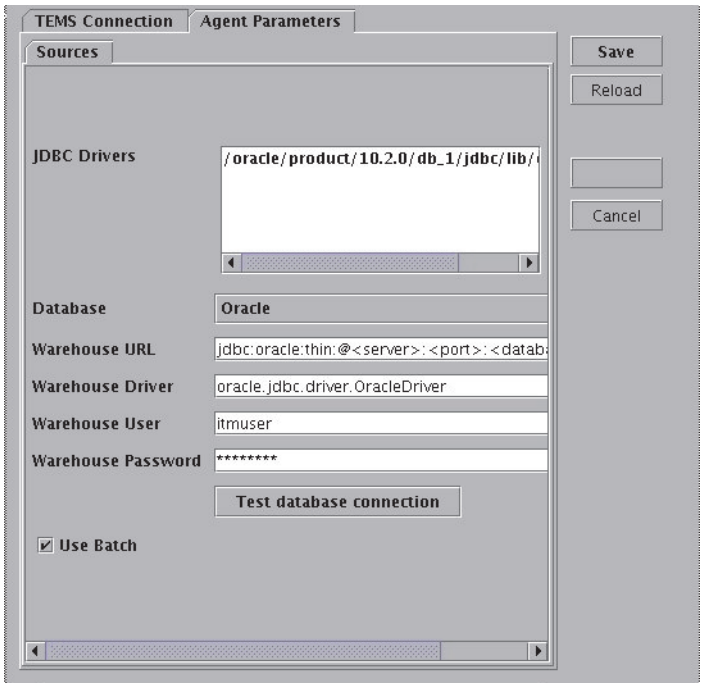


Figure 53. Configure Warehouse Proxy window (Agent Parameters tab)

5. In the **Database** drop-down list, select **Oracle**.
6. Add the name and directory location of the JDBC driver JAR file to the **JDBC Drivers** list box:
   a. Use the scroll bar at the bottom of the window to display the **Add** and **Delete** buttons, which are located to the right of the **JDBC Drivers** list box.
   b. Click **Add** to display the file browser window. Navigate to the location of the JDBC driver JAR file on this computer and select the file. The Oracle JDBC driver JAR file name and default location after downloading from the Web are as follows:

      <oracleinstalldir>/jdbc/lib/ojdbc14.jar
   c. Click **OK** to close the browser window and add the driver file to the list.

   If you need to delete an entry from the list, select the entry and click **Delete**.
7. Change the default value displayed in the **Warehouse URL** field if it is not correct. The default Tivoli Data Warehouse URL for Oracle is as follows:

   jdbc:oracle:thin:@localhost:1521:WAREHOUS
   - If the Tivoli Data Warehouse is installed on a remote computer, specify the host name of the remote computer instead of `localhost`.
   - Change the port number if it is different.
   - If the name of the Tivoli Data Warehouse database is not WAREHOUS, replace WAREHOUS with the actual name. (See "Creating the warehouse database on Oracle" on page 320.)
8. Verify the JDBC driver name, which is displayed in the **Warehouse Driver** field. (Note that the **Warehouse Driver** field displays the *driver name*, in contrast to the *driver JAR file* that is listed in the **JDBC Drivers** field.)

   The Oracle JDBC Type 4 driver name is as follows:

oracle.jdbc.driver.OracleDriver

9. If necessary, change the entries in the **Warehouse User** and **Warehouse Password** fields to match the user name and password that were created for the Tivoli Data Warehouse. (See "Creating the warehouse database on Oracle" on page 320.) The default user name is `itmuser` and the default password is `itmpswd1`.
10. Check the **Use Batch** check box if you want the Warehouse Proxy agent to submit multiple execute statements to the Tivoli Data Warehouse database for processing as a batch.

    In some situations, such as crossing a network, sending multiple statements as a unit is more efficient than sending each statement separately. Batch processing is one of the features provided with the JDBC 2.0 API.
11. Click **Test database connection** to ensure you can communicate with the Tivoli Data Warehouse database.
12. Click **Save** to save your settings and close the window.

Starting the Warehouse Proxy

- To start the Warehouse Proxy agent from the Manage Tivoli Enterprise Services window, right-click **Warehouse Proxy** and select **Start**.
- (*Linux or AIX only*) To start the Warehouse Proxy agent from the command line, run the following command from the bin directory of the IBM Tivoli Monitoring installation directory. The default installation directory is /opt/IBM/ITM.

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

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

Step 3: Configure communications between the Tivoli Enterprise Portal Server and the data warehouse

Complete the tasks described in the following table, in the order listed, to configure communications between the portal server and the data warehouse.

Table 95. Tasks for configuring communications between the portal server and an Oracle data warehouse

Task	Procedure
(*Portal server on Windows only*) Install an Oracle database client on the portal server.	Refer to the Oracle documentation for instructions on how to install an Oracle client.
(*Portal server on Windows only*) Create a TNS (Transparent Network Substrate) Service Name on the portal server.	"Creating a TNS Service Name" on page 323
(*Portal server on Linux or AIX only*) Install an Oracle JDBC Type 4 driver on the portal server.	Obtain the Oracle JDBC Type 4 Driver from the following Web site: http://www.oracle.com/technology/software/tech/java/sqlj_jdbc/index.html The Oracle JDBC driver JAR file name and location after installation is as follows: <*oracleinstalldir*>/jdbc/lib/ojdbc14.jar The ojdbc14.jar file supports JRE 1.5 or higher, the required Java Runtime Environment for IBM Tivoli Monitoring.
Configure the portal server to connect to the data warehouse. The configuration procedure on Windows automatically configures an ODBC connection to the data warehouse.	For a portal server on Windows, see "Configuring a Windows portal server (ODBC connection)." For a portal server on Linux or AIX, see "Configuring a Linux or AIX portal server (JDBC connection)" on page 331.
Restart the portal server.	"Starting the portal server" on page 333
Test the connection between the portal server and the Tivoli Data Warehouse by creating a customized query in the Tivoli Enterprise Portal.	"Testing the connection between the portal server and the Tivoli Data Warehouse" on page 351

Configuring a Windows portal server (ODBC connection)

Use this procedure to configure a portal server on Windows to connect to an Oracle Tivoli Data Warehouse:

1. Log on to the Windows system where the portal server is installed and begin the configuration:
   a. Click **Start** → **Programs** → **IBM Tivoli Monitoring** → **Manage Tivoli Monitoring Services**.

      The Manage Tivoli Enterprise Monitoring Services window is displayed.
   b. Right-click **Tivoli Enterprise Portal Server** and click **Reconfigure**.

2. The next two windows (entitled TEP Server Configuration) contain the settings for the connection between the portal server and the hub monitoring server. These settings were specified when the portal server was installed. Click **OK** on each window to accept the settings.
3. Click **Yes** on the message asking if you want to reconfigure the warehouse information for the Tivoli Enterprise Portal Server.
4. Select **Oracle** from the list of databases and click **OK**.

   The following configuration window is displayed.

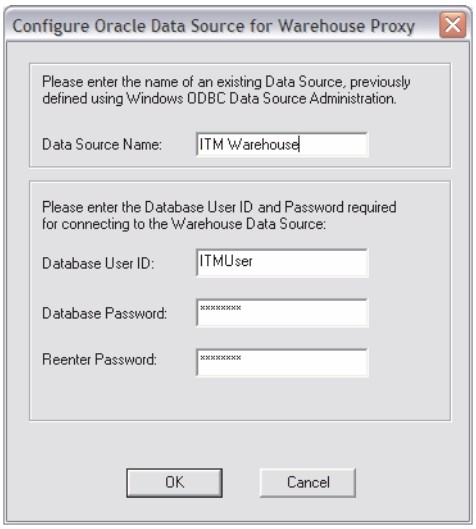


Figure 54. Configure Oracle Data Source for Warehouse Proxy window

5. Click **OK** to accept all default information on this window, or change one or more default values and then click **OK**. The fields on this window are described in the following table:

Table 96. Configuration information for the Tivoli Data Warehouse database on Oracle

Field	Default value	Description
Data Source Name	ITM Warehouse	The name of the data source.
Database User ID	ITMUser	The login name of the database user that the portal server will use to access the Tivoli Data Warehouse database.
Database Password	itmpswd1	The password for the database login user. If your environment requires complex passwords (passwords that require both alpha and numeric characters), specify a password that complies with these requirements.
Reenter Password	itmpswd1	Confirm the password by entering it again.

6. Click **OK**.

Configuring a Linux or AIX portal server (JDBC connection)

Use this procedure to configure a portal server on Linux or AIX to connect to an Oracle Tivoli Data Warehouse on any operating system:

1. Log on to the computer where the Tivoli Enterprise Portal Server is installed and begin the configuration.
   a. Change to the *install_dir*/bin directory and run the following command:
      ```
      ./itmcmd manage [-h install_dir]
      ```
      where *install_dir* is the installation directory for IBM Tivoli Monitoring. The default installation directory is /opt/IBM/ITM.
      The Manage Tivoli Enterprise Monitoring Services window is displayed.
   b. Right-click **Tivoli Enterprise Portal Server** and click **Configure**.
      The Configure Tivoli Enterprise Portal Server window is displayed.
2. On the **TEMS Connection** tab, review the settings for the connection between the portal server and the hub monitoring server. These settings were specified when the portal server was installed.
3. Click the **Agent Parameters** tab.
4. Select the **Oracle** radio button.
   The fields for configuring the connection to an Oracle data warehouse are displayed at the bottom of the window.

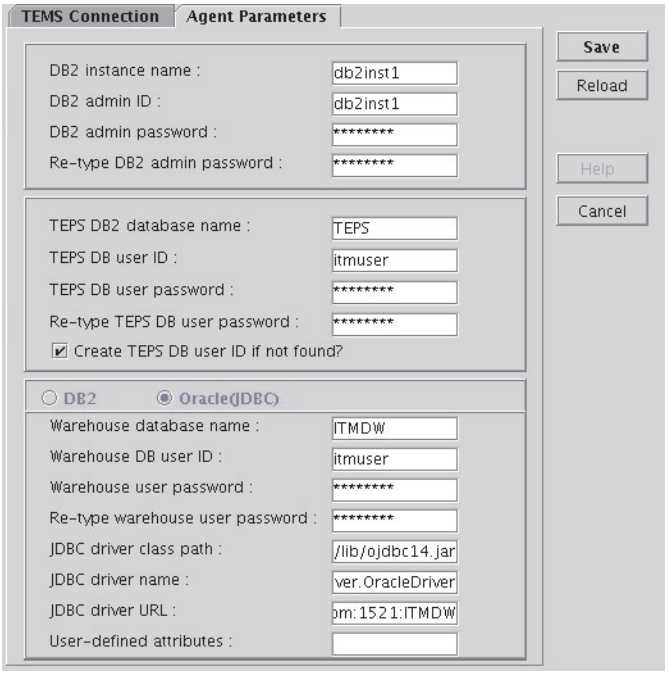


Figure 55. Configuring the connection to an Oracle data warehouse

5. Fill in the fields in Figure 55 with the configuration values described in Table 97.

Table 97. Configuration information for a Tivoli Data Warehouse database on Oracle

Field	Default value	Description
Warehouse database name	WAREHOUS	The name of the Tivoli Data Warehouse database.
Warehouse DB user ID	ITMUser	The database login user that the portal server uses to access the Tivoli Data Warehouse database. This user is referred to as the *warehouse user*.

Table 97. Configuration information for a Tivoli Data Warehouse database on Oracle (continued)

Field	Default value	Description
Warehouse user password	itmpswd1	The password for the warehouse user.
Re-type Warehouse user password	itmpswd1	The password for the warehouse user.
JDBC driver class path	*<oracleinstalldir>*/jdbc/lib/ojdbc14.jar	The full path name of the Oracle JDBC Type 4 driver JAR file on this computer.
JDBC driver name	oracle.jdbc.driver.OracleDriver	The Oracle JDBC Type 4 driver name.
JDBC driver URL	jdbc:oracle:thin:@localhost:1521:WAREHOUS	The Oracle-defined URL that identifies the Oracle instance used for the remote Tivoli Data Warehouse. Replace `localhost` with the host name of the remote computer where the Tivoli Data Warehouse is installed. Change the default port number (`1521`) and Tivoli Data Warehouse name (`WAREHOUS`) if they are different.
User-defined attributes	(no default)	Enter any user-defined attributes that are used to customize the behavior of the driver connection. Use semi-colons (;) to delimit the attributes.

6. Click **Save** to save your settings and close the window.

Starting the portal server

- To start the portal server from the Manage Tivoli Enterprise Services window, right-click **Tivoli Enterprise Portal Server** and select **Start**.
- (*Linux or AIX only*) To start the portal server from the command line, run the following command from the bin directory of the IBM Tivoli Monitoring installation directory. The default installation directory is /opt/IBM/ITM.

  ```
  ./itmcmd agent start cq
  ```

  where cq is the product code for the portal server.

Step 4: Install and configure communications for the Summarization and Pruning agent

Complete the tasks described in the following table, in the order listed, to install and configure the Summarization and Pruning agent.

Table 98. Tasks for installing and configuring communications for the Summarization and Pruning agent

Task	Procedure
Install the Summarization and Pruning agent if you have not already installed it. For best performance, install the Summarization and Pruning agent on the same computer as the data warehouse. The installation procedure for Windows includes steps for configuring the connection between the agent and the hub Tivoli Enterprise Monitoring server. On Linux or AIX, this step is performed in a separate configuration procedure (*Configuring the monitoring agent*). See the information at right. Be sure to perform all referenced installation and configuration procedures. **Note**: The Summarization and Pruning agent is not automatically started after installation. Do not complete any step or procedure for starting the agent at this point.	To install a Summarization and Pruning agent on Windows, complete the procedure "Windows: Installing a monitoring agent" on page 149. To install a Summarization and Pruning agent on Linux or UNIX, complete the procedure "Linux or UNIX: Installing a monitoring agent" on page 152, including the following subsections: • *Installing the monitoring agent* • *Configuring the monitoring agent* • *Changing the file permissions for agents* (if you used a non-root user to install the Warehouse Proxy) *Do not complete the procedure for starting the agent*.
Install an Oracle Type 4 JDBC driver on the computer where the Summarization and Pruning agent is installed.	Obtain the Oracle JDBC Driver from the following Web site: http://www.oracle.com/technology/software/tech/java/sqlj_jdbc/index.html The Oracle JDBC driver JAR file name and location after installation is as follows: <*oracleinstalldir*>/jdbc/lib/ojdbc14.jar The ojdbc14.jar file supports JRE 1.5 or higher, the required Java Runtime Environment for IBM Tivoli Monitoring.
Configure the Summarization and Pruning agent. When you configure the Summarization and Pruning agent, you configure the connection to the Tivoli Data Warehouse and you specify settings that control the operation of the Summarization and Pruning agent. Perform this procedure whether or not the Summarization and Pruning agent and the warehouse database are installed on the same computer.	"Configuring the Summarization and Pruning agent (JDBC connection)" on page 337
Configure history collection. When you configure history collection, you specify settings for how often to collect, aggregate, and prune data for individual monitoring agents and attribute groups. Configure history collection from the Tivoli Enterprise Portal.	See the *IBM Tivoli Monitoring Administrator's Guide* for instructions on how to configure history collection.

Table 98. Tasks for installing and configuring communications for the Summarization and Pruning agent (continued)

Task	Procedure
Start the Summarization and Pruning agent.	"Starting the Summarization and Pruning agent" on page 347

Chapter 16. Tivoli Data Warehouse solutions: common procedures

This chapter contains information and procedures for Tivoli Data Warehouse solutions that use any of the supported database platforms: IBM DB2, Microsoft SQL Server, and Oracle. Read the chapter pertaining to the database platform you are using for the Tivoli Data Warehouse before performing any of these procedures.

- "Configuring the Summarization and Pruning agent (JDBC connection)"
- "Starting the Summarization and Pruning agent" on page 347
- "Installing and configuring multiple Warehouse Proxy agents" on page 347
- "Testing the connection between the portal server and the Tivoli Data Warehouse" on page 351
- "Tuning the performance of the Warehouse Proxy" on page 354
- "WAREHOUSELOG and WSAREHOUSEAGGRLOG tables" on page 356

Configuring the Summarization and Pruning agent (JDBC connection)

Use this procedure to configure the Summarization and Pruning agent to connect to a Tivoli Data Warehouse database created on any of the supported database platforms and operating systems.

Before you begin

The JDBC driver JAR files for your database platform must be located on the computer where you installed the Summarization and Pruning agent. Use a Type 4 JDBC driver. Do not use the Type 2 driver.

- If you are using DB2 for your Tivoli Data Warehouse database, the JDBC driver files are included with the database platform installation. If the warehouse database and the Summarization and Pruning agent are installed on the same computer, the JDBC driver files are already present. It is not necessary to move them from their current location. If your warehouse database is located on a remote computer, copy the driver files to the local computer (the computer where you installed the Summarization and Pruning agent). Copy the files to any directory to which the user the Summarization and Pruning agent is running as has access to.
- If you are using Oracle or Microsoft SQL Server for your Tivoli Data Warehouse database, download the driver file from the company Web site to the computer where you installed the Summarization and Pruning agent. Download the files to any directory to which the user the Summarization and Pruning agent is running as has access to.

Table 99 on page 338 shows where to obtain the driver files for each database platform.

© Copyright IBM Corp. 2005, 2007

Table 99. Where to obtain the JDBC driver files for the Summarization and Pruning agent

Database platform	JDBC driver files
IBM DB2	Use the DB2 UDB JDBC Universal Driver (Type 4 driver). The DB2 driver files are located with your Tivoli Data Warehouse server installation. The Type 4 driver file names and locations are as follows: <*db2installdir*>/java/db2jcc.jar <*db2installdir*>/java/db2jcc_license_cu.jar where <*db2installdir*> is the directory where DB2 was installed. The default DB2 Version 9 installation directory is as follows: • On Windows: C:\Program Files\IBM\SQLLIB • On AIX: /usr/opt/db2_09_01 • On Linux and Solaris: /opt/IBM/db2/V9.1
Microsoft SQL Server	Use the Microsoft SQL Server 2005 Type 4 driver to connect to a Tivoli Data Warehouse on either SQL Server 2000 or SQL Server 2005. (The SQL Server 2005 JDBC Driver works with a Tivoli Data Warehouse on SQL Server 2000.) Obtain the 2005 JDBC driver from the following Microsoft Web page: http://msdn.microsoft.com/data/jdbc/default.aspx Download and install the driver to the computer where you installed the Summarization and Pruning agent. Follow the instructions on the Microsoft download page for installing the driver. The SQL Server 2005 JAR file name and location after installation is as follows: <*mssql2005installdir*>/sqljdbc_1.0/enu/sqljdbc.jar
Oracle	Obtain the Oracle JDBC Type 4 driver from the following Web site: http://www.oracle.com/technology/software/tech/java/sqlj_jdbc/index.html The Oracle JDBC driver JAR file name and location after installation is as follows: <*oracleinstalldir*>/jdbc/lib/ojdbc14.jar The ojdbc14.jar file supports JRE 1.5 or higher, the required Java Runtime Environment for IBM Tivoli Monitoring.

Procedure

Complete the following steps to configure the Summarization and Pruning agent.

Note: A **Reload** button is available on the configuration windows. Click **Reload** at any time during the procedure to restore the original settings.

1. Log on to the computer where the Summarization and Pruning agent is installed and begin the configuration:
   a. Open the Manage Tivoli Enterprise Monitoring Services window:
      - On Windows, click **Start** → **Programs** → **IBM Tivoli Monitoring** → **Manage Tivoli Monitoring Services**.
      - On Linux or UNIX, change to the *install_dir*/bin directory and run the following command:

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

where *install_dir* is the installation directory for IBM Tivoli Monitoring. The default installation directory is /opt/IBM/ITM.

b. Right-click **Summarization and Pruning Agent**.

c. On Windows, click **Configure Using Defaults**. On Linux or UNIX, click **Configure**. If you are reconfiguring, click **Reconfigure**.

2. Review the settings for the connection between the Summarization and Pruning agent and the hub Tivoli Enterprise Monitoring server. These settings were specified when the Summarization and Pruning agent was installed.
   - On Windows, perform the following steps:
     a. On the Warehouse Summarization and Pruning Agent: Agent Advanced Configuration window, verify the communications protocol of the hub monitoring server in the **Protocol** drop down list. Click **OK**.
     b. On the next window, verify the host name and port number of the hub monitoring server. Click **OK**.

     For information about the different protocols available to the hub monitoring server on Windows, and associated default values, see 14e on page 117.
   - On Linux or UNIX, verify the following information on the **TEMS Connection** tab:
     – The hostname of the hub monitoring server in the **TEMS Hostname** field. (If the field is not active, clear the **No TEMS** check box.)
     – The communications protocol that the hub monitoring server uses in the **Protocol** drop down list.
       - If you select IP.UDP, IP.PIPE, or IP.SPIPE, enter the port number of the monitoring server in the **Port Number** field.
       - If you select SNA, enter information in the **Net Name**, **LU Name**, and **LOG Mode** fields.

       For information about the different protocols available to the hub monitoring server on Linux or UNIX, and associated default values, seeTable 32 on page 121.

3. When you are finished verifying or entering information about the hub monitoring server:
   - On Windows, click **Yes** on the message asking if you want to configure the Summarization and Pruning agent.
   - On Linux or UNIX, click the **Agent Parameters** tab.

   A multi-tabbed configuration window is displayed with the **Sources** tab at the front.

   Figure 56 on page 340 shows the configuration window for a Summarization and Pruning agent on Windows (with values displayed for a DB2 warehouse database). The configuration window for a Summarization and Pruning agent on Linux or UNIX is similar.

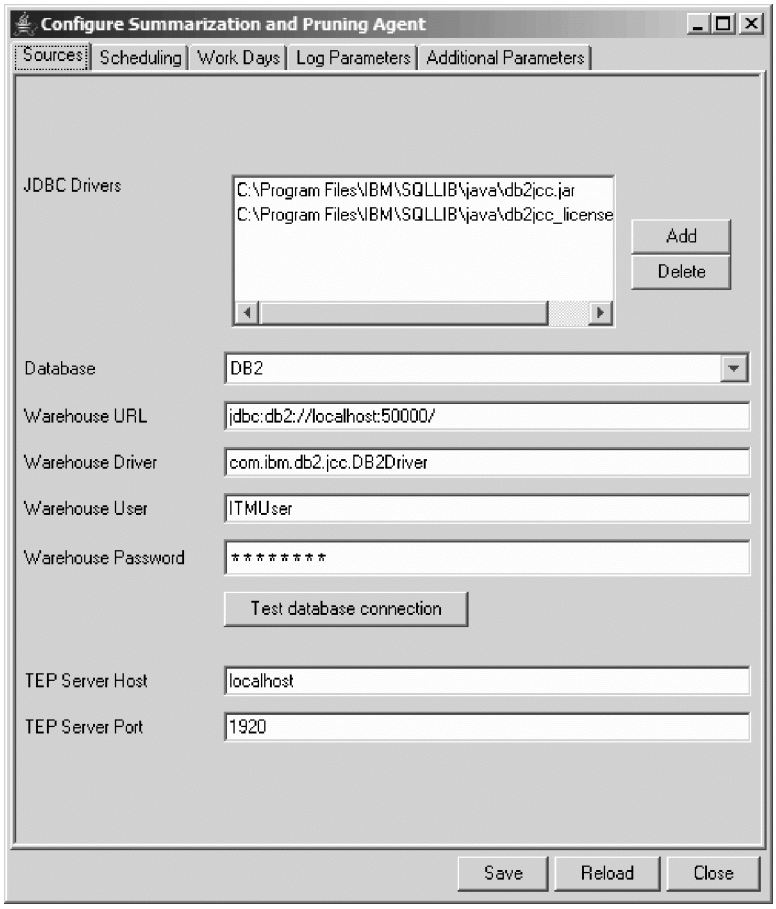


Figure 56. Sources tab of Configure Summarization and Pruning Agent window

4. Add the names and directory locations of the JDBC driver JAR files to the **JDBC Drivers** list box:
   a. On Linux or UNIX, use the scroll bar at the bottom of the window to display the **Add** and **Delete** buttons, which are located to the right of the **JDBC Drivers** list box.
   b. Click **Add** to display the file browser window. Navigate to the location of the driver files on this computer and select the Type 4 driver files for your database platform. See Table 99 on page 338 for the names and default locations of the driver files to add.
   c. Click **OK** to close the browser window and add the JDBC driver files to the list.

   If you need to delete an entry from the list, select the entry and click **Delete**.
5. In the **Database** field, select the database platform you are using for the Tivoli Data Warehouse from the drop-down list: **DB2**, **SQL Server**, or **Oracle**.

   The default values for the database platform you selected are displayed in the other text fields on the **Sources** tab.
6. Change the default value displayed in the **Warehouse URL** field if it is not correct. The following table lists the default Tivoli Data Warehouse URLs for the different database platforms:

Table 100. Tivoli Data Warehouse URLs

Database platform	Warehouse URL
IBM DB2	jdbc:db2://localhost:60000/WAREHOUS
Oracle	jdbc:oracle:thin:@localhost:1521:WAREHOUS
Microsoft SQL Server 2000 or SQL Server 2005	jdbc:sqlserver://localhost:1433;databaseName=WAREHOUS

- If the Tivoli Data Warehouse is installed on a remote computer, specify the host name of the remote computer instead of `localhost`.
- Change the port number if it is different.
- If the name of the Tivoli Data Warehouse database is not WAREHOUS, replace WAREHOUS with the actual name.

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

   The following table lists the JDBC Type 4 driver names for each database platform:

Table 101. JDBC driver names

Database platform	JDBC driver name
IBM DB2	com.ibm.db2.jcc.DB2Driver
Oracle	oracle.jdbc.driver.OracleDriver
Microsoft SQL Server	com.microsoft.sqlserver.jdbc.SQLServerDriver **Note:** This is the name of the 2005 SQL Driver. Do not use the SQL Server 2000 JDBC driver, even if the Tivoli Data Warehouse was created in Microsoft SQL 2000. (The name of the 2000 SQL driver was com.microsoft.jdbc.sqlserver.SQLServerDriver. Note the reversal of the string `jdbc.sqlserver`.)

8. If necessary, change the entries in the **Warehouse User** and **Warehouse Password** fields to match the user name and password that were created for the Tivoli Data Warehouse. The default user name is `itmuser` and the default password is `itmpswd1`.
9. In the **TEP Server Host** and **TEP Server Port** fields, enter the host name of the computer where the Tivoli Enterprise Portal Server is installed and the port number that it uses to communicate with the Tivoli Data Warehouse server.
10. Click **Test database connection** to ensure you can communicate with the Tivoli Data Warehouse database.
11. Select the **Scheduling** tab to specify when you want summarization and pruning to take place. You can schedule it to run on a fixed schedule or on a flexible schedule:

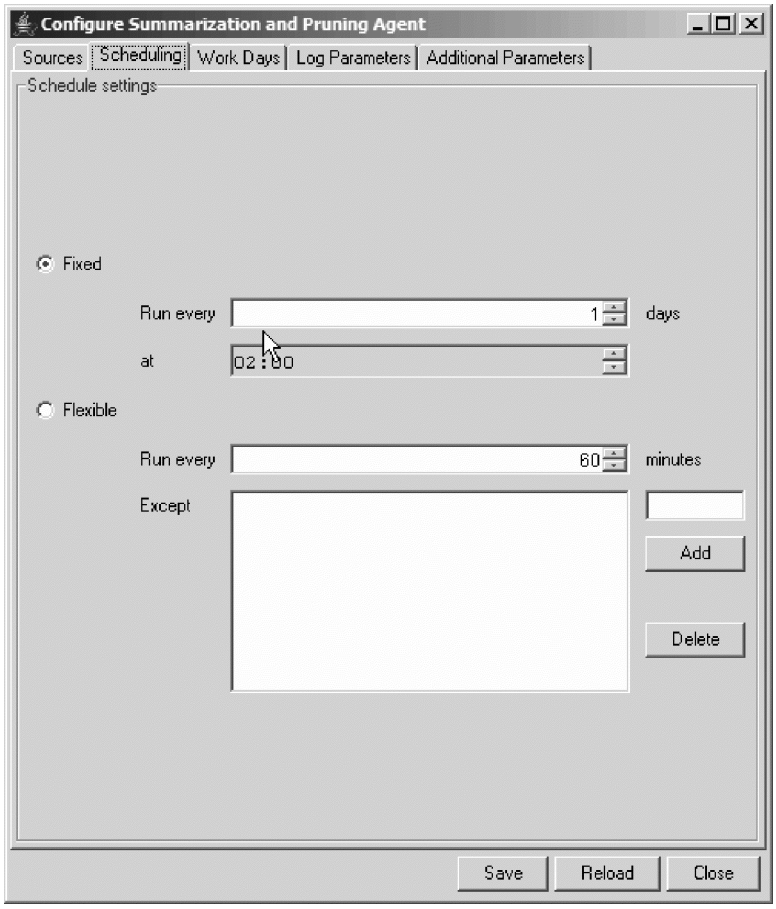


Figure 57. Scheduling tab of Configure Summarization and Pruning Agent window

- Fixed
  - Schedule the Summarization and Pruning agent to run every *x* days.
  - Select the time of the day that you want the agent to run.

    Set the time to at least 5 minutes from the current time of you want it to run right away.
- Flexible
  - Schedule the Summarization and Pruning agent to run every *x* minutes.
  - Optionally, specify the times when the agent should *not* run, using the format HH:MM-HH:MM. Press **Add** to add the text. For example, to block the agent from running between 00:00 and 01:59 and between 04:00 and 04:59, type 00:00-01:59, click **Add**, type 04:00-04:59 and click **Add**. Do not use the **Add** button unless you are adding a blackout period. All values must be between 00:00 and 23:59 and the end time must be greater than start time.

Note: If you select Fixed, the Summarization and Pruning agent does not immediately perform any summarization or pruning when it *starts*. It performs summarization and pruning when it *runs*. It runs according to the schedule you specify on the **Scheduling** tab. If you select Flexible, the Summarization and Pruning agent runs once immediately after it is started and then at the interval you specified except during any black out times.

12. Specify shift and vacation settings in the **Work Days** tab:

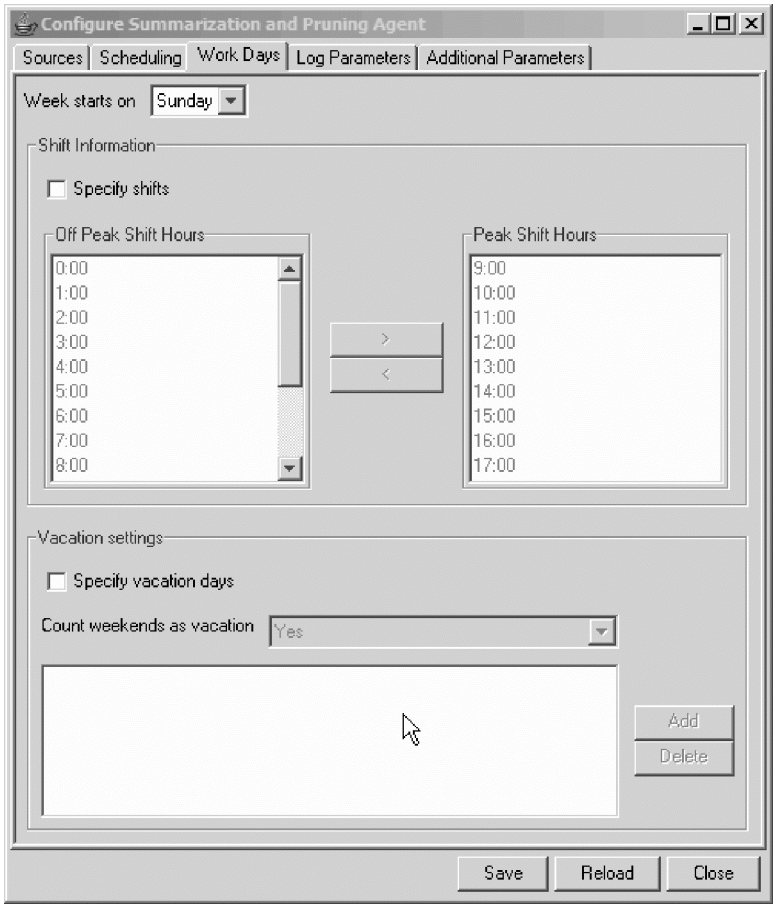


Figure 58. Work Days tab of Summarization and Pruning Agent configuration window

When you enable and configure shifts, IBM Tivoli Monitoring produces three separate summarization reports:

- Summarization for peak shift hours
- Summarization for off-peak shift hours
- Summarization for all hours (peak and off-peak)

Similarly, when you enable and configure vacations, IBM Tivoli Monitoring produces three separate summarization reports:

- Summarization for vacation days
- Summarization for non-vacation days
- Summarization for all days (vacation and non-vacation)

Complete the following steps to enable shifts, vacations, or both:

- Select when the beginning of the week starts.
- To configure shifts:
  a. Select **Specify shifts** to enable shifts.
  b. Optionally change the default settings for peak and off peak hours by selecting and moving hours between the **Peak Shift Hours** box and the **Off Peak Shift Hours** box using the arrow buttons.

Note: Changing the shift information after data has been summarized creates an inconsistency in the data. Data that was previously collected is not summarized again to account for the new shift values.

- To configure vacation settings:
  a. Select **Specify vacation days** to enable vacation days.
  b. Select **Yes** in the drop down list if you want to specify weekends as vacation days.
  c. Select **Add** to add vacation days.
  d. Select the vacation days you want to add from the calendar.

     On UNIX or Linux, right-click, instead of left-click, to select the month and year.

     The days you select are displayed in the list box.

     If you want to delete any days you have previously chosen, select them and click **Delete**.

     Notes:

     1) Add vacation days in the future. Adding vacation days in the past creates an inconsistency in the data. Data that was previously collected is not summarized again to account for vacation days.
     2) Enabling shifts or vacation periods can significantly increase the size of the warehouse database. It will also negatively affect the performance of the Summarization and Pruning Agent.

13. Select the **Log Parameters** tab to set the intervals for log pruning:

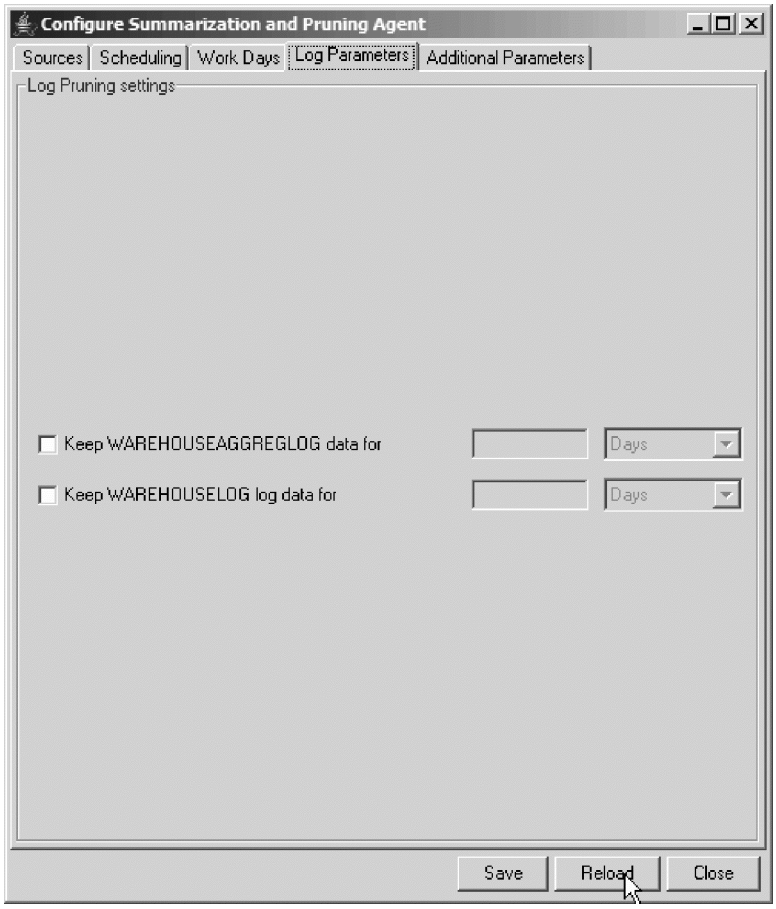


Figure 59. Log Parameters tab of Summarization and Pruning Agent configuration window

- Select Keep WAREHOUSEAGGREGLOG data for, select the unit of time (day, month or year), and the number of units for which data should be kept.
- Select Keep WAREHOUSLOG data for, select the unit of time (day, month or year), and the number of units for which data should be kept.

14. Specify additional summarization and pruning settings in the **Additional Parameters** tab:

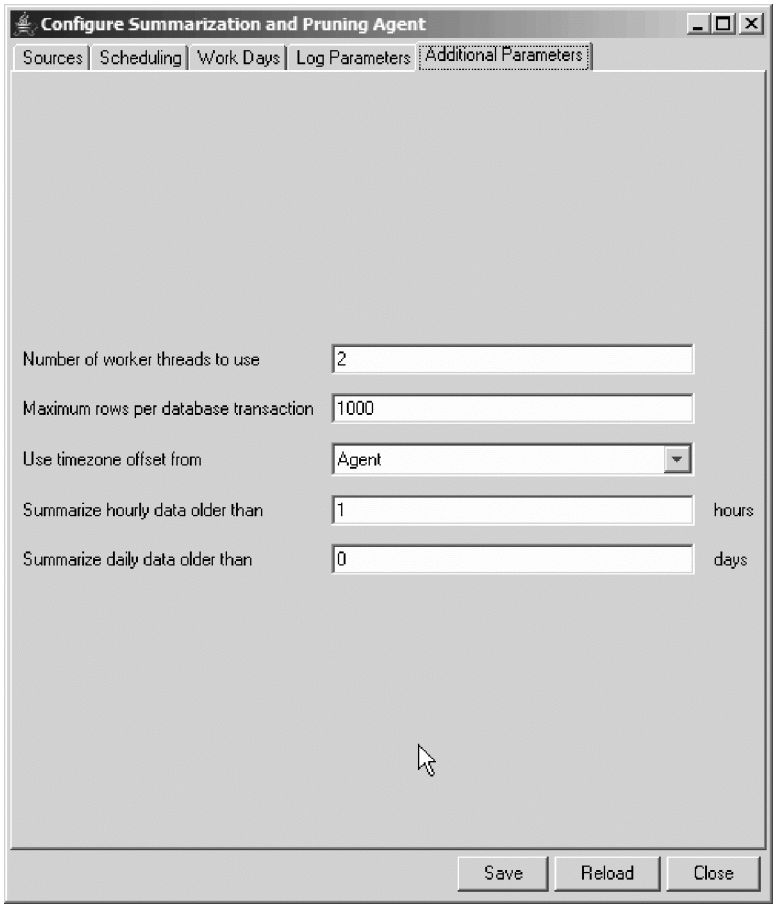


Figure 60. Additional Parameters tab of Summarization and Pruning Agent configuration window

a. Specify the number of additional threads you want to use for handling summarization and pruning processing. The number of threads should be 2 * N, where N is the number of processors where the Summarization and Pruning agent is running. A higher number of threads can be used, depending on your database configuration and hardware.

b. Specify the maximum rows that can be deleted in a single pruning transaction. Any positive integer is valid. The default is `1000`. There is no value that indicates you want all rows deleted.

   If you increase the number of threads, you might consider increasing this value if your transaction log allows for it. The effective number of rows deleted per transaction is based on this value divided by the number of worker threads.

c. Indicate a time zone for historical data from the **Use timezone offset from** drop down list.

   This field indicates which time zone to use when a user specifies a time period in a query for monitoring data.

   - Select **Agent** to use the time zone (or time zones) where the monitoring agents are located.
   - Select **Warehouse** to use the time zone where the Summarization and Pruning agent is located.

   Note:

- Skip this field if the Summarization and Pruning agent and the monitoring agents that collect data are all in the same time zone.
- If the Tivoli Data Warehouse and the Summarization and Pruning agent are in different time zones, the **Warehouse** choice indicates the time zone of the Summarization and Pruning agent, not the warehouse.

d. Specify the age of the data you want summarized in the **Summarize hourly data older than** and **Summarize daily data older than** fields. The default is `1` for hourly data and `0` for daily data.

15. Save your settings and close the window. Click **Save** to save your settings. On Windows, click **Close** to close the configuration window.
    - On Windows, click **Save** and then click **Close**.
    - On Linux or UNIX, click **Save** and then click **Cancel**.

Starting the Summarization and Pruning agent

- To start the Summarization and Pruning agent from the Manage Tivoli Enterprise Services window, right-click **Summarization and Pruning** and select **Start**.
- (*Linux or UNIX only*) To start the Summarization and Pruning agent from the command line, run the following command from the bin directory of the IBM Tivoli Monitoring installation directory. The default installation directory is /opt/IBM/ITM.

  ```
  ./itmcmd agent start sy
  ```

  where `sy` is the product code for the Summarization and Pruning agent.

Installing and configuring multiple Warehouse Proxy agents

IBM Tivoli Monitoring supports multiple warehouse proxies within a single hub monitoring server environment. The provision for multiple warehouse proxies provides for greater scalability and performance in historical data collection. More importantly, provides reliability by providing a failover mechanism. If a Warehouse Proxy is unavailable, data can be inserted into the warehouse by a different Warehouse Proxy agent (if the agents are configured properly for failover).

The support for multiple Warehouse Proxy agents has the following important features:

- All Warehouse Proxy agents within a single hub monitoring server environment export data to a single Tivoli Data Warehouse.
- Each Warehouse Proxy agent is associated with a subset of monitoring server instances that you specify when you configure the proxy agent. Each Warehouse Proxy exports data only for monitoring agents that report to one of the monitoring servers (hub or remote) on the specified list. Alternatively, a given Warehouse Proxy agent can be configured to service *any* monitoring server. This is important for backward compatibility and for configuring failover.

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

1. When a Warehouse Proxy agent starts, it registers with the Global Location Broker on the hub monitoring server, sending it the list of monitoring servers that it is configured to serve, oran indication that the Warehouse Proxy agent can service any monitoring server. This registration process is repeated every hour.

2. Each monitoring server queries the Global Location Broker at regular intervals to determine which Warehouse Proxy it is associated with. The monitoring server then sends the address of this Warehouse Proxy to all of its child monitoring agents to use during historical data exports. You can change the default query interval of 60 minutes to some other value.

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

Installing and configuring the proxy agents

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

1. Install each proxy agent using the following procedures:
   - To install a Warehouse Proxy agent on Windows, complete the procedure "Windows: Installing a monitoring agent" on page 149.
   - To install a Warehouse Proxy agent on Linux or AIX, complete the procedure "Linux or UNIX: Installing a monitoring agent" on page 152, including the following subsections:
     - *Installing the monitoring agent*
     - *Configuring the monitoring agent*
     - *Changing the file permissions for agents* (if you used a non-root user to install the Warehouse Proxy)
2. Associate each proxy agent with the list of monitoring servers that you want the proxy agent to serve:
   a. Open the environment file for the proxy agent:
      - (Windows) *ITMinstall_dir*\TMAITM6\KHDENV
      - (Linux or AIX) *ITMinstall_dir*/config/hd.ini

      where *ITMinstall_dir* is the directory where you installed the product.
   b. Add the environment variable KHD_WAREHOUSE_TEMS_LIST to the file and set it to specify a space- or comma-delimited list of monitoring server instance names. For example:

      ```
      KHD_WAREHOUSE_TEMS_LIST=REMOTE_TEMS1 REMOTE_TEMS2
      ```

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

      Each proxy agent will register with an annotation representing one or more monitoring server names, indicating that it will serve all the agents reporting to those monitoring servers. The default annotation (or the string "*ANY") in the KHD_WAREHOUSE_TEMS_LIST variable indicates that a proxy may serve as a possible failover agent. Adding the "*ANY" string in the monitoring server list for the third proxy agent means that this agent will serve as a failover agent if one or more proxy agents stop working.

      When a lookup to find the address of the proxy agent is done by a monitoring agent (if data collected at the monitoring agent) or by the monitoring server (if data collected at the monitoring server), the address of the proxy agent registered with an annotation equal to the name of the monitoring server the agents are connected to is found first, then the proxy agents registered with a default annotation are found in the order they were

registered on the hub monitoring server. If an historical export has been redirected to a proxy agent, the historical exports will continue to be sent to that agent as long as the connection is working. To reestablish the original configuration, stop and restart the fall-back WHP.

The name of a particular monitoring server can be specified in the list for *only one proxy agent*. *Do not specify the same monitoring server name in more than one list.* Do not try to do load balancing by specifying the same monitoring server name in two different KHD_WAREHOUSE_TEMS_LIST variables.

3. Optionally modify the interval at which a monitoring server queries the Global Location Broker to find out which Warehouse Proxy it is associated with:
   a. Open the environment file for the monitoring server:
      - (Windows) *ITMinstall_dir*\CMS\KBBENV
      - (Linux or UNIX) *ITMinstall_dir*/config/ms.ini

      where *ITMinstall_dir* is the directory where you installed the product.
   b. Change the following entry to specify a different query interval:

      ```
      KPX_WAREHOUSE_REGCHK=60
      ```

      The query interval is specified in minutes. The default value is 60 minutes.
4. (Optional) Use the KDC_FAMILIES options COUNT and SKIP with all IBM Tivoli Monitoring products running on the Warehouse Proxy agent computer.

   This step should only done to guarantee the port that Warehouse Proxy listens for firewall consideration. Using these options guarantees that the Warehouse Proxy agent always obtains the same listening port that was opened by the network administrator. The Warehouse Proxy agent uses the KDC_FAMILIES COUNT option to obtain its listening port. All other non-monitoring server processes (agents, portal server) running on the computer with the Warehouse Proxy agent use the KDC_FAMILIES SKIP option to bypass reserved ports.

   The network administrator must open access for inbound data for the Warehouse Proxy port thru the firewall. Example:

   ```
   HUB TEMS
   IP.PIPE PORT:1918
   (listens on port 1918)

   WH Proxy Agent
   IP.PIPE COUNT:1
   (listens on port 6014)

   Windows Agent
   IP.PIPE SKIP:2
   (listens on port 11010)

   TEPServer
   IP.PIPE SKIP:2
   (listens on port 16124)

   WHProxy port 6014
   Open through firewall for export

   TEMS port 1918
   Open through firewall
   ```
5. Start the Warehouse Proxy agent:
   - To start a Warehouse Proxy agent on Windows or Linux from the Manage Tivoli Enterprise Services window, right-click **Warehouse Proxy** and select **Start**.

- To start a Warehouse Proxy agent on Linux or AIX from the command line, enter the following command:

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

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

Setting a permanent socket address for a proxy agent

In some network environments, use of the Global Location Broker default registration algorithm is not supportable and a specific monitoring server variable must be used. This applies also when monitoring agents configure their connections as ephemeral (using `KDC_FAMILIES=ip.pipe use:y ephemeral:y` for instance).

KPX_WAREHOUSE_LOCATION is the variable that allows a fixed warehouse route to be delivered to connected agents. KPX_WAREHOUSE_LOCATION is an optional list of fully qualified, semicolon delimited network names and should be added in the monitoring server environment file located in different place depending on the platform:

- Windows: <*install_dir*>/CMS/KBBENV
- UNIX and Linux: <*install_dir*>/config/kbbenv.ini

KPX_WAREHOUSE_LOCATION is used instead of the routing string currently derived by the monitoring server from the Location Broker monitoring. If the variable KPX_WAREHOUSE_LOCATION is set on the hub monitoring server, then the Warehouse Proxy agent is registered in the Global Location Broker. If the variable is set on the remote monitoring server, then the Warehouse Proxy agent is registered in the Local Location Broker. This variable has a maximum length of 200 bytes. The syntax is:

```
KPX_WAREHOUSE_LOCATION= <family protocol>:#<network address>[<port number>];
```

Verifying the configuration

Use the following trace settings to verify the configuration:

- To verify that a Warehouse Proxy is registering with the hub monitoring server and placing the correct entries into the Global Location Broker:
  1. Open the environment file for the proxy agent:
     - (Windows) *ITMinstall_dir*\TMAITM6\KHDENV
     - (Linux or AIX) *ITMinstall_dir*/config/hd.ini

     where *ITMinstall_dir* is the directory where you installed the product.
  2. Add the following entry to the KBB_RAS1 trace setting:

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

     This setting prints the value of KHD_WAREHOUSE_TEMS_LIST and shows any errors associated with its components.
- To determine which Warehouse Proxy a particular monitoring server uses for its agents:
  1. Open the environment file for the monitoring server:
     - (Windows) *ITMinstall_dir*\CMS\KBBENV
     - (Linux or UNIX) *ITMinstall_dir*/config/ms.ini

     where *ITMinstall_dir* is the directory where you installed the product.
  2. Add the following entry to the KBB_RAS1 trace setting:

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

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

Testing the connection between the portal server and the Tivoli Data Warehouse

To test the connection between the Tivoli Enterprise Portal Server and the Tivoli Data Warehouse database, use the Tivoli Enterprise Portal to create a custom SQL query to the warehouse database and display the results. The procedure described in this section creates an SQL query to the WAREHOUSELOG table, a status table that is created in the warehouse database when the Warehouse Proxy agent starts. See "WAREHOUSELOG and WSAREHOUSEAGGRLOG tables" on page 356 for a description of this table.

Before you begin, make sure that the following components are installed and started:

- The Tivoli Enterprise Portal Server
- The Warehouse Proxy agent
- The Tivoli Data Warehouse RDBMS server

The test procedure consists of the following steps:

1. Create a custom SQL query to the WAREHOUSELOG table.
2. Create a new workspace to display the results.
3. Assign the query to the workspace.

1. Create the query

1. Start the Tivoli Enterprise Portal using the desktop or browser client. See "Starting the Tivoli Enterprise Portal client" on page 188 for instructions.

   Log in as the system administrator. (The default system administrator ID is `sysadmin`.)
2. Click **Query Editor** on the Tivoli Enterprise Portal tool bar.
3. In the Query Editor window, click **Create New Query**.

   The Create Query window is displayed.

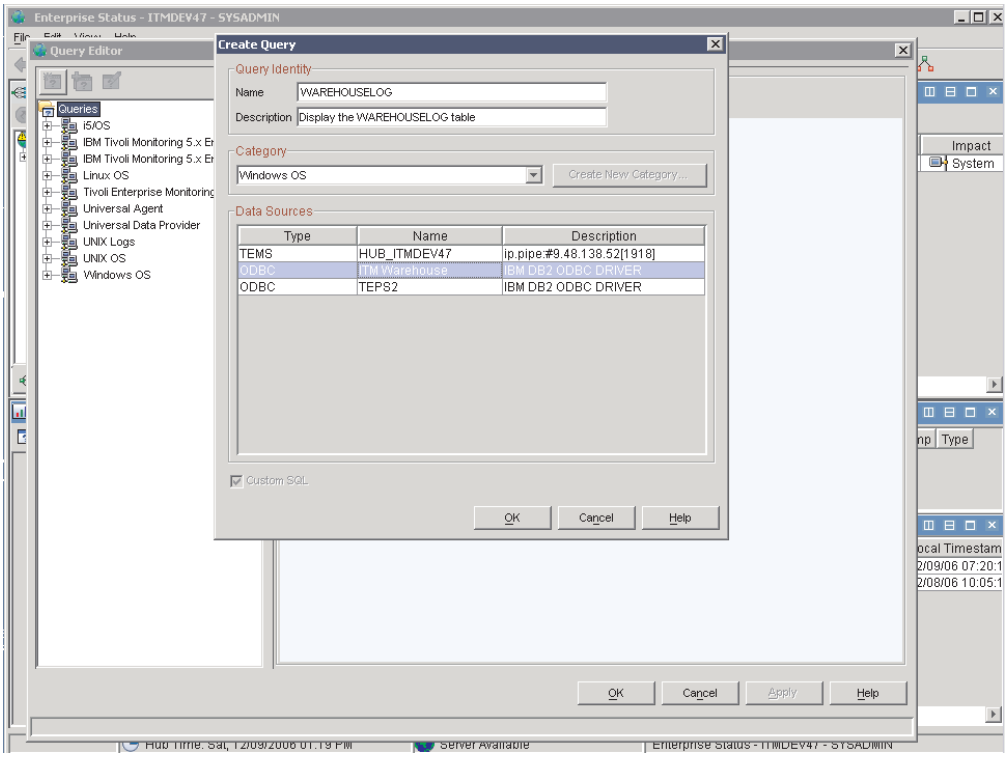


Figure 61. Create Query window

4. Enter a name and description for the query. For this test, enter `WAREHOUSELOG` for the query name.
5. From the **Category** drop-down list, select the folder where you want the WAREHOUSELOG query to appear in the Query tree.

   For example, select a folder name that corresponds to the operating system (Windows OS or UNIX OS) where the Tivoli Data Warehouse is installed.
6. Select the name of the data source for the Tivoli Data Warehouse in the **Data Sources** list.
7. Click **OK**.

   The WAREHOUSELOG query appears in the Query tree in the Custom_SQL folder under the category that you selected. The **Specification** tab opens with a **Custom SQL** text box for you to enter an SQL command.
8. Enter the following SQL statement in the **Custom SQL** text box to select all columns of the WAREHOUSELOG table:

   ```
   select * from WAREHOUSELOG
   ```
9. Click **OK** to save the query and close the Query Editor window.

2. Create a workspace

1. If the Enterprise Status workspace is not open, click the Enterprise Navigator item.
2. Select **Save Workspace As** from the File menu.
3. Enter the name `WAREHOUSELOG` for the new workspace.
4. Click **OK**.

   You now have a duplicate of the Enterprise Status workspace named WAREHOUSELOG that you can modify.

3. Assign the query to the workspace

1. In the WAREHOUSELOG workspace, click **Table** on the tool bar, release the mouse button, then click inside one of the workspace views (for example, the Situation Event Console view).
2. Click **Yes** on the message asking if you want to assign the query now.
3. In the Query tab, select **Click here to assign query**.

   The Query editor opens with a list of all product queries.
4. In the list of queries, expand the category folder you specified when you created the query (for example Windows OS or UNIX OS), and then expand the Custom_SQL folder.
5. Select **WAREHOUSELOG** from the list of queries in the Custom_SQL folder.

   The query definition opens in the right frame.

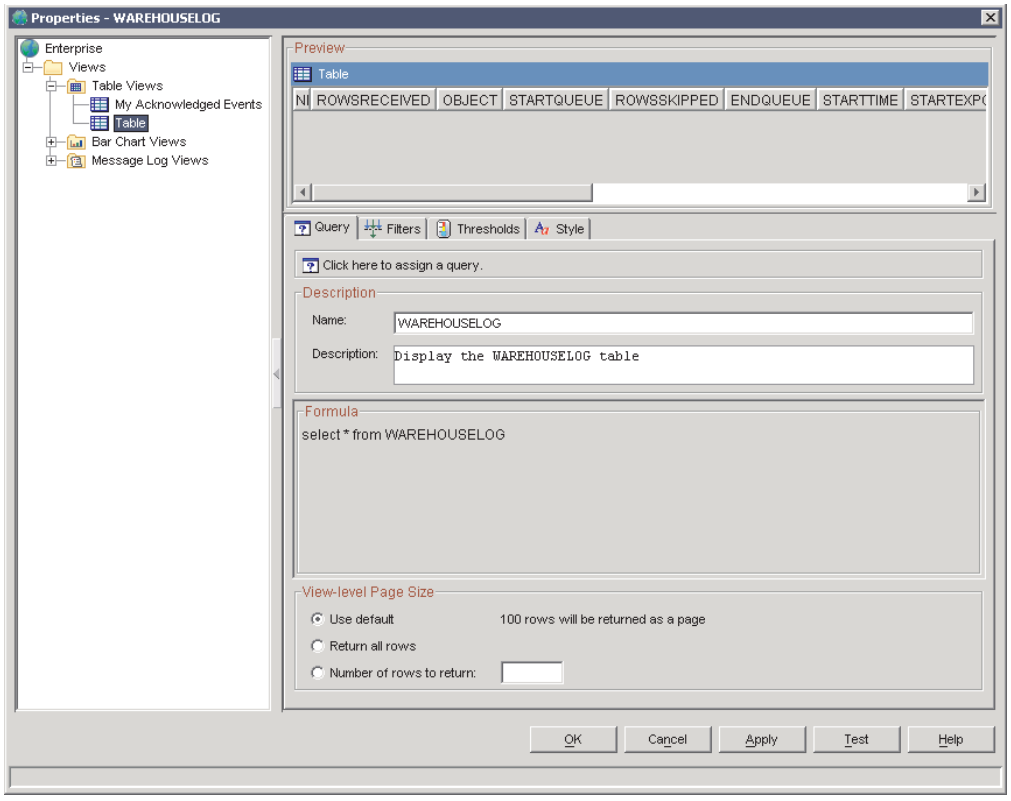


Figure 62. Assigning the WAREHOUSELOG query to a workspace

6. Click **OK** to select the WAREHOUSELOG query for the table and close the Query editor.
7. Click **OK** to close the **Properties** editor.

   The columns of the WAREHOUSELOG table are displayed within the table view in the WAREHOUSELOG workspace. The content of the table is also displayed if the table is not empty.

Tuning the performance of the Warehouse Proxy

You can set the following environment variables to control the way that the Warehouse Proxy works:

- "Database initialization"
- "Work queue"
- "Connection pool" on page 355
- "RPC threads and export requests" on page 355
- "Timeout values" on page 355

You can set that these variables in the KHDENV file.

Database initialization

When the Warehouse Proxy starts, the following tests are done:

- Checks that the Warehouse Proxy can connect to the database.
- If the database is Oracle or DB2, checks that the encoding is set to UTF8.
- If the database is DB2, checks that a bufferpool of page size 8KB is created. If it is not, one is created, along with three new tablespaces that use the 8KB bufferpool. The bufferpool is called "ITMBUF8K" and the tablespaces are named "ITMREG8K," "ITMSYS8K," and "ITMBUF8K."
- Creates a database cache that contains a list of all the tables and columns that exist in the database.

If any of these tests fail, a message is written to the log file and messages are displayed in the Event Viewer.

These tests are repeated every 10 minutes.

You can change this default start up behavior by changing the following environment variables:

KHD_CNX_WAIT_ENABLE
Enables the Warehouse Proxy to wait in between attempts to connect to the database. By default, this variable is set to Y. If you do not want the Warehouse Proxy to wait, change the variable to N. However, this can generate a large log file if the connection to the database fails with each attempt.

KHD_CNX_WAIT
Defines the amount of time, in minutes, that the Warehouse Proxy waits between attempts to connect to the database. The default value is 10 minutes.

Work queue

The work queue consists of a single queue instance and a configurable number of worker threads that run work places on it. There are two primary configuration parameters that you can set. You can set these parameters in the KHDENV file on Windows or the hd.ini file on Linux and UNIX before starting the Warehouse Proxy.

KHD_QUEUE_LENGTH
The length of the KHD work queue. This is an integer that identifies the maximum number of export work requests that can be placed on the work queue before the work queue begins rejecting requests. The default value is 1000. Setting this value to 0 means that the work queue has no limit.

KHD_EXPORT_THREADS
The number of worker threads exporting data to the database. The default value is 10.

Connection pool

The Warehouse Proxy uses several pre-initialized ODBC connections to access the target database. The use of these ODBC connection objects is synchronized through a single connection pool. The connection pool is initialized when the Warehouse Proxy starts.

You can configure the number of connections in the pool by defining the following environment variable in the KHDENV file on Windows or the hd.ini file on Linux and UNIX:

- KHD_CNS_POOL_SIZE: The total number of pre-initialized ODBC connection objects available to the work queue export threads. The default value is 10.

All export worker threads request connections from the connection pool and must obtain a connection before the work of exporting data can continue.

You only see the connections established when a request is active. It is important to set the number of worker threads to greater or equal to the number of ODBC connections. To do this, set `KHD_KHD_EXPORT_THREADS >= KHD_CNX_POOL_SIZE`.

RPC threads and export requests

In addition to the configurable environment variables discussed previously, the standard agent framework provides some control over the scalability and performance profile for the Warehouse Proxy. When the Warehouse Proxy starts, it initializes RPC and registers a group of function pointers that respond to incoming RPC calls.

Use the CTIRA_NCSLISTEN variable to set the number of RPC threads.

Timeout values

You can set two environment variables to control the timeout value. One variable is set on the application agent, the other on the Warehouse Proxy.

- KHD_STATUSTIMEOUT: The time, in seconds, to wait for a status from the Warehouse Proxy before sending an export request again. The default value is 900 seconds, or 15 minutes.
- KHD_SRV_STATUSTIMEOUT: The timeout value, in seconds, for the work queue to perform work. The default value is 600 seconds, or 10 minutes.

Export requests are rejected by the Warehouse Proxy are the following four reasons:

- The time between when an export request is sent to the work queue and when it is extracted from the queue exceeds the timeout. If you have tracing for the Warehouse Proxy set to ERROR, an error similar to the following is logged in the Warehouse Proxy log file:

  ```
  REJECTED: The export for the originnode <OriginNodeName>, the application
  <applicationName> and the table <tableName> has been rejcted for timeout
  reason in stage END_QUEUE.
  ```

- The time between when an export request is sent to the work queue and when the work queue starts to do existence checking in the database exceeds the

timeout. If you have tracing for the Warehouse Proxy set to ERROR, an error similar to the following is logged in the Warehouse Proxy log file and the WAREHOUSELOG table:

```
Sample data rejected for timeout reason at stage START EXPORT
```

- The time between when an export request is sent to the work queue and when the work queue fetches all the rows in the sample exceeds the timeout. If you have tracing for the Warehouse Proxy set to ERROR, a message similar to the following is logged in the Warehouse Proxy log file and the WAREHOUSELOG table:

  ```
  Sample data rejected for timeout reason at stage START SAMPLE
  ```

- The time between when an export request is sent to the work queue and when the work queue commits the rows in the database exceeds the timeout. If you have tracing for the Warehouse Proxy set to ERROR, a message similar to the following is logged in the Warehouse Proxy log file and the WAREHOUSELOG table:

  ```
  Sample data rejected for timeout reason at stage COMMIT
  ```

The KHD_SRV_STATUSTIMEOUT variable should be set less than KHD_STATUSTIMEOUT by at least 60 seconds. Do not change these values unless there is a problem in the environment.

WAREHOUSELOG and WSAREHOUSEAGGRLOG tables

The WAREHOUSELOG table lets you know how many exports succeed and how many failed because of an ODBC error or a timeout value issue.

The WAREHOUSELOG table has the following columns. All times are the local time on the machine where the Warehouse Proxy instance is running.

ORIGINNODE
The name of the computer that made the request. This name is the node name for the agent. For example, Primary::box1:NT.

OBJECT
The attribute group that submitted the request. For example, NT_System.

STARTQUEUE
The time when the request was inserted in the work queue. For example, 10508201154000000.

ENDQUEUE
The time when the request exited the work queue. For example, 10508201155000000.

STARTEXPORT
The amount of time that elapsed before the first row of the sample request was retrieved. For example, 105082011562000000.

EXPORTTIME
The amount of time after the export request transaction was committed. For example, 10508201157000000.

ROWSINSERTED
The number of row inserted in the database for the request. For example, 1000.

ROWSRECEIVED
The number of rows retrieved from the RPC source. For example, 1000.

ROWSSKIPPED
This column is not used.

STARTTIME
The start time of the collection for that sample. For example, 10508150920000000.

ENDTIME
The end time of the collection for that sample. For example, 1050815092000000.

ERRORMSG
An error message when no rows are inserted in the database. The error message can indicate an ODBC error or a TIMEOUT error. For example:

```
Sample data rejected for timeout reason at stage COMMIT EXPORT
```

WPSYSNAME
The name of the Warehouse Proxy Agent that inserted the rows into the database.

The WAREHOUSEAGGRLOG table logs the progress of the Summarization and Pruning agent as it is processing data. Each time the Summarization and Pruning agent executes, it adds an entry for each attribute group (OBJECT column) and origin node (ORIGINNODE column) that was processed. The WSAREHOUSEAGGRLOG table contains the following columns:

ORIGINNODE
The name of the computer that is being summarized. This name is the node name for the agent. For example, Primary::box1:NT. -

OBJECT
The attribute group that was processed.

LOGTMZDIFF
The time zone difference for the Summarization and Pruning agent.

MINWRITETIME
The minimum WRITETIME value that was read from the sample data for the specified ORIGINNODE and OBJECT.

MAXWRITETIME
The maximum WRITETIME value that was read from the sample data for the specified ORIGINNODE and OBJECT

STARTTIME
The time that the Summarization and Pruning agent processing began for the specified ORIGINNODE and OBJECT.

ENDTIME
The time that the Summarization and Pruning agent processing ended for the specified ORIGINNODE and OBJECT.

ROWSREAD
The number of sample data rows read for the specified ORIGINNODE and OBJECT in the time interval MINWRITETIME and MAXWRITETIME.

Part 5. Integrating event management systems

If you are using Tivoli Enterprise Console or Netcool/OMNIbus, in addition to IBM Tivoli Monitoring, to manage events in your enterprise, you can integrate and manage events from a single console.

The *common event console* is a Tivoli Enterprise Portal view that provides an integrated display of events from multiple event systems. The common event console presents normalized events from the supported event systems in a single table. By default, the view displays events reported to a hub Tivoli Enterprise Monitoring Server by Tivoli Enterprise Monitoring Agents (*situation events*); it can also be configured to present events from Tivoli Enterprise Console and Netcool/OMNIbus event systems.

A common event connector (frequently called simply a connector) enables the integrated display of events from an event system in the common event console. The connector retrieves event data from a supported event system and sends user-initiated actions to be run in that event system. To have the events from a specific event system displayed in the common event console, you must configure a connector for that event system. Because the connector for Tivoli Enterprise Monitoring Agents is configured when you install the portal, the common event console includes all situation events by default. However, to have Tivoli Enterprise Console or Netcool/OMNIbus events included in the common event console, you must configure a connector for each of these event systems after you install the Tivoli Enterprise Portal. You might also want to change some of the configuration values for the default connector. For information on configuring the display of events from Tivoli Enterprise Console and Netcool/OMNIbus, see the *IBM Tivoli Monitoring: Administrator's Guide*.

In addition to viewing events from Tivoli Enterprise Console and Netcool/OMNIbus in the Tivoli Enterprise Portal, you can integrate event management by forwarding events reported by Tivoli Enterprise Monitoring Agents to either event system for correlation and management. Changes in event status made on the event system are reflected back to the hub monitoring server that forwarded them. To enable forwarding of situation events, the Tivoli Enterprise Console or Netcool/OMNIbus server (the event server) must be configured to receive the events, a situation update forwarding process must be installed on the event server, situation forwarding must be enabled on the hub monitoring server, and a default event integration facility (EIF) destination must be defined.

The chapters in this section provide instructions for implementing event integration by forwarding situation events to Tivoli Enterprise Console and Netcool/OMNIbus.

After situation forwarding is enabled, by default all situation events are forwarded to the specified event server. However, you can customize which situation events are forwarded and to which event server. For information on specifying which situation events to forward, see the Tivoli Enterprise Portal online help and the *IBM Tivoli Monitoring: User's Guide*.

© Copyright IBM Corp. 2005, 2007

Chapter 17. Setting up event forwarding to Tivoli Enterprise Console

If you are using Tivoli Enterprise Console, you can configure hub monitoring servers to forward situation events to the Tivoli Enterprise Console event server (referred to as the *event server*) for correlation and management.

To view updates to the forwarded situation events in the Tivoli Enterprise Portal, you need to install the event synchronization component on the event server. The event synchronization component enables changes in the event status made on the Tivoli Enterprise Console to be reflected on the Tivoli Enterprise Portal.

The following table provides an overview of the tasks required to configure situation event forwarding and synchronization:

Table 102. Tivoli Enterprise Console event synchronization installation and configuration steps

Task	Where to find information
Plan the deployment of your integration.	"Event integration with Tivoli Enterprise Console" on page 52
Gather information required during the installation and configuration processes.	"Information to gather for event forwarding" on page 60
Install the event synchronization component on your event server.	"Installing event synchronization on your event server" on page 362
Install monitoring agent .baroc files on the event server.	"Installing monitoring agent .baroc files on the event server" on page 377
Configure your monitoring server to forward events to Tivoli Enterprise Console.	"Configuring your monitoring server to forward events" on page 378
Start and stop event synchronization on the event server.	"Starting and stopping the Situation Update Forwarder process" on page 379
Modify the configuration of event synchronization as your monitoring needs change.	"Changing the configuration of the event synchronization component on the event server" on page 379
Define additional monitoring servers to the event server.	"Defining additional monitoring servers to the event server" on page 380
Change the default TCP/IP settings if it is taking a long time to forward events back to the monitoring server.	"Changing the TCP/IP timeout setting on your event server" on page 380

If you are upgrading from IBM Tivoli Monitoring and Tivoli Event Synchronization version 1.x to version 2.0.0.0, see "Upgrading to Tivoli Event Synchronization component version 2.0.0.0" on page 381.

Note: If you have already installed IBM Tivoli Monitoring and Tivoli Event Synchronization, you must upgrade

© Copyright IBM Corp. 2005, 2007

Installing event synchronization on your event server

The installer for the event synchronization component is located in the `/tec` directory of the *IBM Tivoli Monitoring V6.2.0 Tools* DVD.

There are three methods for installing the component:

- "Installing from a wizard" on page 363
- "Installing from the command line" on page 366
- "Installing from the command line using a silent installation" on page 371

When you install the event synchronization component on your event server, the following changes are made:

- If you select to use an existing rule base, the event synchronization .baroc class files (omegamon.baroc and Sentry.baroc [if not present]) and the omegamon.rls rule set file are imported into your existing rule base. If you do not want to modify your existing rule base during the installation, you can choose to manually perform rule base modifications after installation is complete. See "Manually importing the event synchronization class files and rule set" on page 374 for more information.
- For all rule bases that have Sentry.baroc imported, the Sentry2_0_Base class is updated to define additional integration attributes for the situation events received from IBM Tivoli Monitoring.
- A new process, Situation Update Forwarder, is installed along with its supporting binary and configuration files. This process is used to forward updates to the situation events back to the monitoring server. On Windows, a Tivoli Situation Update Forwarder service is also created.

Notes:

1. If your IBM Tivoli Enterprise Console event server is running on Windows 2003 and you are planning to install the event synchronization 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.
2. If you have a monitoring server on an operating system like UNIX or Linux, you must configure your TCP/IP network services in the `/etc/hosts` file to return the fully qualified host name. See "Host name for TCP/IP network services" on page 64 for more information.
3. For a Windows event server, any existing rule base that you use must indicate a relative drive letter (such as C:\) as part of its associated path. To verify that your existing rule base contains a relative drive letter, run the following command from a bash environment on your event server:

   ```
   wrb -lsrb -path
   ```

   If the returned path includes something like *hostname*:*Rulebase_directory*, with no drive letter (such as C:\), copy the `ESync2000Win32.exe` file from the \TEC subdirectory of the IBM Tivoli Monitoring installation image to the drive where the rule base exists and run the installation from that file.
4. If you are using a Windows event server, if you have any rule base with an associated path that does not contain a relative drive letter and that has the Sentry2_0_Base class imported, copy the `ESync2000Win32.exe` file from the \TEC subdirectory of the IBM Tivoli Monitoring installation image to the drive where the rule base exists and run the installation from that file.

To verify if you have any rule bases that have an associated path containing no relative drive letter, run the **wrb -lsrb -path** command as described in the previous note.

To determine if your rule bases have the Sentry2_0_Base class imported, run the following command against all of your rule bases:

```
wrb -lsrbclass rule_base
```

where *rule_base* is the name of the rule base.

Installing from a wizard

Use the following steps to install event synchronization using the installation wizard:

Note: The appearance of the window shown in Figure 63 indicates that the installer did not find an IBM Tivoli Enterprise Console event server installed on the system, so it expects to install event synchronization for Netcool/OMNIbus. If you see this window when you launch the installation, cancel the installation and install the event server on the system before restarting the installer, or install the synchronization component on another system where an event server is installed.

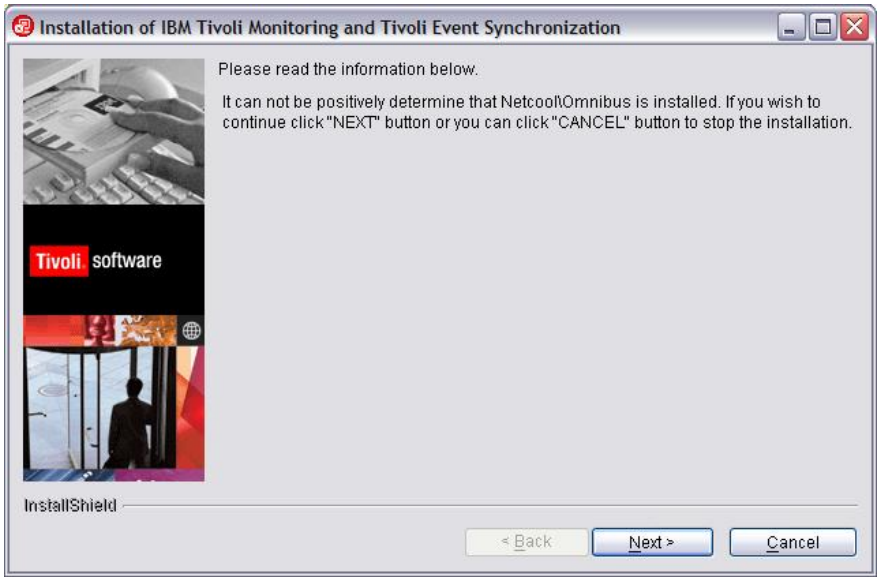


Figure 63. Window shown when no Tivoli Enterprise Console event server is found.

1. On the host of the event server, launch the event synchronization installer from the installation media:

   On Windows, double-click the `ESync2000Win32.exe` file in the `\tec` subdirectory on the IBM Tivoli Monitoring V6.2.0 Tools DVD or DVD image.

   On Linux or UNIX, change to the `\tec` subdirectory of the IBM Tivoli Monitoring V6.2.0 Tools DVD and run the following command:

   ```
   ESync2000<operating_system>.bin
   ```

   where *<operating_system>* is the operating system you are installing on (`aix`, `HP11`, `Linux`, `linux390`, or `Solaris`). For example, run the following command on an AIX computer:

   ```
   ESync2000Aix.bin
   ```

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

Table 103. IBM Tivoli Enterprise Console event synchronization configuration fields

Field	Description
Name of configuration file	The name of the file where event synchronization configuration information is stored. The default name is situpdate.conf.
Number of seconds to sleep when no new situation updates	The polling interval, in seconds. The minimum value is 1, while the default value is 3. If there are no situation events, the Situation Update Forwarder rests for 3 seconds.
Number of bytes to use to save last event	Number of bytes that the long-running process uses 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 CMS 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, http://*hostname*:*port*///cms/soap, where *hostname* is the host name of the monitoring server and *port* is the port.
Rate for sending SOAP requests to CMS from TEC via web services	The maximum number of event updates 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: • Low (default) • Medium • Verbose

5. Complete the following information about the files where events will be written and click **Next**:

Table 104. IBM Tivoli Enterprise Console event synchronization configuration fields, continued

Field	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 (specify 50000 instead of 50,000).
Maximum number of caches files	The maximum number of event caches files at any given time. The minimum value is 2, while the default value is 10. When this value is reached, the oldest file is deleted to make room for a new file.

Table 104. IBM Tivoli Enterprise Console event synchronization configuration fields, continued (continued)

Field	Description
Directory for cache files to be located	The location where event cache files are located. The default locations are as follows: • On Windows: C:\tmp\TME\TEC\OM_TEC\persistence. • On UNIX: /var/TME/TEC/OM_TEC/persistence

6. Type the following information for each monitoring server with which you want to synchronize events and click **Add**. You must specify information for at least one monitoring server.

   Host name
   The fully qualified host name for the computer where the monitoring server is running. This name must match the information that will be in events that are issued from this monitoring server.

   User ID
   The user ID to access the computer where the monitoring server is running.

   Password
   The password to access the computer.

   Confirmation
   The same password, for confirmation.

   You can add information for up to 10 monitoring servers in this wizard. If you want to add additional monitoring servers, add them after you install them by using the steps provided in "Defining additional monitoring servers to the event server" on page 380.
7. When you have provided information about all of the monitoring servers, click **Next**.

   You are presented with the options of having the installer automatically perform rule base modifications, or manually performing the modifications after installation is complete (see Table 105).

Table 105. Options for rule base modification

Option	Description
Automatically install rules and classes	The installation wizard will ask for the rule base into which event synchronization class files and rule set will be imported, and automatically execute the rule base commands to do this.
Manually install rules and classes	The installation wizard will not create or update any rule base with event synchronization files. **Important:** You will have to manually create or update the rule base with event synchronization files after the installation is complete. See "Manually importing the event synchronization class files and rule set" on page 374.

   If you select the automatic option, continue with step 8. If you select the manual option, skip to step 11.
8. Specify the rule base that you want to use to synchronize events. You have two choices:
   - **Create a new rulebase**
   - **Use existing rulebase**

If you select to use an existing rule base, the event synchronization .baroc class files (omegamon.baroc and Sentry.baroc [if not present]) and the omegamon.rls rule set file are imported into your existing rule base. Also, if Sentry.baroc has already been imported into the existing rule base, the Sentry2_0_Base class is extended to define additional integration attributes for the situation events from IBM Tivoli Monitoring.

- 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.

Note: This step is only available if you are creating a new rule base.

9. Click **Next**.
10. If you indicated in the previous step that the installer uses an existing rule base to import the event synchronization class files and rule set, a window is displayed that allows you to specify whether you want the installer to back up the rule base before updating it. If you request a backup, specify both the backup rule base name and backup rule base path. If you leave these fields blank, no backup is made. Click **Next** to proceed to the pre-installation summary panel.
11. Verify the installation location, then click **Next**.

    The installation begins.
12. When the installation and configuration steps are finished, a message telling you to stop and restart the event server is displayed.

    If you chose to have the installer automatically update the rule base, you are offered the option of having the installer restart the event server for you. Check the box to have the installer restart the server. If you want to restart the event server yourself, leave the box unchecked.
13. Click **OK**.
14. 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.

Perform the following tasks after the installation is finished:

- Stop and restart the event server for the configuration changes to take effect.
- Install the monitoring agent .baroc files on the event server as described in "Installing monitoring agent .baroc files on the event server" on page 377.
- Configure the monitoring server to forward events to the event server as described in "Configuring your monitoring server to forward events" on page 378.
- If you did not choose to have the rule base updated automatically, update the rule base as described in "Manually importing the event synchronization class files and rule set" on page 374.

Installing from the command line

Use the following steps to install the event synchronization from the command line on your event server:

1. Change to the tec directory on the IBM Tivoli Monitoring V6.2.0 Tools DVD or DVD image.
2. Run the following command to launch the installation:

   On Windows:

   ```
   ESync2000Win32.exe -console
   ```

   On UNIX or Linux:

   ```
   ESync2000<operating_system>.bin -console
   ```

   where <*operating_system*> is the operating system you are installing on (`aix`, `HP11`, `Linux`, `linux390`, or `Solaris`). For example, run the following command on an AIX computer:

   ```
   ESync2000Aix.bin -console
   ```

   The following prompt is displayed:

   ```
   Press 1 for Next, 3 to Cancel or 4 to Redisplay [3]
   ```
3. Type 1 to start the installation and press Enter.

   The following prompt is displayed:

   ```
   Software Licensing Agreement:
   Press Enter to display the license agreement on your screen. Please
   read the agreement carefully before installing the Program. After
   reading the agreement, you will be given the opportunity to accept it
   or decline it. If you choose to decline the agreement, installation
   will not be completed and you will not be able to use the Program.
   ```
4. Press Enter to display the software license agreement.
5. Type 1 and press Enter to accept the license.

   The following prompt is displayed:

   ```
   Press 1 for Next, 2 for Previous, 3 to Cancel, or 4 to Redisplay [1]
   ```
6. Type 1 and press Enter to continue.

   The following prompt is displayed:

   ```
   Name of configuration file [situpdate.conf]
   ```
7. Press Enter to use the default configuration file, situpdate.conf. If you want to use a different configuration file, type the name and press Enter.

   The following prompt is displayed:

   ```
   Number of seconds to sleep when no new situation updates [3]
   ```
8. Type the number of seconds that you want to use for the polling interval. The default value is 3, while the minimum value is 1. Press Enter.

   The following prompt is displayed:

   ```
   Number of bytes to use to save last event [50]
   ```
9. Type the number of bytes to use to save the last event and press Enter. The default and minimum value is 50.

   The following prompt is displayed:

   ```
   URL of the CMS SOAP server [cms/soap]
   ```
10. Type the URL for the monitoring server SOAP server and press Enter. The default value is cms/soap (which you can use if you set up your monitoring server using the defaults for SOAP server configuration).

    The following prompt is displayed:

    ```
    Rate for sending SOAP requests to CMS from TEC via Web Services [10]
    ```
11. Type maximum number of event updates to send to the monitoring server at one time and press Enter. The default and minimum value is 10.

    The following prompt is displayed:

```
Level of debug for log

[x] 1 low
[ ] 2 med
[ ] 3 verbose

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

12. Type the level of debugging that you want to use and press Enter. The default is Low, indicated by an `x` next to `Low`.
13. Type `0` when you have finished and press Enter.

    The following prompt is displayed:

    ```
    Press 1 for Next, 2 for Previous, 3 to Cancel, or 4 to Redisplay [1]
    ```
14. Type `1` and press Enter to continue.

    The following prompt is displayed:

    ```
    Maximum size of any single cache file, in bytes [50000]
    ```
15. Type the maximum size, in bytes, for the cache file and press Enter. The default is 50000. Do not use commas (,) when specifying this value.

    The following prompt is displayed:

    ```
    Maximum number of cache files [10]
    ```
16. Type the maximum number of cache files to have at one time and press Enter. The default is 10, while the minimum is 2.

    On Windows, the following prompt is displayed:

    ```
    Directory for cache files to reside [C:/tmp/TME/TEC/OM_TEC/persistence]
    ```

    On UNIX, the following prompt is displayed:

    ```
    Directory for cache files to reside [/var/TME/TEC/OM_TEC/persistence]
    ```
17. Type the directory for the cache files and press Enter. The default directory on Windows is C:\tmp\TME\TEC\OM_TEC\persistence; on UNIX, /var/TME/TEC/OM_TEC/persistence.

    The following prompt is displayed:

    ```
    Press 1 for Next, 2 for Previous, 3 to Cancel, or 4 to Redisplay [1]
    ```
18. Type `1` and press Enter to continue.
19. The following prompt is displayed:

    ```
    --- Tivoli Enterprise Monitoring Server 1 ---

    Host name []
    ```

    Type the fully qualified host name for the computer where the monitoring server is running. This name must match the information that is in events issued by this monitoring server. Press Enter.

    The following prompt is displayed:

    ```
    User ID []
    ```
20. Type the user ID to use to access the computer where the monitoring server is running and press Enter.

    The following prompt is displayed:

    ```
    Password:
    ```
21. Type the password to access the computer and press Enter.

    The following prompt is displayed:

    ```
    Confirmation:
    ```
22. Type the password again to confirm it and press Enter.

    The following prompt is displayed:

```
--- Tivoli Enterprise Monitoring Server 2 ---

Host name []
```

23. Repeat steps 19 to 22 for each monitoring server for which you want to receive events on this event server.

    When you have provided information for all the monitoring servers *and* you specified information for less than 10 monitoring servers, press Enter to move through the remaining fields defining additional monitoring servers. Do not specify any additional monitoring server information.

    The following prompt is displayed:

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

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

24. If you want to have the installer automatically install the rules and classes, enter 1 and continue with step 25. If you prefer to manually install the rules and classes, enter 2 and proceed to step 35.
25. When you see the following prompt, type 1 and press Enter to continue:

```
Press 1 for Next, 2 for Previous, 3 to cancel or 4 to Redisplay [1]
```

    The following prompt is displayed:

```
[x] 1 - Create a new rulebase (name and path required)
[ ] 2 - Use Existing Rulebase (path is optional)

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

26. Type 1 to create a new rule base or 2 to use an existing rule base. Press Enter.
27. Type 0 when you are finished and press Enter.
28. If you are creating a new rule base, the following prompt is displayed:

```
Rulebase Name []
```

    type the name for the rule base and press Enter.

    The following prompt is displayed:

```
Rulebase Path []
```

29. If you are creating a new rule base, type the path for the new rule base and press Enter.
30. If you are using an existing rule base, the following prompt is displayed:

```
Rulebase Name []
```

    Type the name of the rule base and press Enter.

31. If you are creating a new rule base, the following prompt is displayed:

```
Existing rulebase name to import: []
```

    If you want to import an existing rule base into the new rule base, type the name of the existing rule base and press Enter.

    The following prompt is displayed:

```
Press 1 for Next, 2 for Previous, 3 to Cancel, or 4 to Redisplay [1]
```

32. Type 1 and press Enter to continue.

    The following prompt is displayed:

```
You indicated on the previous dialog that you want to modify an existing
rule base. If you want this installer to back up the existing rule base
 before modifying it please provide a backup rule base name. Leave backup
 rule base name blank and click Next if you do not want a backup made.

Backup rule base name. []
```

33. Type the name for the backup rule base and press Enter to continue. If you do not want the installer to back up the existing rule base, press Enter without providing a backup rule base name.

    The following prompt is displayed:

    ```
    If you have provided a backup rule base name you must provide a backup
    rule base path. NOTE: We append the backup rule base name to the backup
    rule base path for clarity and easy lookup.

    Backup rule base path. []
    ```

34. Type the path for the backup rule base and press Enter to continue. If you did not provide a name for a backup rule base, press Enter without providing a rule base path.

    The following prompt is displayed:

    ```
    Press 1 for Next, 2 for Previous, 3 to Cancel or 4 to Redisplay [1]
    ```

35. Type 1 and press Enter to continue.

    The event synchronization is installed.

    The following prompt is displayed:

    ```
    Installation and Configuration has completed. Please stop and restart the
    Tivoli Enterprise Console Server.

    Press 1 for Next, 2 for Previous, 3 to Cancel, or 4 to Redisplay [1]
    ```

36. Type 1 and press Enter to continue.

    The following prompt is displayed:

    ```
    Installation and configuration has completed.
    Please restart the Tivoli Enterprise Console server for the changes
    to take effect.
    Mark appropriately below to restart the Tivoli Enterprise Console
    server.
    [ ] 1 - Restart the Tivoli Enterprise Console server to make changes
    effective
    To select an item enter its number, or 0 when you are finished: [0]
    ```

    The option to automatically restart the Tivoli Enterprise Console is presented only if you chose to have the installer automatically update the rules and classes.

37. If you want the installer to stop and restart the Tivoli Enterprise Console server, type 1 and press Enter. If you want to stop and restart yourself, type 0 and press Enter to continue. The following prompt is displayed:

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

38. Type 3 to finish and press Enter.

Perform the following tasks after the installation is finished:

- If you did not have the installer do it, stop and restart the event server for the configuration changes to take effect.
- Install the monitoring agent .baroc files on the event server as described in "Installing monitoring agent .baroc files on the event server" on page 377.
- Configure the monitoring server to forward events to the event server as described in "Configuring your monitoring server to forward events" on page 378.
- If you did not choose to have the rule base updated automatically, update the rule base as described in "Manually importing the event synchronization class files and rule set" on page 374.

Installing from the command line using a silent installation

Use the following steps to install the event synchronization using a silent installation from the command line on your event server. This installation method runs silently, so you will not see status messages during the actual installation.

1. Change to the `tec` directory of the IBM Tivoli Monitoring V6.2.0 Tools DVD or DVD image.
2. Run the following command to generate the configuration file:

   On Windows:

   ```
   ESync2000Win32.exe -options-template filename
   ```

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

   On UNIX:

   ```
   ESync2000<operating_system>.bin -options-template filename
   ```

   where *<operating_system>* is the operating system you are installing on (`Aix, HP11, Linux, linux390, or Solaris`). For example, run the following command on an AIX computer:

   ```
   ESync2000Aix.bin -options-template filename
   ```
3. Edit the output file to specify the following values.

   Notes:

   a. Remove the pound signs (###) from the beginning of any value that you want to specify.

   b. Do not enclose any values in quotation marks (").

   c. You must specify the following values:

      - **configInfoPanel2.fileLocn**
      - Information for at least one monitoring server (the **cmdSvrsPnlNotGuiMode.hostname1**, **cmdSvrsPnlNotGuiMode.userID1**, **cmdSvrsPnlNotGuiMode.pswd1**, and **cmdSvrsPnlNotGuiMode.retypePswd1** values)
      - **rulebasePanel.chooseNewOrExistingRB**
      - **rulebasePanel.rbName**
      - **rbInstallTypePanel.rbInstallType**

      If you are creating a new rule base, **rulebasePanel.rbPath** is also required. If "manual" is specified for rbInstallTypePanel.rbInstallType, all the other rulebasePanel.* options are ignored.

      If you do not specify any of the other values, the default values are used.

   d. The following values are specified only when installing event synchronization on a Netcool/Omnibus Objectserver:

      ```
      ### -P installLocation
      ### -W configInfoPanel3.filesize
      ### -W configInfoPanel3.fileNumber
      ### -W configInfoPanel3.fileLocn
      ```

   e. If you specify values, ensure that the value you specify meets the minimum required values. Otherwise, the installation stops and an error is written to the log file.

Table 106. IBM Tivoli Enterprise Console event synchronization configuration values

Value	Description
installLocation	The directory where you want the product to be installed. If the directory path contains spaces, enclose it in double quotes (" "). For example, to install the product to C:\Program Files\My Product, use `-P installLocation="C:\Program Files \My Product"` Any specified value is ignored if an event server is detected.
configInfoPanel.filename	The name of the file where event synchronization configuration information is stored. The default file name is situpdate.conf.
configInfoPanel.pollingInt	The polling interval, in seconds. The minimum value is 1, while the default value is 3. If there are no situation events, the process that forwards events to IBM Tivoli Enterprise Console rests for 3 seconds.
configInfoPanel.crcByteCnt	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.
configInfoPanel.cmsSoapURL	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, http://*hostname*:*port*///cms/soap, where *hostname* is the host name of the monitoring server and *port* is the port.
configInfoPanel.bufFlushRate	The maximum number of event updates sent to the monitoring server at one time. The minimum (and default) value is 10 events.
configInfoPanel.logLevel	The level of debug information for event synchronization that is logged. You have the following choices: • Low (default) • Medium • Verbose
configInfoPanel2.filesize	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).
configInfoPanel2.fileNumber	The maximum number of event caches files at any given time. The minimum value is 2, while the default value is 10. When this value is reached, the oldest file is deleted to make room for a new file.

Table 106. IBM Tivoli Enterprise Console event synchronization configuration values (continued)

Value	Description
configInfoPanel2.fileLocn	The location where event cache files are located. The default locations are as follows: • On Windows: C:\tmp\TME\TEC\OM_TEC\persistence. • On UNIX: /var/TME/TEC/OM_TEC/persistence
cmsSvrsPnlNotGuiMode.hostname# **Note:** The pound sign (#) stands for a number between 1 and 10. For example, "hostname1".	The host name of each monitoring server that will send events to the event server. Specify up to 10 monitoring servers.
cmsSvrsPnlNotGuiMode.userID#	The user ID for the monitoring server, identified in hostname#, to use to access the computer where the monitoring server is running.
cmsSvrsPnlNotGuiMode.pswd#	The password for the user ID used to access the computer where the monitoring server is running.
cmsSvrsPnlNotGuiMode.retypePswd#	The password confirmation for the user ID.
rbInstallTypePanel.rbInstallType	Specifies whether the installer will automatically update a specified rule base, or if a rule base must be manually modified after installation is complete. Specify either automatic or manual. If manual is specified, all other rulebasePanal.* options are ignored.
rulebasePanel.chooseNewOrExistingRB	Specifies whether you are going to create a new rule base or use an existing rule base. Specify either `new` or `existing`.
rulebasePanel.rbName	The name of the rule base (existing or new).
rulebasePanel.rbPath	The path for the new rule base. There is no default location. You must specify a path.
rulebasePanel.fromRB	If you are creating a new rule base, identify any existing rule bases that you want to import into the new rule base.
bckupERB.backupName	If you want the install to back up an existing rule base before modifying it, specify the name of the back up rule base.
rulebasePanel.backupPath	Specify the directory where the back up rule base should be created.
restartTECQ.restartTEC	Specify whether or not the installer should recycle the event server to implement the changes. Specify `Yes` to have the installer restart the server; specify `No` if you want to restart the server yourself after installation is completed. If the directory path contains spaces, enclose it in double quotes (" "). For example, to install the product to C:\Program Files\My Product, use `-P installLocation="C:\Program Files \My Product"`

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

   On Windows:

   ```
   ESync2000Win32.exe -options filename -silent
   ```

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

   On UNIX:

   ```
   ESync2000<operating_system>.bin -options filename -silent
   ```

   where <*operating_system*> is the operating system you are installing on (`Aix`, `HP11`, `Linux`, `linux390`, `Solaris`). For example, on AIX, run the following command:

   ```
   ESync2000Aix.bin -options filename -silent
   ```

You must stop and restart the event server for these changes to take effect.

When installation is complete, the results are written to the itm_tec_event_sync_install.log file. On UNIX, this log file is always created in the /tmp directory. For Windows, this file is created in the directory defined by the %TEMP% environment variable. To determine where this directory is defined for the current command line window, run the following command:

```
echo %TEMP%
```

If you specified the monitoring servers in the silent installation configuration file, you might consider deleting that file after installation, for security reasons. The passwords specified in the files are not encrypted.

If you want to define additional monitoring servers (in addition to the one required monitoring server), run the sitconfsvruser.sh command as described in "Defining additional monitoring servers to the event server" on page 380. Repeat this command for each monitoring server.

If you specified your monitoring servers after the installation, you must stop and restart the Situation Update Forwarder process manually. See "Starting and stopping the Situation Update Forwarder process" on page 379 for information.

Perform the following tasks after the installation is finished:

- Install the monitoring agent .baroc files on the event server as described in "Installing monitoring agent .baroc files on the event server" on page 377.
- Configure the monitoring server to forward events to the event server as described in "Configuring your monitoring server to forward events" on page 378.
- If you did not choose to have the rule base updated automatically, update the rule base as described in "Manually importing the event synchronization class files and rule set."

Manually importing the event synchronization class files and rule set

If you do not want to permit the installation program to modify your rule base, you can run choose the manual rule base modification option during the installation and then use one of the following methods to manually modify your rule base:

- "Creating a new rule base" on page 375

- "Creating a new rule base and importing an existing rule base into it"
- "Modifying an existing rule base" on page 376

Before you can run any of the commands in the following sections, you must source your Tivoli environment by running the following command:

On Windows, run the following command from a command prompt:

```
C:\Windows\system32\drivers\etc\Tivoli\setup_env.cmd
```

On Linux or UNIX, run the following command from a shell environment:

```
. /etc/Tivoli/setup_env.sh
```

See the *IBM Tivoli Enterprise Console Command and Task Reference* for more information about the **wrb**, **wstopesvr**, and **wstartesvr** commands.

Creating a new rule base

Use the following steps to create a new rule base after you install the event synchronization component:

1. Create the new rule base by running the following command:

   ```
   wrb -crtrb -path <newrb_path> <newrb_name>
   ```

   where *<newrb_path>* is the path to where you want to create the new rule base, and *<newrb_name>* is the name for the new rule base.
2. Import the event synchronization class and rule files into the new rule base from the `$BINDIR/TME/TEC/OM_TEC/rules` directory created during the installation of the event synchronization component. Run the following commands:

   ```
   wrb -imprbclass <path_to_Sentry_baroc_file> <newrb_name>

   wrb -imprbclass <path_to_omegamon_baroc_file <newrb_name>

   wrb -imprbrule <path_to_omegamon_rls_file> <newrb_name>

   wrb -imptgtrule omegamon EventServer <newrb_name>
   ```
3. Compile and load the new rule base by running the following commands:

   ```
   wrb -comprules <newrb_name>

   wrb -loadrb <newrb_name>
   ```
4. Stop and restart the event server by running the following commands:

   ```
   wstopesvr

   wstartesvr
   ```

Creating a new rule base and importing an existing rule base into it

Use the following steps to create a new rule base and import an existing rule base into it:

1. Create the new rule base by running the following command:

   ```
   wrb -crtrb -path <newrb_path> <newrb_name>
   ```

   where *<newrb_path>* is the path to where you want to create the new rule base and *<newrb_name>* is the name for the new rule base.
2. Import the existing rule base into the new rule base by running the following commands:

   ```
   wrb -cprb -overwrite <existing_rbname> <newrb_name>
   ```

where <*existing_rbname*> is the name of the existing rule base that you want to import.

3. If the existing rule base is an older rule base, you must upgrade the tec.baroc file to include the TEC_Generic class. Run the following command:

   ```
   perl $BINDIR/TME/TEC/OM_TEC/bin/upg_tec_baroc.pl <newrb_name>
   ```

4. If the rule base already contains a Sentry.baroc file, you must upgrade it with the event synchronization event class attributes. Run the following command:

   ```
   perl $BINDIR/TME/TEC/OM_TEC/bin/upg_sentry_baroc.pl
   ```

5. If the rule base does not contain a Sentry.baroc file, you must import it from the $BINDIR/TME/TEC/OM_TEC/rules directory created during event synchronization installation. Run the following command:

   ```
   wrb -imprbclass <path_to_Sentry_baroc_file> <newrb_name>
   ```

6. Import the omegamon.baroc and rules file into the rule base from the $BINDIR/TME/TEC/OM_TEC/rules directory created during event synchronization installation. Run the following commands:

   ```
   wrb -imprbclass <path_to_omegamon_baroc_file> <newrb_name>

   wrb -imprbrule <path_to_omegamon_rls_file> <newrb_name>

   wrb -imptgtrule omegamon EventServer <newrb_name>
   ```

7. Compile and load the new rule base by running the following commands:

   ```
   wrb -comprules <newrb_name>

   wrb -loadrb <newrb_name>
   ```

8. Stop and restart the event server by running the following commands:

   ```
   wstopesvr

   wstartesvr
   ```

Modifying an existing rule base

Use the following steps to modify an existing rule base to include the class files and rule set for the event synchronization component:

1. If the existing rule base is an older rule base, you must upgrade the tec.baroc file to include the TEC_Generic class. Run the following command:

   ```
   perl $BINDIR/TME/TEC/OM_TEC/bin/upg_tec_baroc.pl <newrb_name>
   ```

2. If the rule base already contains a Sentry.baroc file, you must upgrade it with the event synchronization event class attributes. Run the following command:

   ```
   perl $BINDIR/TME/TEC/OM_TEC/bin/upg_sentry_baroc.pl
   ```

3. If the rule base does not contain a Sentry.baroc file, you must import it from the $BINDIR/TME/TEC/OM_TEC/rules directory created during event synchronization installation. Run the following command:

   ```
   wrb -imprbclass <path_to_Sentry_baroc_file> <newrb_name>
   ```

4. Import the omegamon.baroc and rules file into the rule base from the $BINDIR/TME/TEC/OM_TEC/rules directory created during event synchronization installation. Run the following commands:

   ```
   wrb -imprbclass <path_to_omegamon_baroc_file> <newrb_name>

   wrb -imprbrule <path_to_omegamon_rls_file> <newrb_name>

   wrb -imptgtrule omegamon EventServer <newrb_name>
   ```

5. Compile and load the new rule base by running the following commands:

   ```
   wrb -comprules <newrb_name>

   wrb -loadrb <newrb_name>
   ```

6. Stop and restart the event server by running the following commands:

   ```
   wstopesvr

   wstartesvr
   ```

Installing monitoring agent .baroc files on the event server

The monitoring server generates Tivoli Enterprise Console events with classes that are unique to each monitoring agent. Each monitoring agent provides a .baroc file with the Tivoli Enterprise Console classes that are generated by IBM Tivoli Monitoring. In order to view this event data in the event console, you must install these monitoring agent .baroc files on the event server.

After you have added application support for each agent to the monitoring server, the monitoring agent .baroc files are located in the following directory:

- On Windows, in the <*itm_installdir*>\cms\TECLIB directory, where <*itm_installdir*> is the directory where you installed IBM Tivoli Monitoring.
- On Linux and UNIX, in the <*itm_installdir*>/tables/<*ms_name*>/TECLIB directory, where <*itm_installdir*> is the directory where you installed IBM Tivoli Monitoring and <*ms_name*> is the name of the monitoring server.

Use the following steps to install the monitoring agent .baroc files on the event server:

1. Copy the monitoring agent .baroc files from the computer where the monitoring server is installed to a temporary directory on the event server computer (for example, /tmp). The location of the agent .baroc files is described above. Do not copy the om_tec.baroc file; this file contains classes that are duplicates of classes in the omegamon.baroc file.
2. Set up the Tivoli Management Framework environment by running the following command:

   On Windows, run the following command:

   ```
   C:\WINDOWS\system32\drivers\etc\Tivoli\setup_env.cmd
   ```

   On Linux and UNIX, run the following command from a shell environment:

   ```
   . /etc/Tivoli/setup_env.sh
   ```

3. For each monitoring agent .baroc file to load into the rule base, run the following command from the same command prompt:

   ```
   wrb -imprbclass /tmp/<agent_baroc_file> <rb_name>
   ```

   where:

   /tmp/<*agent_baroc_file***>**
   Specifies the location and name of the monitoring agent .baroc file. The example above uses the /tmp directory as the location.

   rb_name
   The name of the rule base that you are using for event synchronization.

4. Compile and load the rule base by running the following commands

   ```
   wrb -comprules <rb_name>

   wrb -loadrb <rb_name>
   ```

5. Stop and restart the event server by running the following commands:

   ```
   wstopesvr

   wstartesvr
   ```

When you have loaded each of the agent .baroc files into the rule base and restarted the event server, the event server is ready to receive and correctly parse any events it receives from the monitoring server from one of the installed monitoring agents.

See the *IBM Tivoli Enterprise Console Command and Task Reference* for more information about the **wrb**, **wstopesvr**, and **wstartesvr** commands.

Configuring your monitoring server to forward events

Before the monitoring server forwards any situation events to Tivoli Enterprise Console, you have to enable that forwarding of events. Use the following steps to enable event forwarding on your monitoring server.

For Windows monitoring servers *only*, do the following:

1. Open Manage Tivoli Monitoring Services.
2. Right-click the monitoring server and click **Reconfigure**.
3. On the configuration options window, select **Tivoli Event Integration Facility**.
4. Click **OK** and **OK**.
5. Complete the following fields on the Event Server: Location and Port Number window and click **OK**:

   Server or EIF Probe Location
   Type the host name or IP address for the computer where the IBM Tivoli Enterprise Console event server is installed.

   Port Number
   Type the port number for the event server. If the event server is using port mapping, set this value to 0. If the event server was configured to use a specific port number, specify that number.

   To determine the port number that the event server is using, search for the `tec_recv_agent_port` parameter in the .tec_config file in the *$BINDIR*/TME/TEC directory on the event server. If the parameter is commented out with a pound sign (#), the event server is using port mapping. If it is not, the event server is using the port number specified by this parameter.

For UNIX monitoring servers: You configured the TEC Server and TEC Port information for the UNIX monitoring server during installation, if you installed the monitoring server using the configuration instructions in this installation guide. However, if you did not configure this information, see "Configuring the hub monitoring server" on page 120 for the procedure.

Note: If you already have policies that contain emitter activities that send events to the Tivoli Enterprise Console, turning on Tivoli Event Integration event forwarding will result in duplicate events. You can deactivate the emitter activities within policies so you do not have to modify all your policies when you activate Tivoli Event Integration Facility forwarding by specifying **Disable Workflow Policy/Tivoli Emitter Agent Event Forwarding** when you enable forwarding using the Event Integration Facility.

Using policies gives you more control over which events are sent and you may not want to lose this granularity. Moreover, it is likely the policies that are invoking the TEC emitter are doing little else. If you deactivate these activities, there is no point in running the policy. You may prefer to delete

policies that are longer required, instead of disabling them. Note that events forwarded via the TEC event emitter are not eligible for event synchronization (that is, changes to these events on the TEC side will not be sent back to the monitoring server).

Starting and stopping the Situation Update Forwarder process

To send event updates to a monitoring server, you must start the Situation Update Forwarder. This process is started automatically when the event server starts. To start the process manually, change to the *$BINDIR*/TME/TEC/OM_TEC/bin directory (where *$BINDIR* is the location of the Tivoli Management Framework installation) and run the following command:

On Windows:

```
startSUF.cmd
```

On UNIX:

```
startSUF.sh
```

To stop the process, 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
```

Changing the configuration of the event synchronization component on the event server

If you want to change any of the settings for the event synchronization on the event server, use the **sitconfig.sh** command. You have two options for running this command:

- Manually modify the configuration file for event synchronization (named situpdate.conf by default and located in the /etc/TME/TEC/OM_TEC directory on UNIX and Linux, and the %SystemDrive%\Program Files\TME\TEC\OM_TEC\etc directory on Windows), and then run the following command:

  ```
  sitconfig.sh update filename=<config_filename>
  ```

- Run the **sitconfig.sh** command directly, specifying only those settings that you want to change. See *IBM Tivoli Monitoring Command Reference* for the full syntax of this command.

After you change the configuration of the event synchronization, you must manually stop and restart the Situation Update Forwarder process. See “Starting and stopping the Situation Update Forwarder process” for information.

Defining additional monitoring servers to the event server

To add additional monitoring servers to the list from which you want to receive events, run the following sitconfsvruser.sh command as follows:

1. Source your Tivoli environment by running the following command:
   - On Windows, run the following command from a command prompt:
     ```
     C:\Windows\system32\drivers\etc\Tivoli\setup_env.cmd
     ```
   - On operating systems like UNIX and Linux, run the following command from a shell environment:
     ```
     . /etc/Tivoli/setup_env.sh
     ```
2. On Windows, type BASH to invoke the bash shell.
3. Change to the $BINDIR/TME/TEC/OM_TEC/bin directory (where $BINDIR is the location of the Tivoli Management Framework installation) and enter the following command:
   ```
   sitconfsvruser.sh add serverid=server userid=user password=password
   ```

   where:

   serverid=*server*
   The fully qualified host name of the monitoring server.

   userid=*user*
   The user ID to access the computer where the monitoring server is running.

   password=*password*
   The password to access the computer.

Repeat this command for each monitoring server.

You can also delete monitoring servers. See *IBM Tivoli Monitoring Command Reference* for the full syntax of this command.

After you change the configuration of the event synchronization, you must manually stop and restart the Situation Update Forwarder process. See "Starting and stopping the Situation Update Forwarder process" on page 379 for information.

Changing the TCP/IP timeout setting on your event server

If the Situation Update Forwarder cannot reach a monitoring server to send an update, depending on the TCP/IP settings for the computer where your event server is running, you might have to wait up to 15 minutes before the Situation Update Forwarder tries to connect to the monitoring server again. This might occur if your event server is running on an AIX, Solaris, or HP-UX computer.

Use the following steps to change the TCP/IP timeout value for your computer.

On AIX, run the following command:

```
no -o tcp_keepinit=<timeout_value>
```

where <*timeout_value*> is the length of the timeout period, in half seconds. To configure a timeout of 30 seconds, set the <*timeout_value*> value to 60.

On Solaris and HP-UX, run the following command:

```
ndd -set /dev/tcp tcp_ip_abort_cinterval <timeout_value>
```

where <*timeout_value*> is the length of the timeout period, in milliseconds. To configure a timeout of 30 seconds, set the <*timeout_value*> value to 30000.

Upgrading to Tivoli Event Synchronization component version 2.0.0.0

Upgrading replaces the omegamon.rls file. Any changes you have made to this file will be lost. However, a backup file named omegamon.rls.bac is created, so that you can recover your changes. You must load the non-current rule base and restart the Tivoli Enterprise Console event server after updating either the noncurrent or the current rule base.

You install the upgrade from the IBM Tivoli Monitoring installation media.

There are three methods for upgrading event synchronization:

- "Upgrading from a wizard"
- "Upgrading from the command line" on page 383
- "Upgrading from the command line using a silent installation" on page 384

If you have multiple rule bases that are using IBM Tivoli Monitoring and Tivoli Event Synchronization, you can run the upgrade installation to update each rule base. After you finish the first rule base, restart the upgrade installer and supply the targeted next rule base you want to update.

Note: You cannot uninstall just the upgrade. You must uninstall the entire product. For instructions on uninstalling, see "Uninstalling the event synchronization component" on page 450

Upgrading from a wizard

Use the following steps to upgrade event synchronization from the installation wizard:

1. On the host of the event server, launch the event synchronization upgrade installation:

   On Windows, double-click the `ESUpgradeWin1x2win32.exe` file in the `tec` subdirectory on the IBM Tivoli Monitoring V6.2.0 Tools DVD or DVD image.

   On Linux or UNIX, change to the `tec` subdirectory on the IBM Tivoli Monitoring V6.2.0 Tools DVD or DVD image and run the following command:

   ```
   ESUpgrade1x2<operating_system>.bin
   ```

   where <*operating_system*> is the operating system you are installing on (`aix`, `HP11`, `Linux`, `linux390`, or `Solaris`). For example, run the following command on an AIX computer:

   ```
   ESUpgrade1x2Aix.bin
   ```

2. Click **Next** on the Welcome window.
3. Select **I accept the terms in the license agreement** and click **Next**.

   You are presented with the option of having the installer automatically update the rule base for you.
4. Select whether you want to have the installer update the rule base or whether you prefer to update it manually after the installation is complete, then click **Next**.

If you chose to manually update the rule base, you will see a progress indicator for the installation. Proceed to step 9. If you chose to have the installer automatically update the rule base, the data collection window shown in Figure 64 is displayed:

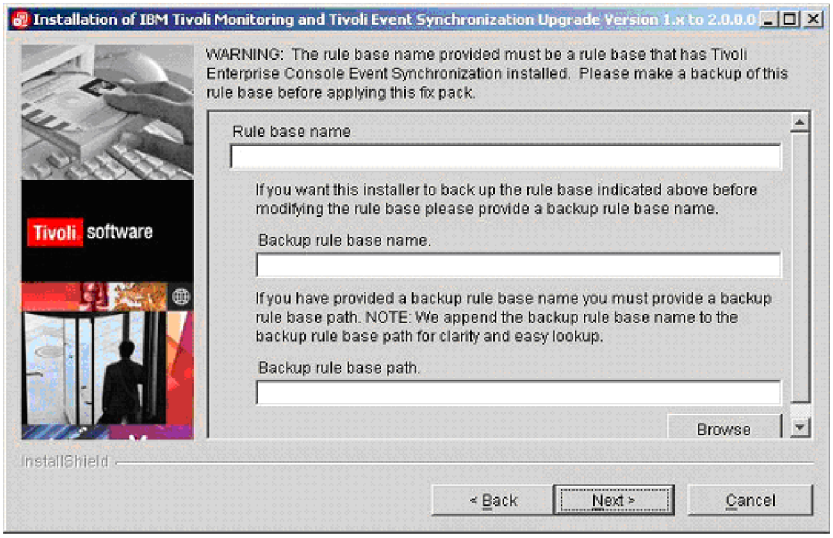


Figure 64. Upgrade data collection window

Proceed to step 5.

5. Specify the name of the rule base to be upgraded. The rule base must be one that has event synchronization previously installed.
6. If you want the installer to back up the rule base before it is modified, specify a name and a path for the backup rule base.
7. Click **Next** to continue.

   A window is displayed which summarizes the information you entered.
8. If the information is correct, click **Next** to proceed with the installation. If the information is not correct, click **Back** and correct the fields as necessary, then click **Next** and **Next** again to proceed.

   A progress indicator shows the progress of the installation and configuration.
9. When the installation completes successfully, you will see a message which reminds you to restart the TEC server. If the updated rule base is not the currently loaded rule base, you are reminded to load the rule base and restart the server. Click **OK** to dismiss the message.

   A window is displayed which reminds you to restart the Tivoli Enterprise Console server.
10. If you want the installer to restart the server for you, check Restart the Tivoli Enterprise Console server to make changes effective, then click **Next**. If you do not want the installer to restart the server, leave the option unchecked and click **Next**.
11. Click **Finish** to exit the installer.

Important:: If you chose the manual update option, you must copy the files in `$BINDIR/TME/TEC/OM_TEC/rules` directory to the rule base, recompile and reload the rule base, and restart the Tivoli Enterprise Console. Refer to "Manually importing the event synchronization class files and rule set" on page 374 for the commands to use to do this.

Upgrading from the command line

Use the following steps to upgrade event synchronization from the command line on your event server:

1. Change to the `tec` directory on the IBM Tivoli Monitoring V6.2.0 Tools DVD or DVD image.
2. Run the following command to launch the installation:

   On Windows:

   ```
   ESUpgrade1x2Win32.exe -console
   ```

   On UNIX or Linux operating systems:

   ```
   ESUpgrade1x2<operating_system>.bin -console
   ```

   where *<operating_system>* is the operating system you are installing on (`Aix`, `HP11`, `Linux`, `linux390`, or `Solaris`). For example, run the following command on an AIX computer:

   ```
   ESUpgrade1x2Aix.bin -console
   ```

   The following prompt is displayed:

   ```
   Press 1 for Next, 3 to Cancel or 4 to Redisplay [1]
   ```

3. Type 1 to start the installation and press Enter.

   The following prompt is displayed:

   ```
   Software Licensing Agreement:
   Press Enter to display the license agreement on your screen. Please
   read the agreement carefully before installing the Program. After
   reading the agreement, you will be given the opportunity to accept it
   or decline it. If you choose to decline the agreement, installation
   will not be completed and you will not be able to use the Program.
   ```

4. Press Enter to display the software license agreement.
5. Type 1 and press Enter to accept the license.

   The following prompt is displayed:

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

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

6. If you want to have the installer automatically install the rules and classes, enter 1. The following prompt is displayed:

   ```
   Rule base Name []
   ```

   Continue with step 7. If you prefer to manually install the rules and classes, enter 2 and proceed to step 11.
7. Type 1 and press Enter to continue.
8. Type the name of the rule base to upgrade then press Enter.

   The rule base must be one in which event synchronization was previously installed.

   The following prompt is displayed:

   ```
   Backup rule base name. []
   ```

9. If you want the installer to back up the rule base before modifying it, type a name for the back up rule base, then press Enter. If you do not want the installer to create a back up rule base, press Enter without typing any name. If you provide a name for the back up rule base, you are prompted for the path for the back up rule base:

```
If you have provided a backup rule base name you must provide a backup
rule base path. NOTE: We append the backup rule base name to the
backup rule base path for clarity and easy look-up.

Backup rule base path. []
```

10. Type the path and press Enter. The following prompt is displayed:

```
Press 1 for Next, 2 for Previous, 3 to Cancel, or 4 to Redisplay []
```

11. Type 1 and press Enter to continue.

    The following prompt is displayed:

```
IBM Tivoli Monitoring

Press 1 for Next, 2 for Previous, 3 to Cancel, or 4 to Redisplay [1]
```

12. Type 1 and press Enter to continue.

    The event synchronization is installed. The following prompt is displayed:

```
Installation and Configuration has completed. Please stop
and restart the Tivoli Enterprise Console Server.

Press 1 for Next, 2 for Previous, 3 to Cancel, or 4 to Redisplay [1]
```

13. Type 1 and press Enter to continue.

    The following prompt is displayed:

```
Installation and configuration has completed.
Please restart the Tivoli Enterprise Console server for the changes
to take effect.

Mark appropriately below to restart the Tivoli Enterprise Console
server.
[ ] 1 - Restart the Tivoli Enterprise Console server to make changes
effective

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

    If you did not chose to have the installer automatically update the rule base, you will not be offered the option of restarted the Tivoli Enterprise Console automatically.

14. If you want the installer to stop and restart the Tivoli Enterprise Console server, type 1 and press Enter. If you want to stop and restart yourself, type 0 and press Enter to continue. The following prompt is displayed:

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

15. Type 3 to finish and press Enter.

You must stop and restart the event server for these changes to take effect.

Important:: If you chose the manual update option, you must copy the files in `$BINDIR/TME/TEC/OM_TEC/rules` directory to the rule base, recompile and reload the rule base, and restart the Tivoli Enterprise Console. Refer to "Manually importing the event synchronization class files and rule set" on page 374 for the commands to use to do this.

Upgrading from the command line using a silent installation

If you have already installed Fix Pack 1, be aware that if you define the rulebasePanel.rbName, this silent installation will update the rule base. If you do not want to apply the updated rules file to a rule base leave the rulebasePanel.rbName commented out (do not delete the pound signs ### preceding the parameter).

Use the following steps to install the event synchronization using a silent installation from the command line on your event server. This installation method runs silently, so you will not see status messages during the actual installation.

1. Change to the `tec` directory on the IBM Tivoli Monitoring V6.2.0 Tools DVD or DVD image.
2. Run the following command to generate the configuration file:

   On Windows:

   ```
   ESUpgrade1x2Win32.exe -options-template filename
   ```

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

   On UNIX:

   ```
   ESUpgrade1x2<operating_system>.bin -options-template filename
   ```

   where <*operating_system*> is the operating system you are installing on (`Aix`, `HP11`, `Linux`, `linux390`, or `Solaris`). For example, run the following command on an AIX computer:

   ```
   ESUpgrade1x2Aix.bin -options-template filename
   ```

3. Edit the output file to specify the following values.

   rbInstallTypePanel.rbInstallType
   Specifies whether the installer will automatically update a specified rule base, or if a rule base must be manually modified after installation is complete. Specify either automatic or manual. If manual is specified, all other rulebasePanel.* options are ignored.

   rulebasePanel.rbName
   The name of the rule base to be updated.

   rulebasePanel.backupName
   The name of the backup rule base.

   rulebasePanel.backupPath
   The path for the backup rule base.

   restartTEC.startTEC
   Indicates that you want the installer to restart the Tivoli Enterprise Console event server.

   Notes:

   a. Remove the pound signs (###) from the beginning of any value that you want to specify.
   b. Do not enclose any values in quotation marks (").
   c. Specify the following value only if you want the indicated rule base updated:

      ```
      rulebasePanel.rbName
      ```

   d. If you specify values, ensure that the value you specify meets the minimum required values. Otherwise, the installation stops and an error is written to the log file.

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

   On Windows:

   ```
   ESUpgrade1x2Win32.exe -options filename -silent
   ```

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

On UNIX:

```
ESUpgrade1x2<operating_system>.bin -options filename -silent
```

where <*operating_system*> is the operating system you are installing on (`Aix`, `HP11`, `Linux`, `linux390`, `Solaris`). For example, on AIX, run the following command:

```
ESUpgrade1x2Aix.bin -options filename -silent
```

The rule base that is updated during silent installation is made current.

Important:: If you chose the manual update option, you must copy the files in `$BINDIR/TME/TEC/OM_TEC/rules` directory to the rule base, recompile and reload the rule base, and restart the Tivoli Enterprise Console. Refer to "Manually importing the event synchronization class files and rule set" on page 374 for the commands to use to do this.

Chapter 18. Setting up event forwarding to Netcool/OMNIbus

If you are already using Netcool/OMNIbus to monitor events from other sources in your enterprise, you can also view and manage situation events from a Tivoli Enterprise Monitoring Server in the Netcool/OMNIbus console. Event integration requires Netcool/OMNIbus V7.x and Netcool/OMNIbus V7.x Probe for Tivoli EIF.

Situation events are sent to Netcool/OMNIbus Probe for Tivoli EIF using the Tivoli Event Integration Facility (EIF) interface. The Netcool/OMNIbus EIF Probe receives events, maps them to and then inserts into Netcool/OMNIbus Server. When an Netcool/OMNIbus user acknowledges, closes, or reopens a situation event, Netcool/OMNIbus sends those changes to the originating monitoring server (see Figure 65).

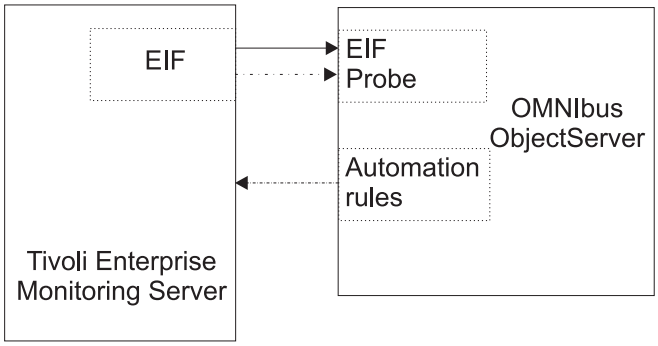


Figure 65. Event flow and synchronization between Tivoli Monitoring and Netcool/OMNIbus

Setting up event integration for Netcool/OMNIbus involves four tasks:

- "Installing the event synchronization component" on page 388

  The event synchronization component enables changes in event status made on a Netcool/OMNIbus Objectserver to be sent back to the Tivoli Enterprise Monitoring Server and reflected on the Tivoli Enterprise Portal. When you install the event synchronization component for Netcool/OMNIbus, a new process, Situation Update Forwarder, is installed along with its supporting binary and configuration files. This process is used to forward updates to the situation events back to the originating monitoring server. On Windows, a Situation Update Forwarder service is also created.
- "Configuring the Netcool/OMNIbus event server" on page 397

  You configure the Netcool/OMNIbus server to receive situation event information and reflect changes to their status to the Netcool/OMNIbus console. You also configure the Objectserver to send changes in event status back from Netcool/OMNIbus to the monitoring server.
- "Configuring the monitoring server" on page 402

  You configure the hub Tivoli Enterprise Monitoring Server monitoring server to enable situation event forwarding and to define the default event receiver.
- "Customizing the OMNIbus configuration" on page 403

  After you have set up event integration, you can customize:
  - How events are mapped
  - How events are synchronized

© Copyright IBM Corp. 2005, 2007

- "Defining additional monitoring servers to the event server" on page 403

  By default, all situations are forwarded to the default EIF destination defined when you configured the monitoring server, but you can configure additional destinations (EIF probes), and selectively forward events to different destinations. See the *IBM Tivoli Monitoring: Administrator's Guide* for more information.

The following products must be installed and configured before you install the event synchronization component and configure event forwarding for Netcool/OMNIbus:

- Netcool/OMNIbus V7.x
- Netcool/OMNIbus V7.x probe for Tivoli EIF
- IBM Tivoli Monitoring V6.2

Installing the event synchronization component

You install event synchronization on the host of the Netcool/OMNIbus Objectserver using the IBM Tivoli Monitoring V6.2.0 Tools DVD or DVD image. Installing event synchronization installs a new process, Situation Update Forwarder, and its supporting binary and configuration files. This process is used to forward updates to the situation events back to the monitoring server. On Windows, a Situation Update Forwarder service is also created.

If you are forwarding situation events to multiple Objectservers, install event synchronization on each server.

There are three methods for installing the event synchronization component:

- "Installing from a wizard"
- "Installing from the command line" on page 391
- "Installing from the command line using a silent installation" on page 394

Notes:

1. You cannot install event synchronization for Netcool/OMNIbus on the same system as an IBM Tivoli Enterprise Console event server.
2. If the Objectserver is running on Windows 2003 and you are planning to install the event synchronization 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, which 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.
3. If you have a monitoring server on an operating system like UNIX or Linux, you must configure your TCP/IP network services in the `/etc/hosts` file to return the fully qualified host name. See "Host name for TCP/IP network services" on page 64 for more information.

Installing from a wizard

Take the following steps to install event synchronization using the installation wizard:

1. On the computer where the Objectserver is installed, launch the event synchronization installation:
   - On Windows, double-click the `ESync2000Win32.exe` file in the `tec` subdirectory on the IBM Tivoli Monitoring V6.2.0 Tools DVD or DVD image.

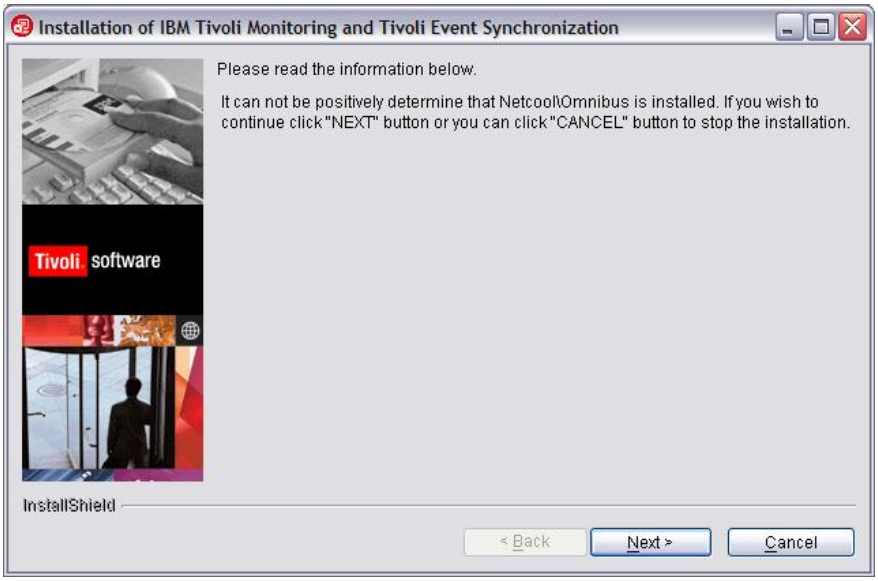
- On Linux or UNIX operating systems, change to the `tec` subdirectory on the IBM Tivoli Monitoring V6.2.0 Tools DVD or DVD image and run the following command:

  `ESync2000<operating_system>.bin`

  where *<operating_system>* is the operating system you are installing on (`aix`, `HP11`, `Linux`, `linux390`, or `Solaris`). For example, run the following command on an AIX computer:

  `ESync2000Aix.bin`

  If the installer cannot locate OMNIbus in its usual place, the following window is displayed. Click **Next** to continue installing the event synchronization:



2. Click **Next** on the Welcome window.
3. Review the license agreement, select **I accept the terms in the license agreement** and click **Next**.
4. Click **Next** to install the synchronization component in the default location, or use the **Browse** button to select another location and then click **Next** to continue.
5. Complete the fields in the installation windows using the configuration values described in Table 107 and click **Next**.

Table 107. Netcool/OMNIbus event synchronization configuration fields

Field	Description
Name of configuration file	The name of the file where event synchronization configuration information is stored. The default name is `situpdate.conf`.
Number of seconds to sleep when no new situation updates	The polling interval, in seconds. The minimum value is 1, while the default value is 3. If there are no situation events, the Situation Update Forwarder rests for 3 seconds.

Table 107. Netcool/OMNIbus event synchronization configuration fields (continued)

Field	Description
Number of bytes to use to save last event	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 CMS 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, `http://`*`hostname`*`:`*`port`*`///cms/soap`, where *hostname* is the host name of the monitoring server and *port* is the port.
Rate for sending SOAP requests to the monitoring server from the OMNIbus probe via web services	The maximum number of event updates 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: • Low (default) • Medium • Verbose

6. Complete the fields on the installation window about the files where events will be written using the values described in Table 108 and click **Next**:

Table 108. Netcool/OMNIbus event synchronization configuration fields, continued

Field	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 (specify 50000 instead of 50,000).
Maximum number of caches files	The maximum number of event caches files at any given time. The minimum value is 2, while the default value is 10. When this value is reached, the oldest file is deleted to make room for a new file.
Directory for cache files to be located	The location where event cache files are located. The default locations are as follows: • On Windows: `C:\Program Files\IBM\SitForwarder\persistence`. • On UNIX: `/opt/IBM/TEC/SitForwarder/persistence`

7. Type the following information for each hub monitoring server with which you want to synchronize events and click **Add**. You must specify information for at least one hub monitoring server.

   Host name
   The fully qualified host name for the computer where the monitoring

server is running. The name must match the information that will be in events coming from this monitoring server.

User ID
The user ID to access the computer where the monitoring server is running.

Password
The password to access the computer.

Confirmation
The password, again.

You can add information for up to 10 monitoring servers in this wizard. If you want to add additional monitoring servers, do so after install by using the steps provided in "Defining additional monitoring servers to the event server" on page 380.

8. When you have provided information about all of the monitoring servers, click **Next**.

   A summary window is displayed.

9. Click **Next** to proceed.

   The installation begins and a progress indicator is displayed. When the installation is completed, a message is displayed telling you that the installation has been successful.

10. Click **Finish** to exit the wizard.

Note: If any configuration errors occurred during installation and configuration, you are directed to a log file that contains additional troubleshooting information.

Installing from the command line

Use the following steps to install the event synchronization from the command line on your event server:

1. Change to the `tec` directory on the IBM Tivoli Monitoring V6.2.0 Tools DVD or DVD image.
2. Run the following command to launch the installation:

   On Windows:

   ```
   ESync2000Win32.exe -console
   ```

   On UNIX or Linux:

   ```
   ESync2000<operating_system>.bin -console
   ```

   where *<operating_system>* is the operating system you are installing on (`aix`, `HP11`, `Linux`, `linux390`, or `Solaris`). For example, run the following command on an AIX computer:

   ```
   ESync2000Aix.bin -console
   ```

   The following prompt is displayed:

   ```
   Press 1 for Next, 3 to Cancel or 4 to Redisplay [1]
   ```

3. Type 1 to start the installation and press Enter.

   The following prompt is displayed:

   ```
   Software Licensing Agreement:
   Press Enter to display the license agreement on your screen. Please
   read the agreement carefully before installing the Program. After
   reading the agreement, you will be given the opportunity to accept it
   or decline it. If you choose to decline the agreement, installation
   will not be completed and you will not be able to use the Program.
   ```

4. Press Enter to display the software license agreement.
5. Type 1 and press Enter to accept the license.

   The following prompt is displayed:

   ```
   Press 1 for Next, 2 for Previous, 3 to Cancel, or 4 to Redisplay [1]
   ```
6. Type 1 and press Enter to continue.

   The following prompt is displayed:

   ```
   Name of configuration file [situpdate.conf]
   ```
7. Press Enter to use the default configuration file, situpdate.conf. If you want to use a different configuration file, type the name and press Enter.

   The following prompt is displayed:

   ```
   Number of seconds to sleep when no new situation updates [3]
   ```
8. Type the number of seconds that you want to use for the polling interval. The default value is 3, while the minimum value is 1. Press Enter.

   The following prompt is displayed:

   ```
   Number of bytes to use to save last event [50]
   ```
9. Type the number of bytes to use to save the last event and press Enter. The default and minimum value is 50.

   The following prompt is displayed:

   ```
   URL of the CMS SOAP server [cms/soap]
   ```
10. Type the URL for the monitoring server SOAP Server and press Enter. The default value is cms/soap (which you can use if you set up your monitoring server using the defaults for SOAP server configuration).

    The following prompt is displayed:

    ```
    Rate for sending SOAP requests to CMS from TEC via Web Services [10]
    ```
11. Type maximum number of event updates to send to the monitoring server at one time and press Enter. The default and minimum value is 10.

    The following prompt is displayed:

    ```
    Level of debug for log

    [x] 1 low
    [ ] 2 med
    [ ] 3 verbose

    To select an item enter its number, or enter 0 when you are finished: [0]
    ```
12. Type the level of debugging that you want to use and press Enter. The default is Low, indicated by an x next to Low.
13. Type 0 when you have finished and press Enter.

    The following prompt is displayed:

    ```
    Press 1 for Next, 2 for Previous, 3 to Cancel, or 4 to Redisplay [1]
    ```
14. Type 1 and press Enter to continue.

    The following prompt is displayed:

    ```
    Maximum size of any single cache file, in bytes [50000]
    ```
15. Type the maximum size, in bytes, for the cache file and press Enter. The default is 50000. Do not use commas (,) when specifying this value.

    The following prompt is displayed:

    ```
    Maximum number of cache files [10]
    ```
16. Type the maximum number of cache files to have at one time and press Enter. The default is 10, while the minimum is 2.

    On Windows, the following prompt is displayed:

```
Directory for cache files to reside [C:/tmp/TME/TEC/OM_TEC/persistence]
```

On UNIX, the following prompt is displayed:

```
Directory for cache files to reside [/var/TME/TEC/OM_TEC/persistence]
```

17. Type the directory for the cache files and press Enter. The default directory on Windows is `C:\Program Files\IBM\SitForwarder\persistence`; on UNIX, `/opt/IBM/SitForwarder/persistence`.

    The following prompt is displayed:

    ```
    Press 1 for Next, 2 for Previous, 3 to Cancel, or 4 to Redisplay [1]
    ```

18. Type 1 and press Enter to continue.
19. The following prompt is displayed:

    ```
    --- Tivoli Enterprise Monitoring Server 1 ---

    Host name []
    ```

    Type 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. Press Enter.

    The following prompt is displayed:

    ```
    User ID []
    ```

20. Type the user ID to use to access the computer where the monitoring server is running and press Enter.

    The following prompt is displayed:

    ```
    Password:
    ```

21. Type the password to access the computer and press Enter.

    The following prompt is displayed:

    ```
    Confirmation:
    ```

22. Type the password again to confirm it and press Enter.

    The following prompt is displayed:

    ```
    --- Tivoli Enterprise Monitoring Server 2 ---

    Host name []
    ```

23. Repeat steps 19 to 22 for each monitoring server for which you want to receive events on this event server.

    When you have provided information for all the monitoring servers *and* you specified information for less than 10 monitoring servers, press Enter to move through the remaining fields defining additional monitoring servers. Do not specify any additional monitoring server information.

24. When you see the following prompt, type 1 and press Enter to continue:

    ```
    Press 1 for Next, 2 for Previous, 3 to cancel or 4 to Redisplay [1]
    ```

    The event synchronization is installed. The following prompt is displayed:

    ```
    IBM Tivoli Monitoring and Tivoli Enterprise Console Event
    Synchronization will
    be installed in the following location:

    /opt/IBM/SitForwarder

    for a total size:

    101.3 MB

    Press 1 for Next, 2 for Previous, 3 to Cancel or 4 to Redisplay [1]
    ```

25. Type 1 and press Enter to continue.

The following prompt is displayed:

```
The InstallShield Wizard has successfully installed IBM Tivoli
Monitoring and Tivoli Enterprise Console Event Synchronization.
Choose Finish to exit the wizard.
Press 3 to Finish, or 4 to Redisplay [1]
```

26. Type 3 to finish and press Enter.

Installing from the command line using a silent installation

Use the following steps to install the event synchronization using a silent installation from the command line on your event server. This installation method runs silently, so you will not see status messages during the actual installation.

1. Change to the tec directory on the IBM Tivoli Monitoring V6.2.0 Tools DVD or DVD image.
2. Run the following command to generate the configuration file:

   On Windows:

   ```
   ESync2000Win32.exe -options-template filename
   ```

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

   On UNIX:

   ```
   ESync2000<operating_system>.bin -options-template filename
   ```

   where <*operating_system*> is the operating system you are installing on (aix, HP11, Linux, linux390, or Solaris). For example, run the following command on an AIX computer:

   ```
   ESync2000Aix.bin -options-template filename
   ```

3. Edit the output file to specify the values described in Table 109.

Table 109. Netcool/OMNIbus event synchronization configuration values

Value	Description
installLocation	The directory into which the product should be installed. If the directory path contains spaces, enclose it in double quotes (" "). For example, to install the product to C:\Program Files\My Product, use `-P installLocation="C:\Program Files \My Product"`
configInfoPanel.filename	The name of the file where event synchronization configuration information is stored. The default file name is situpdate.conf.
configInfoPanel.pollingInt	The polling interval, in seconds. The minimum value is 1, while the default value is 3. If there are no situation events, the process that forwards events rests for 3 seconds.
configInfoPanel.crcByteCnt	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.

Table 109. Netcool/OMNIbus event synchronization configuration values (continued)

Value	Description
configInfoPanel.cmsSoapURL	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 the EIF probe sends event information. For example, http://*hostname:port*///cms/soap, where *hostname* is the host name of the monitoring server and *port* is the port.
configInfoPanel.bufFlushRate	The maximum number of event updates sent to the monitoring server at one time. The minimum (and default) value is 10 events.
configInfoPanel.logLevel	The level of debug information for event synchronization that is logged. You have the following choices: • Low (default) • Medium • Verbose
configInfoPanel3.filesize	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).
configInfoPanel3.fileNumber	The maximum number of event caches files at any given time. The minimum value is 2, while the default value is 10. When this value is reached, the oldest file is deleted to make room for a new file.
configInfoPanel3.fileLocn	The location where event cache files are located. The default locations are as follows: • On Windows: `C:\Program Files\IBM\SitForwarder\persistence`. • On UNIX: `/opt/IBM/SitFowarder/persistence`
cmsSvrsPnlNotGuiMode.hostname# **Note:** The pound sign (#) stands for a number between 1 and 10. For example, "hostname1".	The host name of each monitoring server that will send events to the event server. Specify up to 10 monitoring servers.
cmsSvrsPnlNotGuiMode.userID#	The user ID for the monitoring server, identified in hostname#, to use to access the computer where the monitoring server is running.
cmsSvrsPnlNotGuiMode.pswd#	The password for the user ID used to access the computer where the monitoring server is running.
cmsSvrsPnlNotGuiMode.retypePswd#	The password confirmation for the user ID.
rulebasePanel.rbPath	The path for the new rule base. There is no default location. You must specify a path.
rulebasePanel.fromRB	If you are creating a new rule base, identify any existing rule bases that you want to import into the new rule base.

Table 109. Netcool/OMNIbus event synchronization configuration values (continued)

Value	Description
rbInstallTypePanel.rbInstallType	Specifies whether the installer will automatically update a specified rule base, or if a rule base must be manually modified after installation is complete. Specify either automatic or manual. If manual is specified, all other rulebasePanal.* options are ignored. Not used for OMNIbus event synchronization installation.
bckupERB.backupName	If you want the install to back up an existing rule base before modifying it, specify the name of the back up rule base.
rulebasePanel.backPath	Specify the directory where the back up rule base should be created.
restartTECQ.restartTEC	Specify whether or not the installer should recycle the event server to implement the changes. Specify `Yes` to have the installer restart the server; specify `No` if you want to restart the server yourself after installation is completed. If the directory path contains spaces, enclose it in double quotes (" "). For example, to install the product to `C:\Program Files\My Product`, use `-P installLocation="C:\Program Files \My Product"`

Notes:

a. Remove the pound signs (###) from the beginning of any value that you want to specify.

b. You must specify the following values:

```
### -P installLocation="<value>"
### -W configInfoPanel3.fileLocn="<value>"
```

and the following information for at least one monitoring server:

```
cmdSvrsPnlNotGuiMode.hostname1,
cmdSvrsPnlNotGuiMode.userID1
cmdSvrsPnlNotGuiMode.pswd1
cmdSvrsPnlNotGuiMode.retypePswd1
```

If you do not specify any of the other values, the default values are used. If you specify values, ensure that the values you specify meets the minimum required values. Otherwise, the installation stops and an error is written to the log file.

c. The following values are specified only when you are installing event synchronization on a Tivoli Enterprise Console event server:

```
### -W configInfoPanel2.filesize="<value>"
### -W configInfoPanel2.fileNumber="<value>"
### -W configInfoPanel2.fileLocn="<value>"
### -W rulebasePanel.chooseNewOrExistingRB="<value>"
### -W rulebasePanel.rbName="<value>"
### -W rulebasePanel.rbPath="<value>"
### -W rulebasePanel.fromRB="<value>"
### -W rulebasePanel.fromRB="<value>"
### -W restartTECQ.restartTEC="<value>"
```

4. Save the file.

5. Run the following command:

   On Windows:

   ```
   ESync2000Win32.exe -options filename -silent
   ```

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

   On UNIX:

   ```
   ESync2000<operating_system>.bin -options filename -silent
   ```

   where <*operating_system*> is the operating system you are installing on (`aix`, `HP11`, `Linux`, `linux390`, `Solaris`). For example, on AIX, run the following command:

   ```
   ESync2000Aix.bin -options filename -silent
   ```

When installation is complete, the results are written to the **itm_tec_event_sync_install.log** file. On UNIX, this log file is always created in the `/tmp` directory. For Windows, this file is created in the directory defined by the %TEMP% environment variable. To determine where this directory is defined for the current command line window, run the following command:

```
echo %TEMP%
```

If you specified the monitoring servers in the silent installation configuration file, you might consider deleting that file after installation, for security reasons. The passwords specified in the files are not encrypted.

If you want to define additional monitoring servers (in addition to the one required monitoring server), run the sitconfsvruser.sh command as described in "Defining additional monitoring servers to the event server" on page 403. Repeat this command for each monitoring server.

If you specified your monitoring servers after the installation, you must stop and restart the Situation Update Forwarder process manually. See for information.

Perform the following tasks after the installation is finished:

- Configure OMNIbus to receive events and update event status as described in "Configuring the Netcool/OMNIbus event server."
- Configure the monitoring server to forward events to OMNIbus as described in "Configuring the monitoring server" on page 402.

Configuring the Netcool/OMNIbus event server

In this step you configure the OMNIbus Objectserver to receive and map the situation event information forwarded by a monitoring server and to reflect the events to the OMNIbus console. You also configure the OMNIbus server to send event synchronization information back to the originating monitoring server and configure the EIF probe to map the situation event attributes to OMNIbus event attributes. Optionally, you can configure the event synchronization component to send error events to the OMNIbus system when errors are detected in the synchronization process. The configuration comprises the following steps:

- "Configuring the OMNIbus server for program execution from scripts" on page 398
- "Updating the OMNIbus db schema" on page 398
- "Configuring the EIF probe" on page 400
- "Configuring error event flow to OMNIbus (optional)" on page 402

Configuring the OMNIbus server for program execution from scripts

To run the event synchronization program from SQL automation scripts for sending sychronization events to the monitoring server, the OMNIbus event server must be running under process control and the properties **PA.Username** and **PA.Password** must be set in *OMNIHOME*/etc/NCOMS.props file, where *OMNIHOME* is the system-defined variable defining the installation location of OMNIbus.

By default, the process control grants access to the members of the default group **ncoadmin**. For default configuration, create a `ncoadmin` group and add `root` as a user to this group. The **PA.Username** property must be set to the username for connecting to the process control agent. On UNIX, the default value is `root`. The **PA.Password** property must be set to the password for the user connecting to the process control agent. For default setting, specify the password of the root user. Refer to OMNIbus documentation for configuring OMNIbus server under process control.

Updating the OMNIbus db schema

The command to configure OMNIbus pipes the SQL command set into the SQL command line tool and performs the updates to the Objectserver.

Note: If you have already installed the TEC to OMNIbus or the Netview to OMNIbus SQL updates, executing this step will result in error messages for adding columns that already exist. Ignore these error messages.

1. Update the Objectserver database with the following commands:
   - On UNIX

```
$OMNIHOME/bin/nco_sql -user <username>
     -password <password>
     -server <server_name>
     < <path_to_file>/itm_proc.sql
$OMNIHOME/bin/nco_sql -user <username>
     -password <password>
     -server <server_name>
     < <path_to_file>/itm_db_update.sql
$OMNIHOME/bin/nco_sql -user <username>
     -password <password>
     -server <server_name>
     < <path_to_file>/itm_proc.sql
$OMNIHOME/bin/nco_sql -user <username>
     -password <password>
     -server <server_name>
     < <path_to_file>/itm_db_update.sql
$OMNIHOME/bin/nco_sql -user <username>
     -password <password>
     -server <server_name>
     < <path_to_file>/itm_sync.sql
```

where:

$OMNIHOME
Is the system-defined variable defining the install location of OMNIbus

<username>
Is the OMNIbus Object Server user name

<password>
Is the OMNIbus Object Server password

<path_to_file>
Is the fully qualified path to specified SQL file

- On Windows:

```
%OMNIHOME%\..\bin\redist\isql -U <username>
     -P <password>
     -S <server_name>
     < <path_to_file>\itm_proc.sql
%OMNIHOME%\..\bin\redist\isql -U <username>
     -P <password>
     -S <server_name>
     < <path_to_file>\itm_db_update.sql
%OMNIHOME%\..\bin\redist\isql -U <username>
     -P <password>
     -S <server_name>
     < <path_to_file>\itm_proc.sql
%OMNIHOME%\..\bin\redist\isql -U <username>
     -P <password>
     -S <server_name>
     < <path_to_file>\itm_db_update.sql
%OMNIHOME%\..\bin\redist\isql -U <username>
     -P <password>
     -S <server_name>
     < <path_to_file>\itm_sync.sql
```

where:

$OMNIHOME
Is the system-defined variable defining the install location of OMNIbus

<username>
Is the OMNIbus Object Server user name

<password>
Is the OMNIbus Object Server password

<path_to_file>
Is the fully qualified path to specified SQL file

2. Stop the OMNIbus server:
   - On Windows: In the Control Panel, open Administrative Tools, then Services. In the list of services, double-click OMNIbus server, then click Stop.
   - On UNIX: Issue the following command from command line

```
$OMNIHOME/bin/nco_pa_stop -process <server_name>
```

   where:

   $OMNIHOME
   Is the system-defined variable defining the install location of OMNIbus.

   <server_name>
   Is the OMNIbus Objectserver name defined for process control.

3. Restart the OMNIbus server.
   - On Windows: In the list of services, double-click OMNIbus server, then click Start.
   - On UNIX: Issue the following command from command line:

```
$OMNIHOME/bin/nco_pa_start -process <server_name>
```

$OMNIHOME
Is the system-defined variable defining the install location of OMNIbus.

<server_name>
Is the OMNIbus Objectserver name defined for process control.

Configuring the EIF probe

This step configures the probe with the rules for mapping situation events to OMNIbus events. Configuring the mapping involves updating the tivoli_eif.rules file installed with the probe with the contents of the tivoli_eif.rules file shipped with the synchronization component. You must recycle the probe after you update the file. The default mapping is shown in Table 110.

Table 110. Mapping of situation attributes to OMNIbus attributes

Situation attribute	OMNIbus Attribute
situation_name + situation_origin +situation_displayitem + event_class	(for ITMProblem)
situation_name + situation_origin + situation_displayitem + event_class + ITMResolution	Identifier (for ITMResolution)
situation_name	AlertKey
situation_origin	Node
situation_origin	NodeAlias
source	Agent
default	Type (20) (for ITMProblem)
situation_status = “P” and integration_type = “U”	Type (21) (for ITMResolution)
situation_status = “D” and integration_type = “U”	Type (21) (for ITMResolution)
situation_status = “N” and integration_type = “U”	Type (21) (for ITMResolution)
situation_displayitem	ITMDisplayItem
situation_status	ITMStatus
situation_time	ITMTime
situation_type	ITMSitType
situation_thrunode	ITMThruNode
situation_eventdata	ITMEventData
cms_hostname	ITMHostname
master_reset_flag	ITMResetFlag
integration_type	ITMIntType
event_class	AlertGroup
msg	Summary
“tivoli_eif probe on ”+hostname()	Manager
6601	Class

Table 110. Mapping of situation attributes to OMNIbus attributes (continued)

Situation attribute	OMNIbus Attribute

severity
`FATAL / 60 = Critical`
`CRITICAL / 50 = Critical`
`MINOR / 40 = Minor`
`WARNING / 30 = Warning`
`UNKNOWN / 10 = Indeterminate`
	Severity

getdate	LastOccurrence/FirstOccurrence
date	TECDate
repeat_count	TECRepeatCount
fqhostname	TECFQHostname
hostname	TECHostname

Take the following steps to update the rules file:

1. Copy the contents of `<event_sync_install_dir>\omnibus\tivoli_eif.rules` (Windows) or `<event_sync_install_dir>/omnibus/tivoli_eif.rules` (UNIX) to the following file:

   `%OMNIHOME%\probes\<os_dir>\tivoli_eif.rules (Windows)`

   or

   `$OMNIHOME/probes/<os_dir>/tivoli_eif.rules (UNIX)`

   where:

   %OMNIHOME%
   Is a system-defined variable defining the install location of OMNIbus.

   $OMNIHOME
   Is a system-defined variable defining the install location of OMNIbus .

   <os_dir>
   Is the operating system, such as Windows or AIX.
2. Stop the EIF probe.
   - On Windows: In the Control Panel, open Administrative Tools, then Services. In the list of services, double-click the EIF probe, then click Stop.
   - On UNIX: Issue the following command from command line

     `$OMNIHOME/bin/nco_pa_stop -process <probe_name>`

     where:

     $OMNIHOME
     Is the system-defined variable defining the install location of OMNIbus.

     <server_name>
     OMNIbus EIF probe name defined for Process Control.
3. 3) Restart the OMNIbus probe.
   - On Windows: In the list of services, double-click OMNIbus EIF Probe, then click **Start**.
   - On UNIX: Issue the following command from command line:

     `$OMNIHOME/bin/nco_pa_start -process <probe_name>`

$OMNIHOME
Is the system-defined variable defining the install location of OMNIbus.

<probe_name>
Is the Probe for Tivoli EIF name defined for process control.

Configuring error event flow to OMNIbus (optional)

To send error events to the OMNIbus system when errors are detected in the event synchronization process, update the values for the following parameters in the `<eventsync_install>/omnibus/errorevent.conf file`:

```
ServerName
ServerPort
```

Where

<eventsync_install>
Is the location where event synchronization program is installed (on Windows the default install directory is `C:\Program Files\IBM\SitForwarder`; on Linux and UNIX operating systems, the default is `/opt/IBM/SitForwarder`).

ServerName Is the name of the computer where the EIF probe is running.

ServerPort Is the listening port for EIF probe. The default value is 9999.

Configuring the monitoring server

Before the monitoring server forwards any situation events to Netcool/OMNIbus, you must enable event forwarding and define a default event destination.

Take the following steps to enable event forwarding for each hub monitoring server from which you want to forward events to an OMNIbus Objectserver:

For Windows monitoring servers *only*, do the following:

1. Open Manage Tivoli Monitoring Services.
2. Right-click the monitoring server and click **Reconfigure**.
3. On the configuration options window, select **Tivoli Event Integration Facility**.
4. Click **OK** and **OK**.
5. Complete the following fields on the Event Server: Location and Port Number window and click **OK**:

   Server or EIF Probe Location
   Type the host name or IP address for the computer where the EIF probe is installed.

   Port Number
   Type the port number on which the probe is listening.

For UNIX monitoring servers: You configured the EIF probe and port information for the UNIX monitoring server during installation, if you installed the monitoring server using the configuration instructions in this installation guide. However, if you did not configure this information, see "Configuring the hub monitoring server" on page 120 for the procedure.

Customizing the OMNIbus configuration

The get_config_parms procedure in the <event_sync_install_dir>/omnibus/itm_proc.sql file defines three configuration parameters:

```
set sit_ack_expired_def_action = 'REJECT'
set sit_resurface_def_action = 'ACCEPT'
set situpdate_conf_file = 'situpdate.conf'
```

The **sit_ack_expired_def_action** variable defines the action to be taken for an event by the OMNIbus server when acknowledgement expiration information is received for an event from a monitoring server. The default action is to reject the request. OMNIbus sends information to change the state of the event to Acknowledge back to the monitoring server. If you want to change the action taken by the OMNIbus server to accept the acknowledgement expiration, modify the statement to set sit_ack_expired_def_action = 'ACCEPT'.

The **sit_resurface_def_action** variable defines the action to be taken by the OMNIbus server when a situation event has resurfaced. The default action of the OMNIbus server is to accept this request and deacknowledge the event. If you want to change the action taken by OMNIbus server to reject the resurface of the event, modify the statement to set sit_resurface_def_action = 'REJECT'. OMNIbus then sends information back to the monitoring server to change the state of the event back to Acknowledge.

The **situpdate_conf_file** variable specifies the name of the configuration file to be used by the SitUpdate Forwarder. If you want to change the name of the configuration file, modify the statement to set **situpdate_conf_file** = *'newname.conf'*.

After modifying itm_proc.sql, issue the following command:

- For UNIX:

```
$OMNIHOME/bin/nco_sql -user <username>
     -password <password>
     -server <server_name>
     < <path_to_file>/itm_proc.sql
```

- For Windows:

```
%OMNIHOME%\..\bin\redist\isql -U <username>
      -P <password>
      -S <server_name>
      < <path_to_file>\itm_proc.sql
```

Defining additional monitoring servers to the event server

To add additional monitoring servers to the list from which you want to receive events, issue the **sitconfuser** command as described below. Ensure that the event synchronization is configured for both fully qualified host name and the short host name of the monitoring server.

- On Windows, change to the %SystemDrive%\Program Files\SitForwarder\bin directory and enter the following command:

```
sitconfuser.cmd  add  serverid=server  userid=user  password=password
```

  where:

  server
  Is the fully qualified host name of the monitoring server.

user
Is the user ID used to access the computer where the monitoring server is running.

password
Is the password used to access the host computer.

Repeat this command to add short host name information for the same monitoring server by specifying the short host name value for the serverid parameter.

- On UNIX, change to the `/opt/IBM/SitForwarder/bin` directory and enter the following command:

```
sitconfuser.sh  add  serverid=server  userid=user  password=password
```

where:

server
Is the fully qualified host name of the monitoring server.

user
Is the user ID used to access the computer where the monitoring server is running.

password
Is the password used to access the host computer.

Repeat this command to add short host name information for the same monitoring server by specifying the short host name value for the **serverid** parameter.

Repeat this step for each monitoring server that you want to add.

You can also delete monitoring servers. See *IBM Tivoli Monitoring Command Reference* for the full syntax of this command.

After you change the configuration of the event synchronization, you must manually stop and restart the Situation Update Forwarder process. See "Starting and stopping the Situation Update Forwarder process" on page 379 for information.

Verifying installation and configuration

Take the following steps to verify that the event synchronization component has been installed and event integration has been configured successfully.

1. Stop and restart the hub Tivoli Enterprise Monitoring Server:
   - On Windows computers:
     a. Start the Manage Tivoli Monitoring Services utility (**Start > (All) Programs > IBM Tivoli Monitoring > Manage Tivoli Monitoring Services**).
     b. Right-click the hub monitoring server and select **Recycle** from the popup menu.
   - On UNIX and Linux computers, enter the following commands:

```
$ITM_INSTALL_PATH/bin/itmcmd stop <tems_server>
$ITM_INSTALL_PATH/bin/itmcmd start <tems_server>
```

Where

$ITM_INSTALL_PATH
Is the system variable defining the installation location of the monitoring server.

tems_server
Is the host name of the computer where the monitoring server is installed (the host where you are executing this command).

2. On the OMNIbus server machine, run the following command to start the OMNIbus console:

   ```
   $OMNIHOME/bin/nco_event
   ```

3. Refresh the event view in the OMNIbus console and check for situation events from the monitoring server.

Starting and stopping the situation update forwarder

To send event updates to a monitoring server, you must start the Situation Update Forwarder. This process is started automatically when the event server starts. To start the process manually, change to the <*install_esynch*>/bin directory and run the following command:

On Windows:

```
startSUF.cmd
```

On UNIX:

```
startSUF.sh
```

To stop the process, 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 **Administrative Tools > Services** utility or with the following commands:

```
net start situpdate
net stop situpdate
```

Part 6. Appendixes

© Copyright IBM Corp. 2005, 2007

Appendix A. Installation worksheets

Use the following worksheets to gather information you need during the installation of the IBM Tivoli Monitoring components:

- "Windows hub monitoring server worksheet" on page 410
- "Linux or UNIX hub monitoring server installation worksheet" on page 411
- "Windows remote monitoring server worksheet" on page 412
- "Linux or UNIX remote monitoring server installation worksheet" on page 413
- "Windows portal server worksheet" on page 414
- "Linux portal server worksheet" on page 415
- "Generic Windows monitoring agent worksheet" on page 416
- "Generic Linux or UNIX monitoring agent worksheet" on page 417
- "Windows portal desktop client worksheet" on page 418
- "Linux portal desktop client worksheet" on page 419
- "Monitoring server communications protocol details worksheet" on page 420

© Copyright IBM Corp. 2005, 2007

Windows hub monitoring server worksheet

Use the following worksheet to gather information for your installation of the hub monitoring server on a Windows computer.

Table 111. Windows hub monitoring server installation worksheet

Host name of computer	
IP address	
IBM Tivoli Monitoring installation directory	
Encryption key	
Agents to install on this computer	
Agents to add to the deployment depot	
Program folder name	
Monitoring server name	
Communications protocol details	See Monitoring server communications protocol details worksheet.
Agents for which to add application support data	

Linux or UNIX hub monitoring server installation worksheet

Use the following worksheet to gather information for the installation of the hub monitoring server on a Linux or UNIX computer.

Table 112. Linux or UNIX hub monitoring server installation worksheet

Host name of computer	
IP address	
IBM Tivoli Monitoring installation directory	
Encryption key	
Monitoring server name	
Communications protocol details	See Monitoring server communications protocol details worksheet.
KDC_PARTITION	
NIC interface name ("Optional Primary Network Name")	
Agents to install on this computer	
Agents for which to add application support data	
Agents to add to the deployment depot	

Windows remote monitoring server worksheet

Use the following worksheet to gather information for the installation of the remote monitoring server on a Windows computer.

Table 113. Windows remote monitoring server installation worksheet

Host name of computer	
IP address	
IBM Tivoli Monitoring installation directory	
Encryption key	
Agents to install on this computer	
Agents to add to the deployment depot	
Program folder name	
Monitoring server name	
Agents for which to add application support data	
Hub monitoring server name	
Hub monitoring server host name	
Hub monitoring server communications protocol details	See Monitoring server communications protocol details worksheet.

Linux or UNIX remote monitoring server installation worksheet

Use the following worksheet to gather information for the installation of the remote monitoring server on a Linux or UNIX computer.

Table 114. Linux or UNIX remote monitoring server installation worksheet

Host name of computer	
IP address	
IBM Tivoli Monitoring installation directory	
Encryption key	
Monitoring server name	
KDC_PARTITION	
NIC interface name ("Optional Primary Network Name")	
Agents for which to add application support data	
Hub monitoring server host name	
Hub monitoring server communications protocol details	See Monitoring server communications protocol details worksheet.
Agents to add to the deployment depot	

Windows portal server worksheet

Use the following worksheet to gather information for the installation of the portal server on a Windows computer.

Table 115. Windows portal server worksheet

Installation location	
Encryption key used on the hub monitoring server	
Program folder	
Host name of the computer where you are installing the portal server	
Portal server database administrator ID	
Portal server database administrator password	
Portal server database user ID (default = TEPS)	
Portal server database user password	
Warehouse database administrator ID	
Warehouse database administrator password	
Warehouse database user ID (default = ITMUser)	
Warehouse database user password	
Warehouse data source name (default = ITM Warehouse)	
Warehouse database name	
Hub monitoring server host name	
Hub monitoring server communications protocol details	See Monitoring server communications protocol details worksheet.

Linux portal server worksheet

Use the following worksheet to gather information for the installation of the portal server on a Linux computer.

Table 116. Linux portal server worksheet

Installation location	
Encryption key for the hub monitoring server	
Host name for the hub monitoring server	
Hub monitoring server communications protocol details	See Monitoring server communications protocol details worksheet.
NIC interface name (Primary Optional Network Name)	
DB2 instance name (default = db2inst1)	
DB2 administrator ID (default = db2inst1)	
DB2 administrator password	
Portal server database name (default = TEPS)	
Portal server database user (default = itmuser)	
Portal server database user password	
Warehouse database name (default = WAREHOUS)	
Warehouse database user (default = itmuser)	
Warehouse database user password	

Generic Windows monitoring agent worksheet

Use the following worksheet to gather information for the installation of a monitoring agent on a Windows computer. Depending on the agent you are installing, you might need additional information to configure the agent. See the agent user's guide for more information.

Table 117. Generic Windows monitoring agent worksheet

Installation directory	
Encryption key for the hub monitoring server	
Agents to install	
Program folder name	
Monitoring server host name	
Monitoring server communications protocol details	See Monitoring server communications protocol details worksheet.

Generic Linux or UNIX monitoring agent worksheet

Use the following worksheet to gather information for the installation of a monitoring agent on a Linux or UNIX computer. Depending on the agent you are installing, you might need additional information to configure the agent. See the agent user's guide for more information.

Table 118. Generic monitoring agent for a Linux or UNIX computer worksheet

Installation directory	
Encryption key for the hub monitoring server	
Agents to install	
Agent product code or codes	
Monitoring server host name	
Monitoring server communications protocol details	See Monitoring server communications protocol details worksheet.
KDC_PARTITION	
NIC interface name (Optional Primary Network Name)	
root user password	
User group name	
Optional user name	

Windows portal desktop client worksheet

Use the following worksheet to gather information for the installation of a the portal desktop client on a Windows computer.

Table 119. Windows portal desktop client worksheet

Installation directory	
Encryption key for the monitoring server	
Program folder name	
Portal server host name	
Monitoring server host name	
Monitoring server communications protocol details	See Monitoring server communications protocol details worksheet.

Linux portal desktop client worksheet

Use the following worksheet to gather information for the installation of a the portal desktop client on a Windows computer.

Table 120. Linux portal desktop client worksheet

Installation directory	
Encryption key for the monitoring server	
Instance name for the portal server	
Portal server host name	

Monitoring server communications protocol details worksheet

Use the following worksheet to gather the communications protocol details for your hub and remote monitoring servers.

Table 121. Monitoring server communications protocol details worksheet

IP.UDP Settings	
Host name or IP address	
Port number or port pools	
IP.PIPE Settings	
Host name or IP address	
Port number	
IP.SPIPE Settings	
Host name or IP address	
Port number	
SNA Settings	
Network name	
LU name	
LU 6.2 LOGMODE	
TP name	
Local LU alias	

Appendix B. Performing a silent installation of IBM Tivoli Monitoring

This appendix provides information about installing IBM Tivoli Monitoring using the silent installation method. This method of installation is useful for advanced users who prefer to input installation information once through a response file instead of repeatedly through an installation wizard.

You might run through the installation wizard one time to determine the values that you need to set for your monitoring needs and then use silent installation to install the rest of your environment. For more information about installing through the installation wizard, see Chapter 6, "Installing IBM Tivoli Monitoring," on page 113.

The following table outlines the steps for performing a silent installation of IBM Tivoli Monitoring.

Table 122. Installation and configuration steps

Step	Where to find detailed information
Assess your monitoring needs to determine the best deployment of IBM Tivoli Monitoring components.	Chapter 3, "Preparing for installation," on page 59
Ensure you have the required hardware and software.	"Hardware and software requirements" on page 70
Gather any information required for successful installation (such as DB2 user information and security specifications).	"Specific information to have ready" on page 59
Run the silent installation.	"Creating and using a Windows response file" "Performing a silent installation on a Linux or UNIX computer" on page 423
Install application support files on the monitoring server, portal server, and portal desktop client.	"Installing and enabling application support" on page 159
Start the portal client to verify that you can view the monitoring data.	"Starting the Tivoli Enterprise Portal client" on page 188

Creating and using a Windows response file

A sample Windows silent installation response file is provided on the product installation media. Use the following steps to edit that response file as appropriate for your environment:

1. Locate the silent.txt file on the product installation media. Copy this file to a temporary directory on your system.
2. Open your copy of the silent.txt file in a text editor.
3. Change the parameters as appropriate for your environment. The silent.txt file contains descriptions of all the parameters, including directions on how to use them.

© Copyright IBM Corp. 2005, 2007

Complete all of the steps listed in the file. Each line of the file must be either a comment (containing a semi-colon in column one) or a meaningful statement that starts in column one.

Note: If you want to use the TCP/IP protocol, make sure to specify ″IP.UDP.″ If you specify ″TCP/IP,″ IP.PIPE is used by default.

Attention: Do not modify any other files that come with the installation (for example, the SETUP.ISS file).

4. Save the file and close the editor.
5. Run the silent installation using one of the following methods:
   - "Running the silent installation from the command line with parameters"
   - "Using SMS"

Note: If the installation fails for any reason, a log file, ″Abort IBM Tivoli Monitoring <*date*> <*time*>.log,″ is created to document the problem. If the installation fails before reading in the installation location, the log file is written to the Windows boot drive, typically the C:\ drive. If the installation fails after reading the installation location, the log file is written to an `\install` subdirectory in the installation directory. For example, if you use the default installation directory, the log file is written to the `C:\ibm\itm\installITM` directory.

Running the silent installation from the command line with parameters

Use the following steps to run the installation from the command line:

1. Start a DOS Command Shell.
2. From the shell, change to the directory containing this installation (where setup.exe and setup.ins are located).
3. Run the setup as follows. You must specify the parameters in the same order as listed.

   ```
   start /wait setup /z"/sfC:\temp\SILENT.TXT" /s /f2"C:\temp\silent_setup.log"
   ```

   where:

   /z″/sf″
   Specifies the name of the installation driver you customized for your site. This is a required parameter. This file must exist.

   /s Specifies that this is a silent installation. This causes nothing to be displayed during installation.

   /f2 Specifies the name of the InstallShield log file. If you do not specify this parameter, the default is to create Setup.log in the same location as the setup.iss file. In either case, the Setup program must be able to create and write to this file.

Using SMS

Use the following steps:

1. Copy the all the installation files to a LAN-based disk that SMS will mount on the desired computers. (Copy all files in the directory that contains the setup.exe and setup.ins files.)

2. Replace the original SILENT.TXT file on the LAN disk with your modified version.
3. Edit the PDF file located with the setup.exe file and change the Setup invocation as follows:

```
Setup /z"/sfC:\temp\SILENT.TXT" /s /f2"C:\temp\silent_setup.log"
```

Performing a silent installation on a Linux or UNIX computer

Just as the interactive installation on Linux and UNIX requires both an installation of code and then a separate configuration, so does the silent installation method. Both the installation and configuration use parameter files to define what you are installing or configuring. Sample installation and configuration parameter files are shipped with IBM Tivoli Monitoring and with monitoring agents. The files are located in the following locations:

- Silent installation files:
  - On the product installation media (both base IBM Tivoli Monitoring and agent installation media)
  - After installation, a sample file is located in the <*install_dir*>/samples directory
- Silent configuration files: After you install the product, a configuration file for each component that requires configuration is located in the <*install_dir*>/samples directory. There is also a sample configuration file that you can use to configure any component.

Before editing any of the response files, note the following syntax rules:

- Comment lines begin with a pound sign (#).
- Blank lines are ignored.
- Parameter lines are PARAMETER=value. Do not use a space before the parameter; you can use a space before or after an equal sign (=).
- Do not use any of the following characters in any parameter value:
  - Dollar sign ($)
  - Equal sign (=)
  - Pipe sign (|)

Use the following procedures to perform silent installations:

- "Installing components with a response file"
- "Configuring components with a response file" on page 425

Installing components with a response file

The silent_install.txt response file specifies the installation parameters for IBM Tivoli Monitoring components. To use this file to perform a silent installation, edit the file to identify what you want to install and then run the following command:

```
./install.sh -q -h <install_dir> -p <response_file>
```

where:

install_dir
: Identifies the installation location for the IBM Tivoli Monitoring component. The default installation location is /opt/IBM/ITM.

response_file
: Identifies the response file that you edited to specify installation parameters. Specify the absolute path to this file.

The parameters that you can configure in the silent_install.txt file vary depending on the component that you are installing. Each of the files contains comments that explain the options. The following procedure is an example of installing all available components on one computer. Use this to get an idea of what type of information you need to gather when you are setting up your own silent installation.

Use the following steps to perform a silent installation on a UNIX computer:

1. Edit the silent_install.txt file.
2. Set the following parameters as appropriate for your environment:

Table 123. Silent installation parameters for UNIX

Parameter	Definition
INSTALL_ENCRYPTION_KEY	REQUIRED. The data encryption key used to encrypt data sent between systems. This key must be the same for all components in your IBM Tivoli Monitoring environment. Do not use the following characters in the key: • $ • = • |
INSTALL_FOR_PLATFORM	The operating system for which to install the components. You can specify an architecture code. If you do not specify an architecture code, the operating system for the current computer is used. You can find a list of the architecture codes for the supported architectures in **archdsc.tbl** in the registry directory.

INSTALL_PRODUCT	The product code for the components (or "products") that you want to install. See Appendix D, “IBM Tivoli product codes,” on page 437 for a list of the codes for the base components. You can use the `./cinfo` command to view the product codes for the applications installed on this computer. You can also find a list of the product codes in the registry directory in **proddsc.tbl**.
	
	You can specify "all" to install all available components.
	
	To install multiple components (but not all), repeat this parameter for each component that you want to install. For example:
	`INSTALL_PRODUCT=ms`
	`INSTALL_PRODUCT=cj`
	`INSTALL_PRODUCT=cq`
	
	This example installs the monitoring server, portal server, and portal desktop client on a Linux computer.

Table 123. Silent installation parameters for UNIX (continued)

Parameter	Definition
MS_CMS_NAME=	If you are installing a monitoring server, use this parameter to specify the name for the monitoring server, such as HUB_*hostname*. Do not specify an IP address or fully qualified host name.

3. Save and close the file.
4. Run the following command to install IBM Tivoli Monitoring in the /opt/IBM/ITM directory:

   ```
   ./install.sh -q -h /opt/ibm/itm -p /tmp/silent_install.txt
   ```

Configuring components with a response file

You can use the **itmcmd config** command with the **-p** <*filename*> parameter to configure IBM Tivoli Monitoring components silently.

The following sample configuration response files are provided with IBM Tivoli Monitoring:

- ms_silent_config.txt: Used to configure the monitoring server
- cq_silent_config.txt: Used to configure the portal server
- cj_silent_config.txt: Used to configure the portal desktop client
- silent_config.txt: A generic configuration file used to configure agents that do not require unique configuration parameters

If an agent requires unique configuration parameters, configure the agent by using the **itmcmd config** command or the Manage Tivoli Enterprise Monitoring Services utility.

Use the following steps to configure a component using the silent method:

1. Edit the configuration file for the component that you want to configure.
2. Complete the parameters identified in the file. Each file contains comments that define the available parameters and the values to specify.
3. Save the file and exit.
4. Run one of the following commands.

   To configure the monitoring server:

   ```
   ./itmcmd config -S -p <response_file> -t <ms_name>
   ```

   To configure the portal server, desktop client, or an agent:

   ```
   ./itmcdm config -A -p <response_file> pc
   ```

   where:

   <*response_file*>
   : The name of the configuration response file. Use an absolute path to this file.

   <*ms_name*>
   : The name of the monitoring server that you want to configure.

   pc
   : The product code for the component or agent that you want to configure. See Appendix D, "IBM Tivoli product codes," on page 437 for the list of product codes.

Appendix C. Firewalls

There are four options for achieving interoperability between Tivoli Management Services components across network firewalls:

1. Automatic (do nothing)
2. Configure IP.PIPE with the `ephemeral` keyword
3. Use a broker partition file
4. Implement a firewall gateway

Use the following topics to select and implement the appropriate option for your environment:

- "Determining which option to use"
- "Basic (automatic) implementation" on page 429
- "Implementation with ephemeral pipe" on page 429
- "Implementation with partition file" on page 430
- "Implementation with firewall gateway" on page 434

Determining which option to use

To determine which option is needed in a particular the firewall environment, four factors must be considered:

- "Flow of connection establishment"
- "Permission at the firewall"
- "Server address continuity" on page 428
- "Number of internet zones" on page 428

Flow of connection establishment

Products based on Tivoli Management Services typically establish connections in a traditional client-server flow: connect requests flow from a client in the public network to a server in the trusted network. If the network configuration allows this connection flow, permissions at the firewall are the next consideration in determining how interoperability is achieved.

If the configuration requires that the physical connect requests flow from the secure, trusted server network to the public, untrusted client network, then option 4, a firewall gatewall, is required for interoperability. See "Implementation with firewall gateway" on page 434.

Permission at the firewall

If the network configuration allows traditional connection flow, the next consideration is what firewall permissions, if any, are required of the firewall that separates the private, trusted server network from the public, untrusted client network. For simplicity the firewall between these disjoint networks is referred to as the *barrier firewall*.

If all ports are permitted across the barrier firewall, then server address continuity becomes a consideration (see "Server address continuity" on page 428).

© Copyright IBM Corp. 2005, 2007

If no ports are permitted at the barrier firewall, then to achieve interoperability among components in this firewall environment, full-duplex traffic must be permitted by the firewall administrator for as many ports as there are servers being concurrently accessed. For example, if Tivoli Enterprise Monitoring Agents are accessing only the Tivoli Enterprise Monitoring Server, then only one port must be permitted (for full-duplex traffic) or opened at the barrier firewall. This would be the well-known monitoring server port (the default is 1918 for IP.PIPE, 3660 for IP.SPIPE). If agents are accessing two servers concurrently, a monitoring server and a Warehouse Proxy server, then two ports must be opened at the firewall, one for the monitoring server (typically 1918) and one for the Warehouse Proxy (typically 63358) for interoperability in this firewall environment.

Server address continuity

If the barrier firewall has no restrictions and all ports are permitted, the next factor to consider is server address continuity. Address continuity refers to the validity and reachability of published IP addresses. Address continuity exists when a published server address is universally reachable by all network clients requesting that service. An example of a server address with address continuity is update.microsoft.com (207.46.211.124).

Tivoli Management Services server components register their services and the location of these services (IP address) with a *location broker*. Clients send queries to the location broker to request address information for a service, and receive responses that a list of protocols (address families) and IP addresses at which these services are available. The client then sends a specific server request to one of the addresses in the list received from the location broker. Service registration with the location broker assumes address continuity.

If the published address of the Tivoli service (a remote monitoring server, for example) is identical and reachable for either side of the barrier firewall, then nothing further needs to be done to achieve interoperability in this firewall environment. If the same address cannot be reached from either side of the barrier firewall, then option 2 (ephemeral pipe configuration) or option 3 (broker partition files) is required for interoperability.

Both options are used when traversing a firewall with Network Address Translation (NAT) in effect. While option 2 (ephemeral pipe) is easier to implement, it does restrict the endpoint: ephemeral endpoints cannot warehouse data. If warehousing data at the endpoint is required, then partition files must be used for interoperability in this firewall environment (see “Implementation with partition file” on page 430); otherwise ephemeral pipes are sufficient to traverse the translating firewall (see “Implementation with ephemeral pipe” on page 429).

Number of internet zones

The final factor to be taken into consideration is the number of internet zones, that is, how many barrier firewalls must be crossed. If there are two or more translating firewalls, then option 4, a firewall gateway, must be used for interoperability in this firewall environment (see “Implementation with firewall gateway” on page 434).

Basic (automatic) implementation

IBM Tivoli Monitoring supports most common firewall configurations. To enable this support, IBM Tivoli Monitoring uses the IP.PIPE socket address family, a TCP-based protocol that opens a single port on the firewall for communication by IBM Tivoli Monitoring components. If your target environment includes a firewall between any IBM Tivoli Monitoring components, you must specify IP.PIPE or IP.SPIPE as your communication protocol during configuration. Typically, no other special configuration is needed unless one of the factors discussed in "Determining which option to use" on page 427 requires it.

Implementation with ephemeral pipe

Configure your communications to use ephemeral pipe when addresses on either side of a barrier firewall are not identical or are not reachable from either side. (Note that use of ephemeral pipe may be dictated by the per-machine agent count, as well as any form of discontiguous addressing such as a NAT firewall.)

You configure an IP.PIPE or IP.SPIPE connection as an ephemeral pipe by adding the ephemeral keyword `ephemeral:y` the KDE_TRANSPORT environment variable immediately following the protocol keyword (IP.PIPE or IP.SPIPE) in the associated K*PP*ENV file for that process. You must then restart the process for the change to be effective.

Some K*PP*ENV files use KDC_FAMILIES instead of KDE_TRANSPORT. The process is exactly the same for the KDC_FAMILIES environment variable: adding the ephemeral keyword `ephemeral:y` immediately following the protocol keyword (IP.PIPE or IP.SPIPE) that is to be designated ephemeral.

For example, to configure the KNTAGENT to make an ephemeral connection to the monitoring server, KDE_TRANSPORT (or KDC_FAMILIES) in the file KNTENV would be changed from

```
KDE_TRANSPORT=IP.PIPE PORT:1918 IP SNA
```

to

```
KDE_TRANSPORT=IP.PIPE ephemeral:y PORT:1918 IP SNA
```

or from

```
KDC_FAMILIES=IP.PIPE PORT:1918 IP SNA
```

to

```
KDC_FAMILIES=IP.PIPE ephemeral:y PORT:1918 IP SNA
```

To configure a remote monitoring server to make an ephemeral connection to the hub, KDE_TRANSPORT (or KDC_FAMILIES) in the file KDSENV would be changed from

```
KDE_TRANSPORT=IP.PIPE PORT:1918 IP SNA
```

to

```
KDE_TRANSPORT=IP.PIPE ephemeral:y PORT:1918 IP SNA
```

or from

```
KDC_FAMILIES=IP.PIPE PORT:1918 IP SNA
```

to

```
KDC_FAMILIES=IP.PIPE ephemeral:y PORT:1918 IP SNA
```

Monitoring agents that configure their connections as ephemeral cannot warehouse data unless KPX_WAREHOUSE_LOCATION is also configured at the remote monitoring server to which the monitoring agent reports. The variable KPX_WAREHOUSE_LOCATION is an optional list of fully qualified, semicolon-delimited network names that must be added to environment file of the monitoring server to which the agents are connected. This file is located in different places, depending on the platform:

- On Windows systems: <*install_dir*>/CMS/KBBENV
- On UNIX systems:<*install_dir*>\config\kbbenv.ini

The syntax is:

```
KPX_WAREHOUSE_LOCATION= <family proctocol>: #<network address>[<portnumber>];
```

For example:

```
KPX_WAREHOUSE_LOCATION=ip.pipe:#192.168.0.14[18303];ip:#192.168.0.14[34543];
```

See also "Setting a permanent socket address for a proxy agent" on page 350.

Implementation with partition file

Address translation is an enhanced security feature of some firewall configurations. With this feature, components that must be reached across the firewall have two unique, but corresponding addresses: the external address (valid for components outside the firewall) and the internal address (valid for components inside the firewall).

In IBM Tivoli Monitoring, the component that typically must be reached for connection is the monitoring server; however, the Warehouse Proxy, which runs on Windows as a server-type application, must also be accessible to clients and also requires an external and internal address. A component on either side of the firewall knows only about the address that is valid for its side, its *partition*.

To accommodate sites with address translation, IBM Tivoli Monitoring uses a partition-naming strategy. This strategy requires two steps:

- The creation of a text file, called a *partition file*, as part of the configuration of a hub or remote monitoring server (or Warehouse Proxy). The partition file contains an entry that defines the address of that component in the other partition.
- The specification of a *partition name* (any alphanumeric string up to 32 characters) as part of the configuration of any agent, a hub or remote monitoring server, or Warehouse Proxy. A partition name must be specified for each component regardless of which side of the firewall it is located on.
- "Sample scenarios"
- "Creating or modifying the partition file in Manage Tivoli Monitoring Services" on page 432
- "Creating the partition file manually" on page 433

Sample scenarios

The following scenarios illustrate how to implement partition files in various configurations. In these scenarios, your site has one firewall that contains two partitions, which are named OUTSIDE and INSIDE:

- "Scenario 1: Hub monitoring server INSIDE and monitoring agents OUTSIDE"
- "Scenario 2: Hub and remote monitoring servers INSIDE and monitoring agents OUTSIDE"
- "Scenario 3: Hub monitoring server INSIDE, remote monitoring server and agents OUTSIDE"

Scenario 1: Hub monitoring server INSIDE and monitoring agents OUTSIDE

The hub monitoring server is contained within the firewall in a partition named INSIDE. A partition file named `parthub.txt` is included in this partition and contains the following entry:

```
OUTSIDE ip.pipe: hub's_external_address
```

OUTSIDE is the partition name outside the firewall and *hub's_external_address* is the address of the hub monitoring server that is valid for the agents.

As part of the configuration of each agent, specify the name of the partition that each is located in OUTSIDE.

When an agent starts, parthub.txt is searched for an entry that matches the partition name *OUTSIDE* and sees the monitoring server address that is valid for the agents (the external address).

Scenario 2: Hub and remote monitoring servers INSIDE and monitoring agents OUTSIDE

Note: In Scenarios 2 and 3, all agents report to the remote monitoring server.

As part of the configuration of the hub monitoring server, specify the name of the partition that it is located in INSIDE. No partition file is needed because the only component that reports to it (the remote monitoring server) is also inside the firewall.

As part of the configuration of the remote monitoring server, specify the name of the partition that it is located in INSIDE. A partition file, `partremote.txt`, must also be created at the remote monitoring server. It contains the following entries:

```
OUTSIDE ip.pipe: remote's_external_address
```

When configuring the agents (all of which are outside the firewall, reporting to the remote monitoring server), specify the name of the partition that they are located in OUTSIDE. When the agents start, partremote.txt is searched for an entry that matches the partition name OUTSIDE and sees the remote monitoring server address that is valid for them (the external address).

Scenario 3: Hub monitoring server INSIDE, remote monitoring server and agents OUTSIDE

As part of the configuration of the hub monitoring server, specify the name of the partition that it is located in INSIDE. Create a partition file, `parthub.txt`, containing the following entry:

```
OUTSIDE ip.pipe: hub's_external_address
```

OUTSIDE is the partition name outside the firewall and *hub's_external_address* is the address of the hub monitoring server that is valid for the remote monitoring server.

As part of the configuration of both the agents and the remote monitoring server, specify the name of the partition they are located in OUTSIDE.

A partition file `partremote.txt` also must be created at the remote monitoring server. It contains the following entry:

INSIDE `ip.pipe:` *remote's_internal_address*

If the hub monitoring server needs to communicate with the remote monitoring server (for example, to issue a report request from an agent that is connected to the remote monitoring server), the `partremote.txt` file is searched for an entry that matches the partition name INSIDE and sees the remote monitoring server address that is valid for it (the internal address).

Creating or modifying the partition file in Manage Tivoli Monitoring Services

The following instructions provide the steps for creating or editing the partition file using Manage Tivoli Monitoring Services:

- "Windows: Editing the partition file"
- "UNIX and Linux: Editing the partition file" on page 433

Windows: Editing the partition file

You can create or modify the partition file using the Tivoli Enterprise Monitoring Server Configuration option in Manage Tivoli Monitoring Services. Use the following steps:

1. Right-click the monitoring server you want to configure and select **Reconfigure**.

   The Tivoli Enterprise Monitoring Server Configuration window is displayed.
2. Select **IP.PIPE** as the communications protocol.
3. Select **Address Translation**.
4. Click **OK**.

   The Hub (or Remote) TEMS Configuration window is displayed.
5. Click **NAT Settings**.

   The NAT Settings window is displayed.
6. To create the file:
   a. For **Partition File**, type the fully qualified name of the partition file, for example `C:\IBM\ITM\CMS\KDCPARTITION.TXT`.
   b. For **Partition Name**, type the name of the partition to which the file applies.
   c. Click **Edit File**.

      A message appears saying that the partition file cannot be found and asking you if you want to create it.
   d. Click **Yes** to create the file.

      The file is created and opened in Notepad.
   e. Create the entry for the partition.

      The format for the entries is `PARTITION-ID IP.PIPE:`*nn.nn.nn.nn* `IP.PIPE:`*nn.nn.nn.nn*. For example, to create a monitoring server partition for a typical scenario with a monitoring agent outside of a NAT firewall connecting to a monitoring server behind a firewall, use the partition ID of your monitoring agent, two spaces, and then the IP address of the host of the monitoring server. Add additional IP.PIPE:*nn.nn.nn.nn* addresses on a

single line for multiple network interface cards. See “Sample partition file” on page 434 for more information on creating entries in the partition file.

f. Save and close the file.

7. Click **OK** to save the changes and close the configuration window.

UNIX and Linux: Editing the partition file

You can create or modify the partition file using the Tivoli Enterprise Monitoring Server Configuration option in Manage Tivoli Monitoring Services. Use the following steps:

1. Select the monitoring server you want to configure.
2. Click **Action → Configure → Basic Settings**.
3. Select **IP.PIPE** as the communications protocol.
4. Select **Use Address Translation**.
5. Enter the full path and file name for the partition file.
6. Click **Create** to create the file (if it does not exist) or **Modify** to edit the file.
7. Enter the partition ID in the first column.
8. Enter the IP address in the second column. If you require a second IP address, enter it in the third column. (If more than two IP addresses are required for a partition ID, use a text editor to add the additional addresses. See “Sample partition file” on page 434.)
9. Click **Save** to save the file and exit or **Cancel** to return to the previous screen without modifying the file.

Creating the partition file manually

If your site is using address translation, you must create a partition file. The partition file is a text file containing the name of a partition and its constituent interface address. You must create or modify this file before implementing firewall support with monitoring servers and agents, the portal server and the hub monitoring server, clients and the portal server, and monitoring agents and Warehouse Proxy agents.

When Tivoli Management Services 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.

When an IBM Tivoli Monitoring component performs a location broker lookup operation, the partition ID of its partition is automatically supplied. The location broker returns only addresses that have been defined for that partition namespace and no other. In effect, the IBM Tivoli Monitoring component sees only addresses that are valid for its partition.

A partition file is a standard text file which is defined to the system using the KDC_PARTITIONFILE environment variable. Within this file, each line describes a partition name with its constituent IP addresses using space delimited tokens. The format is as follows:

```
PARTITION-ID IP.PIPE:nn.nn.nn.nn IP.PIPE:nn.nn.nn.nn
```

The first token on each line is used as a case-insensitive partition ID. The partition ID can be any alphanumeric string with a maximum length of 32 characters.

Subsequent tokens specified are treated as interface addresses in standard NCS format (`address-family:address`). For communication across firewalls, use only IP.PIPE for address-family.

The expected default location of the file is */install_dir*/tables/*tems_name*.

Sample partition file

The following sample partition file illustrates the format and content expected.

```
# SAMPLE PARTITION FILE
#
# IMPORTANT: Do not overwrite this file. Copy to another directory
# before making changes.
#
# Lines beginning with a '#' are treated as comments and are ignored.
# Note: Do not specify a line that starts with an '*' as it might prevent
# proper functioning.
#
# Basic Format
# PARTITION-ID IP.PIPE:nn.nn.nn.nn IP.PIPE:nn.nn.nn.nn
#
# Procedure to edit this sample partition file.
# To create a monitoring server partition file for a typical scenario
# (monitoring agent outside of a NAT firewall connecting to a
# monitoring server behind the firewall),do the following:
# 1) Replace the "$OUTSIDE-PID$" with the partition id of your monitoring agent
# 2) Replace the "$OUTSIDE-TEMS-HOST-ADDRESS$" with the ip address of the monitoring
# server host outside of the firewall.
# 3) Add additional IP.PIPE:nn.nn.nn.nn addresses on a single line for multiple
# Network Interface Cards (NICs) as in the format above. Separate entries with
# two spaces.Lines can be continued by placing a backslash ('\') char at
# the end of the line.
#
################################################################################
$OUTSIDE-PID$ IP.PIPE:$OUTSIDE-CMS-HOST-ADDRESS$
```

Implementation with firewall gateway

The firewall gateway is capable of negotiating multiple firewall hops and network address translation (NAT). It also allows you to configure network traffic so that it is initiated from the more secure network zone.

NAT alone is not a reason to use the firewall gateway, which is content-neutral and can proxy any TCP connection. In most cases, NAT processing is can be handled by the PIPE protocol (IP.PIPE or IP.SPIPE), which can be used without the firewall gateway. Use the gateway when you have any of the following scenarios:

- A single TCP connection cannot be made to span between IBM Tivoli Monitoring components An example would be that there are multiple firewalls between these components and a policy that does not allow a single connection to traverse multiple firewalls.
- Connection requirements do not allow the IBM Tivoli Monitoring default pattern of connections to the hub monitoring server. An example here would be agents residing in a less-secure zone connecting to a monitoring server residing in a more-secure zone. Security policy would only allow a connection to be established from a more-secure zone to a less-secure zone, but not the other way round.
- You must reduce open firewall ports to a single port or connection. For example, rather than opening the port for every system being monitored, you would like

to consolidate the ports to a single “concentrator”. Connection requirements do not allow the IBM Tivoli Monitoring default pattern of connections to the hub monitoring server.

- You must reduce open firewall ports to a single port or connection. You must manage agent failover and monitoring server assignment symbolically at the hub monitoring server end of the gateway. Because gateway connections are made between matching service names, an administrator can change the failover and monitoring server assignment of downstream gateway agents by changing the client proxy bindings next to the hub monitoring server.

For detailed information on implementing the Firewall gateway, see the Firewall Gateway Feature whitepaper at: http://publib.boulder.ibm.com/infocenter/tivihelp/v15r1/index.jsp?topic=/com.ibm.itm.doc/itm_firewall.htm

Appendix D. IBM Tivoli product codes

The following table lists the product codes that identify the different IBM Tivoli Monitoring components and base agents. Use these codes when running commands. For information on the product codes for Tivoli Monitoring distributed agents and other Tivoli Management Services based agents, see the product documentation.

Table 124. Component product codes for infrastructure components and base monitoring agents

Component	Product code
Endpoint monitoring agent	tm
i5/OS monitoring agent	a4
Linux OS monitoring agent	lz
Summarization and Pruning agent	sy
Tivoli Enterprise Monitoring Server	ms
Tivoli Enterprise Portal browser client	cw
Tivoli Enterprise Portal desktop client	cj
Tivoli Enterprise Portal Server	cq
Universal Agent	um
UNIX Log Alert monitoring agent	ul
UNIX OS monitoring agent	ux
Warehouse Proxy	hd
Windows OS monitoring agent	nt
IBM Eclipse Help Server	kf

© Copyright IBM Corp. 2005, 2007

Appendix E. Maintaining the EIB on Linux or UNIX

To ensure the effective operation of your monitoring server, back up your EIB tables as part of your routine maintenance. The EIB contains the attributes and other data that define the agents to the server. The following files, which are stored in the <*install_dir*>/tables/eib directory, comprise the EIB.

Table 125. EIB Files

***.db Files**		***.idx Files**	
qa1cacts.db	qa1daggr.db	qa1cacts.idx	qa1daggr.idx
qa1cckpt.db	qa1dcct.db	qa1cckpt.idx	qa1dcct.idx
qa1ccobj.db	qa1dcct2.db	qa1ccobj.idx	qa1dcct2.idx
qa1ccomm.db	qa1dmobj.db	qa1ccomm.idx	qa1dmobj.idx
qa1ceibl.db	qa1dmtmp.db	qa1ceibl.idx	qa1dmtmp.idx
qa1chost.db	qa1dobja.db	qa1chost.idx	qa1dobja.idx
qa1ciobj.db	qa1dpcyf.db	qa1ciobj.idx	qa1dpcyf.idx
qa1cmcfg.db	qa1drnke.db	qa1cmcfg.idx	qa1drnke.idx
qa1cnodl.db	qa1drnkg.db	qa1cnodl.idx	qa1drnkg.idx
qa1cplat.db	qa1dsnos.db	qa1cplat.idx	qa1dsnos.idx
qa1cpset.db	qa1dspst.db	qa1cpset.idx	qa1dspst.idx
qa1cruld.db	qa1dstms.db	qa1cruld.idx	qa1dstms.idx
qa1csitf.db	qa1dstsa.db	qa1csitf.idx	qa1dstsa.idx
qa1csmni.db	qa1dstua.db	qa1csmni.idx	qa1dstua.idx
qa1cstsc.db	qa1dswrs.db	qa1cstsc.idx	qa1dswrs.idx
qa1cstsh.db	qa1dswus.db	qa1cstsh.idx	qa1dswus.idx
qa1cthre.db	qa1dwgrp.db	qa1cthre.idx	qa1dwgrp.idx
qa1dactp.db	qa1dwork.db	qa1dactp.idx	qa1dwork.idx

© Copyright IBM Corp. 2005, 2007

Appendix F. Securing your Linux or UNIX IBM Tivoli Monitoring installation

On UNIX and Linux operating systems, the product installation process creates the majority of directories and files with **world write** permissions. This configuration creates a security situation that is not acceptable in many enterprises. The **secureMain** utility helps you bring the monitoring environment into compliance with the security standards of your company. Run the **secureMain** utility on all installations, especially those installations that include the UNIX OS Agent, to prevent privilege escalation.

Note: You do not need to be logged in as a root user to run this utility, but you are prompted for the root password when it is required.

Usage

The **secureMain** commands use the following syntax:

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

where variables are defined as follows:

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

If **secureMain** is invoked with no parameters, the usage text is displayed.

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

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

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

© Copyright IBM Corp. 2005, 2007

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

secureMain unlock is used to loosen permissions in an IBM Tivoli Monitoring 6.2 installation. **secureMain unlock** is normally not necessary, but can be run if desired. It should be run before installing or configuring components.

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

Examples

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

```
secureMain -g itmgroup lock
```

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

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

Scenario with secureMain

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

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

Appendix G. Uninstalling IBM Tivoli Monitoring

Use the following steps to uninstall IBM Tivoli Monitoring:

- "Uninstalling the entire IBM Tivoli Monitoring environment"
- "Uninstalling an individual IBM Tivoli Monitoring agent or component" on page 446
- "Uninstalling the event synchronization component" on page 450

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"
- "Uninstalling the environment on Linux or UNIX" on page 445

If you want to remove just one component such as an agent, see "Uninstalling an individual IBM Tivoli Monitoring agent or component" on page 446.

Note: If you plan to reinstall IBM Tivoli Monitoring into a different directory than the one used for this installation, you must stop and restart this computer before reinstalling IBM Tivoli Monitoring.

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**. The following window is displayed.

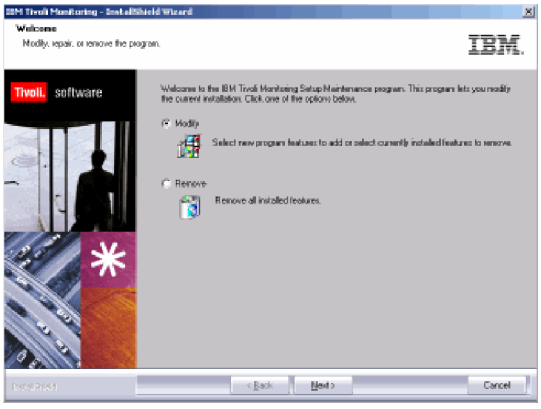


Figure 66. Uninstalling IBM Tivoli Monitoring

4. Select **Remove** and click **Next**.
   The following window is displayed.

© Copyright IBM Corp. 2005, 2007

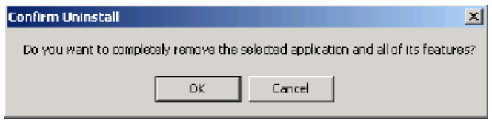


Figure 67. Confirming the uninstallation

5. Click **OK**.
   The following progress window is displayed.

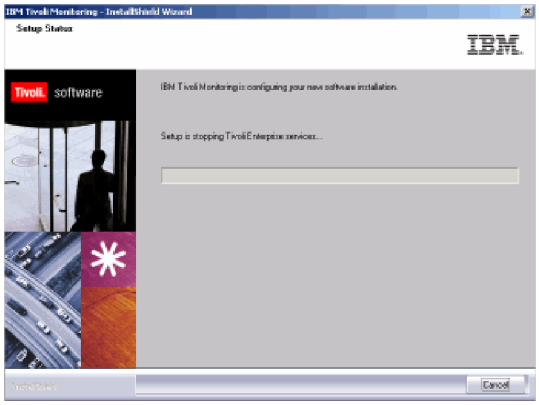


Figure 68. Stopping Tivoli components prior to uninstallation

After Tivoli Enterprise services have stopped, you are asked if you want to remove the Tivoli Enterprise Portal database.

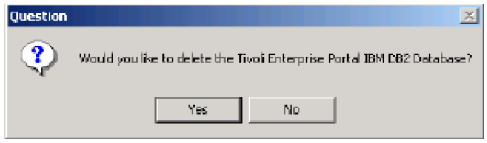


Figure 69. Removing the portal database

6. Click **Yes**.
   The following window is displayed, requesting information required to remove the database:



Figure 70. Database information

7. Type the password for the database administrator in the **Admin Password** field and click **OK**.
   The following progress window is displayed.

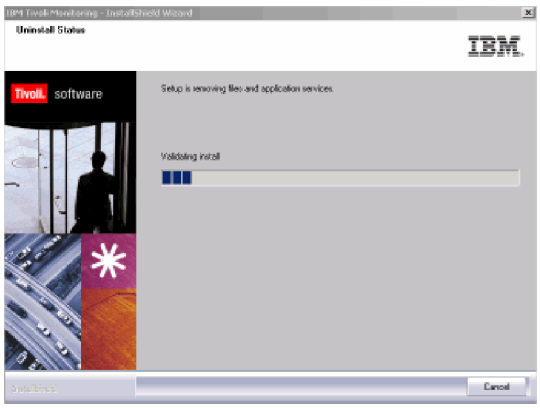


Figure 71. Uninstallation progress window

A pop-up window, indicating that GSKit is being uninstalled, is displayed.



Figure 72. GSKit uninstallation

After GSKit is uninstalled, the following window is displayed:

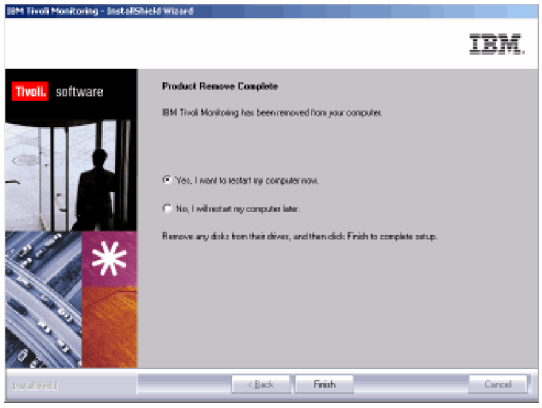


Figure 73. Successful uninstallation

8. Click **Finish**.

Uninstalling the environment on Linux or UNIX

Use the following steps to uninstall IBM Tivoli Monitoring from a UNIX computer:

1. From a command prompt, run the following command to change to the appropriate /bin directory:

   ```
   cd install_dir/bin
   ```

   where *install_dir* 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 installed product that you want to uninstall. Repeat this step for each additional installed product you want to uninstall.
4. After you have removed all installed components, you are asked if you want to remove the installation directory. Type `y` and press Enter.

You can also run the following command to remove all installed components from the command line:

```
./uninstall.sh REMOVE EVERYTHING
```

After the command completes, you can manually remove the IBM Tivoli Monitoring installation directory.

Note: If for any reason, the UNIX uninstallation is not successful, run the following command to remove all IBM Tivoli Monitoring directories:

```
rm -r install_dir
```

This uninstallation program does not delete the database created for Tivoli Enterprise Portal on a Linux portal server. If you want to delete that database, you must remove it manually. See the documentation for your database software for information about deleting a database.

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"
- "Uninstalling a component on Linux or UNIX" on page 447
- "Uninstalling OMEGAMON agents" on page 447
- "Removing an agent through the Tivoli Enterprise Portal" on page 449

Note: If you plan to reinstall a IBM Tivoli Monitoring component into a different directory than the one used for this installation, you must stop and restart this computer before reinstalling the IBM Tivoli Monitoring component.

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). You cannot uninstall the application support files laid down for a Windows Tivoli Enterprise Monitoring Server without uninstalling the monitoring server.

1. From the desktop, click **Start → Settings → Control Panel** (for Windows 2000 or 2003) or **Start → Control Panel** (for Windows XP).
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.

      Note: When you are uninstalling the Tivoli Enterprise Portal Server, the installer gives you the option to remove the portal server database. If there are other databases created by Tivoli Monitoring in this or previous version on the computer, the installer gives you the option to remove them as well.
9. Click **Finish** to complete the uninstallation.

Uninstalling a component on Linux or UNIX

Use the following steps to remove a component on a 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 install_dir/bin
   ```
   where *install_dir* 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.

   Note: When you are uninstalling the Tivoli Enterprise Portal Server, the installer gives you the option to remove the portal server database. If there are other databases created by Tivoli Monitoring in this or previous version on the computer, the installer gives you the option to remove them as well.

Uninstalling OMEGAMON agents

Use the following steps to remove OMEGAMON agents from a computer. Table 126 on page 448 and Table 127 on page 449 list the agents by internal code, release, and descriptive name.

1. Launch Manage Candle Services (350 or 360) or Manage Tivoli Enterprise Monitoring Services.
2. Use the **Description** and **Release** columns to locate the agent service name.

3. Stop the service by right-clicking the name and clicking **Stop**.
4. Take note of any task or subsystem names that are listed in the column for your agent. Usually this column lists `Primary` unless your agent supports instances. If your agent supports instances, record these names for later use.
5. Unconfigure the agent by right-clicking the name and clicking **Advanced → Unconfigure**. The **Configured** column changes from `Yes` to `No`. Continue to unconfigure all instances found in step 4.
6. Open the Windows Explorer and navigate to the installation directory for OMEGAMON 350 or 360 products and IBM Tivoli Monitoring. The default directories are C:\Candle Candle OMEGAMON and C:\IBM\ITM for IBM Tivoli Monitoring. Then navigate to the CMA directory.
7. Delete files K??ENV (Task/SubSystem name Primary) and any instances shown as K??ENV_INSTANCENAME (Task/SubSystem name from step 4).
8. Delete any *PC**.EXE or *PC**.DLL files for the product. *PC* is the product internal identifier three-character code from the tables.
9. Exit Manage Candle Services or Manage Tivoli Enterprise Monitoring Services and launch it again. The agent and all instances should not be shown under the **Service/Application** column.

Note: You can also use this procedure to remove IBM Tivoli Monitoring agents if you use the TMAITM6 directory instead of the CMA directory in step 6. All of the other steps do not change.

Table 126. Candle OMEGAMON Release 04R1

Internal Identifier	Release	Description
K3Z	400®	Windows Server Active Directories Monitoring Agent
KA2	120	Alert Adapter for AF/Remote
KA4	300	Monitoring Agent for OS/400®
KBL	320	CASP Directory Server Monitoring Agent
KBR	320	CASP Exchange Connector Monitoring Agent
KEZ	251	eBA® Solutions Monitoring Agent
KIC	100	WebSphere® InterChange Server Monitoring Agent
KIE	100	WebSphere InterChange Server Data Source
KMA	201	Alert Adapter for Remedy ARS
KMC	360	WebSphere MQ Configuration Agent
KMQ	360	WebSphere MQ Monitoring Agent
KNW	300	NetWare Monitoring Agent
KOQ	301	Microsoft SQL Server Monitoring Agent
KOR	301	Oracle Monitoring Agent
KOY	300	Sybase Monitoring Agent
KPT	201	Alert Adapter for Peregrine Service Center
KQI	120	WebSphere Integration Brokers Monitoring Agent
KSA	301	R/3 Monitoring Agent
KTX	300	Tuxedo Monitoring Agent
KUD	400	DB2 Universal Database™ Monitoring Agent
KWE	130	WebSphere Application Server Monitoring Agent

Table 126. Candle OMEGAMON Release 04R1 (continued)

Internal Identifier	Release	Description
KWL	100	BEA WebLogic Server Monitoring Agent
KWN	100	Windows Management Web Service

Table 127. Candle OMEGAMON Release BIV110

Internal Identifier	Release	Description
KIC	110	WebSphere InterChange Server Monitoring Agent
KIE	110	WebSphere InterChange Server Data Source
KMC	370	WebSphere MQ Configuration Agent
KMQ	370	WebSphere MQ Agent
KQI	130	WebSphere Integration Brokers Monitoring Agent

Removing an agent through the Tivoli Enterprise Portal

You can also uninstall non-OS monitoring agents from the Tivoli Enterprise Portal by stopping the agent and removing its configuration settings. After you have removed the agent from the enterprise, you can completely uninstall the agent from the managed system. When you remove an agent, it is removed from any managed system lists to which it is assigned, any situation or policy distribution lists it was on, and any custom Navigator view items to which it was assigned.

Note: You cannot use the Tivoli Enterprise Portal to remove or uninstall OS agents.

Note: If the Manage Tivoli Monitoring Services utility is running when you uninstall the agent, it is shut down automatically by the uninstallation process.

Use the following steps to remove and optionally uninstall an agent:

1. In the Tivoli Enterprise Portal, right-click the agent Navigator item and click **Remove**.
2. Click **Yes** when you are asked to confirm the removal of the agent.
3. When you are asked to confirm that you want to permanently uninstall the agent, click **Yes** to uninstall or **No** to leave the agent installed on the computer.

Uninstalling the Warehouse Proxy

When you uninstall the Warehouse Proxy, the warehouse database is not removed and historical situations on the agent are not stopped.

Before you uninstall, do the following to account for this:

- Stop the historical situations.
- Drop the warehouse database.
- Remove the ODBC data source.
- Remove the Windows user, ITMUser, that was created to connect to a DB2 database.

Removing the ODBC data source connection

When you uninstall IBM Tivoli Monitoring, the ODBC data source created for the Warehouse Proxy agent is not removed automatically, which can cause problems when you reinstall IBM Tivoli Monitoring. To prevent these problems, manually remove the ODBC data source after you uninstall IBM Tivoli Monitoring.

For example, to remove the DB2 data source from the DB2 command line, run the following command:

```
DB2 UNCATALOG SYSTEM ODBC DATA SOURCE <datasource_name>
```

If you are using a Microsoft SQL database or an Oracle database, use the Windows ODBC Data Source Administrator utility to remove the ODBC data source.

Uninstalling the event synchronization component

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

Note: On Windows 2003 you must run the **change user /install** command from a command prompt before you begin. This puts The computer into the required "install" mode. After the uninstallation, run the **change user /execute** command to return the computer to its previous mode.

1. Set the Tivoli environment:
   - On Windows:

     ```
     C:\windows\system32\drivers\etc\Tivoli\setup_env.cmd
     ```

     or

     ```
     C:\winnt\system32\drivers\etc\Tivoli\setup_env.cmd
     ```
   - On operating systems like UNIX and Linux:

     ```
     . /etc/Tivoli/setup_env.sh
     ```
2. Run the following uninstallation program:
   - On Windows:

     ```
     %BINDIR%\TME\TEC\OM_TEC\_uninst\uninstaller.exe
     ```
   - On operating systems like UNIX and Linux:

     ```
     $BINDIR/TME/TEC/OM_TEC/_uninst/uninstaller.bin
     ```

   You can 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).
3. Follow the prompts in the uninstallation program.

When the uninstallation is completed, you can tell the installer what rule base should be loaded. If initial installation created a new rule base, the value shown in "Rule base name of rule base to be loaded on completion of this uninstall" will be Default, meaning that the Default rule base will be loaded. If the initial install updated an existing rule base, that rule base name is provided as the value for "Rule base name of rule base to be loaded on completion of this uninstall". You can override this value by typing in the name of the rule base you want to have loaded.

You can also tell the uninstaller to stop and restart the event server.

You can run the silent uninstallation using default processing or create a template to change the defaults. The default processing will load the Default rule base (or the existing rule base was chosen during installation) and will *not* restart the TEC server.

To create and use a template:

1. Create the template:
   - On Windows:

     ```
     %BINDIR%\TME\TEC\OM_TEC\_uninst\uninstaller.exe –options-template
       itmeventsynchU.txt
     ```

   - On operating systems like UNIX or Linux:

     ```
     $BINDIR/TME/TEC/OM_TEC/_uninst/uninstaller.bin –options-template
       itmeventsynchU.txt
     ```

2. Modify the template as desired:
   - To specify which rule base to load, modify the `restartTECU.uRBN` file.
   - To automatically restart the event server, modify the `restartTECU.restartTECU` file.
3. Set the Tivoli environment.
4. Run the uninstallation program as follows:
   - On Windows:

     ```
     %BINDIR%\TME\TEC\OM_TEC\_uninst\uninstaller.exe –options
       itmeventsynchU.txt –silent
     ```

   - On operating systems like UNIX or Linux:

     ```
     $BINDIR/TME/TEC/OM_TEC/_uninst/uninstaller.bin –options
       itmeventsynchU.txt –silent
     ```

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.

Uninstalling event synchronization manually

Use the instructions for the appropriate operating system to remove event synchronization manually.

HP11

1. Stop the situation update forwarder long-running process if it is still running:
   a. Find the long-running process using:

      ```
      ps –ef
      ```

   b. Use the kill command to remove the process:

      ```
      kill –9 <process_number>
      ```

2. Run the following to determine whether the operating system still knows that the event synchronization component is there:

   ```
   swlist -v TecEvntSyncInstaller
   ```

   If it is there but all the code has been deleted, or just the uninstaller is deleted, you can try running

   ```
   swremove TecEvntSyncInstaller
   ```

3. If errors are returned saying that TecEvntSyncInstaller cannot be removed due to consistency or dependency checks, create a file named something like "remove_EvntSync.txt" and add these two lines:

```
enforce_dependencies=false
enforce_scripts=false
```

then run the **swremove** command as follows:

```
swremove -X remove_EnvtSync.txt TecEnvtSyncInstaller
```

This tells the **swremove** command to ignore checks and dependencies and remove anyhow.

4. Remove any event synchronization directories that are left behind.

   Remove any directories found in OM_TEC including OM_TEC itself. OM_TEC is found in $BINDIR/TME/TEC. To use $BINDIR you must run the following command:

   ```
   . /etc/Tivoli/setup_env.sh
   ```

   If the installation was for Netcool/OMNIbus, remove files from the location indicated during installation.

Windows

1. Stop the situation update forwarder long running process if it is still running:
   a. In the Control Panel, open **Administrative Tools**, then **Services**.
   b. Find the Tivoli Situation Update Forwarder service, and right-click it and select **Stop**.
2. Go to operating system directory (C:\windows or C:\winnt) and open the vpd.properties file.
3. Remove all lines that have itmTecEvntSyncProduct, EvntSyncForwarder, itmTecEvntSyncLapComp or EvntSyncForwarderWin in them.
4. Remove any event synchronization directories that are left behind.

   Remove any directories found in OM_TEC including OM_TEC itself. OM_TEC is found in %BINDIR%/TME/TEC. To use %BINDIR% you must run the C:\windows\system32\drivers\etc\Tivoli\setup_env.cmd command. If the installation was for Netcool/OMNIbus, remove the files from the location indicated during installation.

AIX

1. Stop the situation update forwarder long running process if it is still running:
   a. Find the long running process using:

      ```
      ps –ef
      ```

   b. Use the kill command to remove the process:

      ```
      kill –9 <process_number>
      ```

2. Go to operating system directory (this is typically /usr/lib/objrepos) and open the vpd.properties file.
3. Remove all lines that have itmTecEvntSyncProduct, EvntSyncForwarder, itmTecEvntSyncLapComp or EvntSyncForwarderWin in them.
4. Remove any event synchronization directories that remain.

   Remove any directories found in OM_TEC including OM_TEC itself. OM_TEC is found in $BINDIR/TME/TEC. To use $BINDIR you must run the following command:

   ```
   . /etc/Tivoli/setup_env.sh
   ```

If the installation was for Netcool/OMNIbus, remove the files from the location specified during installation.

Linux

1. Stop the situation update forwarder long running process if it is still running:
   a. Find the long running process using:
      ```
      ps –ef
      ```
   b. Use the kill command to remove the process:
      ```
      kill –9 <process_number>
      ```
2. Go to operating system directory (this is typicall / or /root) and open the file vpd.properties.
3. Remove all lines that have itmTecEvntSyncProduct, EvntSyncForwarder, itmTecEvntSyncLapComp or EvntSyncForwarderWin in them.
4. Remove any event synchronization directories that are left behind.

   Remove any directories found in OM_TEC including OM_TEC itself. OM_TEC is found in $BINDIR/TME/TEC. To use $BINDIR you must run the following command:

   ```
   . /etc/Tivoli/setup_env.sh
   ```

   If the installation was for OMNIbus, remove the files from the location specified during installation

Solaris

1. Stop the situation update forwarder long running process if it is still running:
   a. Find the long running process using:
      ```
      ps –ef
      ```
   b. Use the kill command to remove the process:
      ```
      kill –9 <process_number>
      ```
2. Run the following command to remove the situation update forwarder:
   ```
   pkgrm –A ISitmTecE
   ```
3. Remove any event synchronization directories that are left behind.

   Remove any directories found in OM_TEC including OM_TEC itself. OM_TEC is found in $BINDIR/TME/TEC. To use $BINDIR you must run the following command:

   ```
   . /etc/Tivoli/setup_env.sh
   ```

   If the installation was for OMNIbus, remove the files from the location specified during installation.

Appendix H. Documentation library

This appendix contains information about the publications related to IBM Tivoli Monitoring and to the commonly shared components of Tivoli Management Services. These publications are listed in the following categories:

- IBM Tivoli Monitoring library
- Related publications

See *IBM Tivoli Monitoring and OMEGAMON XE Products: Documentation Guide*, SC23-8816, for information about accessing and using the publications. You can find the *Documentation Guide* in the IBM Tivoli Monitoring and OMEGAMON XE Information Center at http://publib.boulder.ibm.com/infocenter/tivihelp/v15r1/.

To find a list of new and changed publications, click **What's new** on the Welcome page of the IBM Tivoli Monitoring and OMEGAMON XE Information Center. To find publications from the previous version of a product, click **Previous information centers** on the Welcome page for the product.

IBM Tivoli Monitoring library

The following publications provide information about IBM Tivoli Monitoring V6.2 and about the commonly shared components of Tivoli Management Services:

- *Quick Start Guide*, GI11-8058

  Introduces the components of IBM Tivoli Monitoring.
- *Exploring IBM Tivoli Monitoring*, SC32-1803

  Provides a series of exercises to help you explore IBM Tivoli Monitoring. By completing the activities in this workbook, you will install and configure your monitoring environment, explore both the graphical and command-line interfaces of the product, use some of the new features, and work with several monitoring agents.
- *Installation and Setup Guide*, GC32-9407

  Provides instructions for installing and configuring IBM Tivoli Monitoring components on Windows, Linux, and UNIX systems.
- *IBM Tivoli Management Services on z/OS Program Directory*, GI11-4105

  Gives instructions for the SMP/E installation of the Tivoli Management Services components on z/OS.
- *Configuring IBM Tivoli Enterprise Monitoring Server on z/OS*, SC32-9463

  Gives detailed instructions for using the Configuration Tool to configure Tivoli Enterprise Monitoring Server on z/OS systems. Includes scenarios for using batch mode to replicate monitoring environments across the z/OS enterprise. Also provides instructions for setting up security and for adding application support to a Tivoli Enterprise Monitoring Server on z/OS.
- *Administrator's Guide*, SC32-9408

  Describes the support tasks and functions required for the Tivoli Enterprise Portal Server and clients, including Tivoli Enterprise Portal user administration.
- Tivoli Enterprise Portal online help

  Provides context-sensitive reference information about all features and customization options of the Tivoli Enterprise Portal. Also gives instructions for using and administering the Tivoli Enterprise Portal.

© Copyright IBM Corp. 2005, 2007

- *User's Guide*, SC32-9409

  Complements the Tivoli Enterprise Portal online help. The guide provides hands-on lessons and detailed instructions for all Tivoli Enterprise Portal features.
- *Command Reference*, SC32-6045

  Provides detailed syntax and parameter information, as well as examples, for the commands you can use in IBM Tivoli Monitoring.
- *Problem Determination Guide*, GC32-9458

  Provides information to help you troubleshoot problems with the software.
- *Messages*, SC23-7969

  Lists and explains messages generated by all IBM Tivoli Monitoring components and by z/OS-based Tivoli Management Services components (such as Tivoli Enterprise Monitoring Server on z/OS and TMS:Engine).
- *Upgrading from V5.1.2*, GC32-1976

  Gives instructions for upgrading custom resource models from IBM Tivoli Monitoring V5.1.2 to IBM Tivoli Monitoring V6.2.
- *IBM Tivoli Universal Agent User's Guide*, SC32-9459

  Introduces you to the IBM Tivoli Universal Agent, an agent of IBM Tivoli Monitoring. The IBM Tivoli Universal Agent enables you to use the monitoring and automation capabilities of IBM Tivoli Monitoring to monitor any type of data you collect.
- *IBM Tivoli Universal Agent API and Command Programming Reference Guide*, SC32-9461

  Explains the procedures for implementing the IBM Tivoli Universal Agent APIs and provides descriptions, syntax, and return status codes for the API calls and command-line interface commands.
- *Agent Builder User's Guide*, SC32-1921

  Explains how to use the Agent Builder for creating monitoring agents and their installation packages, and for adding functions to existing agents.
- *Fix Pack Readme and Documentation Addendum*

  Describes the installation process for a fix pack and provides updated information on problems and workarounds associated with the fix pack. A new version of this document is created for each fix pack.

Documentation for the base agents

If you purchased IBM Tivoli Monitoring as a product, you received a set of operating system monitoring agents (also called *OS agents* or *base agents*) as part of the product. If you purchased a monitoring agent product (for example, an OMEGAMON XE product) that includes the commonly shared components of Tivoli Management Services, you did not receive the base agents.

The following publications provide information about using the base agents.

- *Windows OS Agent User's Guide*, SC32-9445
- *UNIX OS Agent User's Guide*, SC32-9446
- *Linux OS Agent User's Guide*, SC32-9447
- *i5/OS Agent User's Guide*, SC32-9448
- *UNIX Log Agent User's Guide*, SC32-9471
- *Monitoring Agent for IBM Tivoli Monitoring 5.x Endpoint User's Guide*, SC32-9490

Related publications

You can find useful information about the OMEGAMON XE monitoring agent products in the IBM Tivoli Monitoring and OMEGAMON XE Information Center at http://publib.boulder.ibm.com/infocenter/tivihelp/v15r1/.

Other sources of documentation

You can also obtain technical documentation about IBM Tivoli Monitoring and OMEGAMON XE products from the following sources:

- IBM Tivoli Open Process Automation Library (OPAL)

  http://www.ibm.com/software/tivoli/opal

  OPAL is an online catalog that contains integration documentation as well as other downloadable product extensions. This library is updated daily.
- Redbooks

  http://www.redbooks.ibm.com/

  IBM Redbooks®, Redpapers, and Redbooks Technotes provide information about products from platform and solution perspectives.
- Technotes

  You can find Technotes through the IBM Software Support Web site at http://www.ibm.com/software/support/probsub.html, or more directly through your product Web site, which contains a link to Technotes (under **Solve a problem**).

  Technotes provide the latest information about known product limitations and workarounds.

Appendix I. Support for problem solving

If you have a problem with your IBM software, you want to resolve it quickly. This section describes the following options for obtaining support for IBM software products:

- "Using IBM Support Assistant"
- "Obtaining fixes"
- "Receiving weekly support updates" on page 460
- "Contacting IBM Software Support" on page 461

Using IBM Support Assistant

The IBM Support Assistant is a free, stand-alone application that you can install on any workstation. You can then enhance the application by installing product-specific plug-in modules for the IBM products you use.

The IBM Support Assistant saves you the time it takes to search the product, support, and educational resources. The IBM Support Assistant helps you gather support information when you need to open a problem management record (PMR), which you can then use to track the problem.

The product-specific plug-in modules provide you with the following resources:

- Support links
- Education links
- Ability to submit problem management reports

For more information, and to download the IBM Support Assistant, see http://www.ibm.com/software/support/isa. After you download and install the IBM Support Assistant, follow these steps to install the plug-in for your Tivoli product:

1. Start the IBM Support Assistant application.
2. Select **Updater** on the Welcome page.
3. Select **New Properties and Tools** or select the **New Plug-ins** tab (depending on the version of IBM Support Assistant installed).
4. Under **Tivoli**, select your product, and then click **Install**. Be sure to read the license and description.

   If your product is not included on the list under **Tivoli**, no plug-in is available yet for the product.
5. Read the license and description, and click **I agree**.
6. Restart the IBM Support Assistant.

Obtaining fixes

A product fix might be available to resolve your problem. To determine which fixes are available for your Tivoli software product, follow these steps:

1. Go to the IBM Software Support Web site at http://www.ibm.com/software/support.
2. Under **Select a brand and/or product**, select **Tivoli**.

© Copyright IBM Corp. 2005, 2007

If you click **Go**, the **Search within all of Tivoli support** section is displayed. If you don't click **Go**, you see the **Select a product** section.

3. Select your product and click **Go**.
4. Under **Download**, click the name of a fix to read its description and, optionally, to download it.

   If there is no **Download** heading for your product, supply a search term, error code, or APAR number in the field provided under **Search Support (this product)**, and click **Search**.

For more information about the types of fixes that are available, see the *IBM Software Support Handbook* at http://techsupport.services.ibm.com/guides/handbook.html.

Receiving weekly support updates

To receive weekly e-mail notifications about fixes and other software support news, follow these steps:

1. Go to the IBM Software Support Web site at http://www.ibm.com/software/support.
2. Click **My support** in the far upper-right corner of the page under **Personalized support**.
3. If you have already registered for **My support**, sign in and skip to the next step. If you have not registered, click **register now**. Complete the registration form using your e-mail address as your IBM ID and click **Submit**.
4. The **Edit profile** tab is displayed.
5. In the first list under **Products**, select **Software**. In the second list, select a product category (for example, **Systems and Asset Management**). In the third list, select a product sub-category (for example, **Application Performance & Availability** or **Systems Performance**). A list of applicable products is displayed.
6. Select the products for which you want to receive updates.
7. Click **Add products**.
8. After selecting all products that are of interest to you, click **Subscribe to email** on the **Edit profile** tab.
9. In the **Documents** list, select **Software**.
10. Select **Please send these documents by weekly email**.
11. Update your e-mail address as needed.
12. Select the types of documents you want to receive.
13. Click **Update**.

If you experience problems with the **My support** feature, you can obtain help in one of the following ways:

Online
Send an e-mail message to erchelp@ca.ibm.com, describing your problem.

By phone
Call 1-800-IBM-4You (1-800-426-4968).

Contacting IBM Software Support

IBM Software Support provides assistance with product defects. The easiest way to obtain that assistance is to open a PMR or ETR directly from the IBM Support Assistant (see "Using IBM Support Assistant" on page 459).

Before contacting IBM Software Support, your company must have an active IBM software maintenance contract, and you must be authorized to submit problems to IBM. The type of software maintenance contract that you need depends on the type of product you have:

- For IBM distributed software products (including, but not limited to, Tivoli, Lotus®, and Rational® products, as well as DB2 and WebSphere products that run on Windows or UNIX operating systems), enroll in Passport Advantage® in one of the following ways:

  Online

  Go to the Passport Advantage Web site at http://www-306.ibm.com/software/howtobuy/passportadvantage/pao_customers.htm .

  By phone

  For the phone number to call in your country, go to the IBM Software Support Web site at http://techsupport.services.ibm.com/guides/contacts.html and click the name of your geographic region.
- For customers with Subscription and Support (S & S) contracts, go to the Software Service Request Web site at https://techsupport.services.ibm.com/ssr/login.
- For customers with IBMLink™, CATIA, Linux, OS/390®, iSeries, pSeries, zSeries, and other support agreements, go to the IBM Support Line Web site at http://www.ibm.com/services/us/index.wss/so/its/a1000030/dt006.
- For IBM eServer™ software products (including, but not limited to, DB2 and WebSphere products that run in zSeries, pSeries, and iSeries environments), you can purchase a software maintenance agreement by working directly with an IBM sales representative or an IBM Business Partner. For more information about support for eServer software products, go to the IBM Technical Support Advantage Web site at http://www.ibm.com/servers/eserver/techsupport.html.

If you are not sure what type of software maintenance contract you need, call 1-800-IBMSERV (1-800-426-7378) in the United States. From other countries, go to the contacts page of the *IBM Software Support Handbook* on the Web at http://techsupport.services.ibm.com/guides/contacts.html and click the name of your geographic region for phone numbers of people who provide support for your location.

To contact IBM Software support, follow these steps:

1. "Determining the business impact"
2. "Describing problems and gathering information" on page 462
3. "Submitting problems" on page 462

Determining the business impact

When you report a problem to IBM, you are asked to supply a severity level. Use the following criteria to understand and assess the business impact of the problem that you are reporting:

Severity 1
The problem has a *critical* business impact. You are unable to use the program, resulting in a critical impact on operations. This condition requires an immediate solution.

Severity 2
The problem has a *significant* business impact. The program is usable, but it is severely limited.

Severity 3
The problem has *some* business impact. The program is usable, but less significant features (not critical to operations) are unavailable.

Severity 4
The problem has *minimal* business impact. The problem causes little impact on operations, or a reasonable circumvention to the problem was implemented.

Describing problems and gathering information

When describing a problem to IBM, be as specific as possible. Include all relevant background information so that IBM Software Support specialists can help you solve the problem efficiently. To save time, know the answers to these questions:

- Which software versions were you running when the problem occurred?
- Do you have logs, traces, and messages that are related to the problem symptoms? IBM Software Support is likely to ask for this information.
- Can you re-create the problem? If so, what steps were performed to re-create the problem?
- Did you make any changes to the system? For example, did you make changes to the hardware, operating system, networking software, and so on.
- Are you currently using a workaround for the problem? If so, be prepared to explain the workaround when you report the problem.

Submitting problems

You can submit your problem to IBM Software Support in one of two ways:

Online
Click **Submit and track problems** on the IBM Software Support site at http://www.ibm.com/software/support/probsub.html. Type your information into the appropriate problem submission form.

By phone
For the phone number to call in your country, go to the contacts page of the *IBM Software Support Handbook* at http://techsupport.services.ibm.com/guides/contacts.html and click the name of your geographic region.

If the problem you submit is for a software defect or for missing or inaccurate documentation, IBM Software Support creates an Authorized Program Analysis Report (APAR). The APAR describes the problem in detail. Whenever possible, IBM Software Support provides a workaround that you can implement until the APAR is resolved and a fix is delivered. IBM publishes resolved APARs on the Software Support Web site daily, so that other users who experience the same problem can benefit from the same resolution.

Appendix J. Notices

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

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

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

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

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

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

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

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

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

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

© Copyright IBM Corp. 2005, 2007

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

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

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

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

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

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

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

Trademarks

AIX, Candle, CICS, DB2, DB2 Universal Database, i5/OS, IBM, the IBM logo, IBMLink, IMS, iSeries, Lotus, Netcool/Objectserver, Netcool/OMNIbus, OMEGAMON, OMEGAMON Monitoring Agent, OS/400, Passport Advantage, pSeries, Rational, Tivoli, Tivoli Enterprise, Tivoli Enterprise Console, WebSphere, z/OS, z/VM, and zSeries are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both.

Adobe is a registered trademark of Adobe Systems Incorporated in the United States, other countries, or both.

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

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

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



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

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

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

Index

Special characters

/3GB boot option 10
/etc/hosts file 362

A

Access Method, Network 69
acting hub monitoring server 37
adding application support
  for non-Base agents 164
  itmcmd support command 122
  Linux desktop client 176
  Linux monitoring server 122, 168
  Linux portal server 172
  to a remote monitoring server from Linux or UNIX 179
  to a remote monitoring server from Windows 178
  UNIX monitoring server 122, 168
  Windows desktop client 174
  Windows monitoring server 166
  Windows portal server 171
Agent Builder 91
agent deployment 195
  deploying OS agents 200
  managing agent depot 199
  OS agents, deploying 200
  populating agent depot 195
  sharing an agent depot 199
  tacmd createNode command 200
  Universal Agent 203
agent depot 195
  DEPOTHOME environment variable 199
  location 199
  managing 199
  populating through install 196
  populating with tacmd addBundles command 198
  sharing 199
agent interoperability 103
agents
  application agents 6
  configuring 209
  deploying 195
  deploying OS agents 200
  IBM Tivoli Monitoring for Applications: mySAP Agent 95
  IBM Tivoli Monitoring for Databases: DB2 Agent 95, 96
  IBM Tivoli Monitoring for Databases: Oracle Agent 96
  IBM Tivoli Monitoring for Databases: Sybase Server Agent 96
  IBM Tivoli Monitoring: UNIX OS Agent 95, 96
  IBM Tivoli Monitoring: Windows OS Agent 95
  non-OS agents 6
  operating system (OS) agents 6
agents *(continued)*
  OS agents 6
  product codes 437
  removing through the portal 449
  starting 210
  stopping 210
  uninstalling OMEGAMON 447
  uninstalling on Linux 447
  uninstalling on UNIX 447
  uninstalling on Windows 446
aggregate data, amount of 21
AIX
  configuring the portal server 139, 143
  installing the portal server 137
  portal server installation 136
application agents 6
application support
  adding to a remote monitoring server from Linux or UNIX 179
  adding to a remote monitoring server from Windows 178
  for agents on Base DVD 164
  for non-Base agents 164
application support files
  installing remotely 11
application support media 161
application support, enabling
  enabling 159
application support, installing
  catalog and attribute files 159
  seed data 159
  SQL files 159
archdsc.tbl 66
architecture codes
  Linux 66
  UNIX 66
assessing the existing environment 14
  organizational perspective 15
  physical perspective 14
asymmetric cryptography 239
asymmetric encryption
  CA certificate request, creating 241
  CA certificate, receiving 242
  key database, creating 241
  password, saving to stash file 243
  public-private key pair, creating 241
  self-signed certificate, using 242
  setting up 240
  stash file 243
attribute files 11
attribute group
  aggregate data, amount of 21
  detailed data, amount of 20
  detailed records per day, number of 20
  hard disk drive footprint 20
attributes
  event synchronization event class 376
authenticating passwords 68
authenticating users 68
authorizing users 68
autostart scripts
  changes to 62

B

backing up a current installation
  UNIX or Linux 92
  Windows 93
backing up the portal server database 94
backing up the Tivoli Data Warehouse database 95
backup monitoring server, configuring 221
barrier firewall 427
Base DVD 115
base monitoring agents 3
basic cluster
  characteristics 46
  setup 45
Big Local Zone 65
Brio 7
browser
  configuring location on UNIX and Linux 186
  configuring location on Windows 186
browser client
  configuring 185
  defined 6
  starting 188, 189

C

CA
  See certificate authority
CA certificate
  receiving 242
  requesting 241
CA-ACF2 69
CA-TOP SECRET 69
Candle Management Workstation coexistence 100
CandleNet Portal database, upgrading 100
cat and atr files
  location of on Windows 178
catalog and attribute (cat and atr) files 159
catalog files 11
certificate
  creating a CA certificate request 241
  receiving a CA certificate 242
  requesting a CA certificate 241
  self-signed certificate, using 242
certificate authority 69
certificates, public key 69
change user /execute command 61

© Copyright IBM Corp. 2005, 2007

Citrix client 61
class, Sentry2_0_Base 61, 362
cluster, definition of 41
clustering concepts 41
clustering configurations 42
clustering deployment scenario 41
clustering technologies 41
CMS key store 69
co-existence 89
command, sitconfuser 403
command, tacmd createNode 202
commands
  cgabge user/execute 61
  db2licm 79
  itmcmd agent 155, 210
  itmcmd config 425
  itmcmd manage 208
  itmcmd server 122, 210
  itmcmd support 122
  sitconfig.sh 379
  sitconfsvruser.sh 380
  tacmd addBundles 198
  tacmd createNode 200
  tacmd startAgent 210
  tacmd stopAgent 210
common event connector
  described 11
Common Event Console view 7, 11
common services components 3
communications
  securing 67
  security options for 67
components
  behavior in a clustered environment 49
  browser client 6
  deciding which to upgrade 90
  desktop client 6
  event synchronization 7
  monitoring agents 6
  monitoring server 5
  portal client 5, 6
  portal server 5
  setting up in a cluster environment 45
  Summarization and Pruning agent 7
  Tivoli Data Warehouse 7
  Tivoli Enterprise Portal 5
  Tivoli Enterprise Portal Server 5
  Universal Agent 6
  Warehouse Proxy 7
configuration fields
  Netcool/OMNIbus event synchronization 390
configuration values
  validation 11
configuring
  agents 209
  hub monitoring server, UNIX 120
  Linux, silent 425
  monitoring agents 209
  monitoring agents on Linux 153
  monitoring agents on UNIX 153
  monitoring server 208
  monitoring server, Linux 120, 128
  password authentication 68
  port number assignments 228
configuring *(continued)*
  portal server 239
  portal server on Linux or AIX 139, 143
  remote monitoring server, UNIX 128
  response file, using 425
  UNIX, silent 425
  user authentication 211
configuring Netcool/OMNIbus Objectserver
  error event flow 402
  for program execution from scripts 398
  updating the Netcool/OMNIbus db schema 398
contents of installation media 9
creating a partition file 432
creating a workspace 352
Crystal Reports 7
customer support
  See Software Support

D

database size, estimating 22
databases, supported
  portal server 77
  Tivoli Data Warehouse 77
DB2
  creating a tablespace 25
  IBMDEFAULTGROUP 25
  increasing the size 25
DB2 data warehouse
  ODBC connection 285
DB2 product license key 79
DB2 UDB Enterprise Edition 77
db2licm command 79
default certificate 68
default event destination, defining 402
Default Small Local Zone 65
defining a portal server interface on Linux or UNIX 248
defining a portal server interface on Windows 247
deploying
  non-OS agents 202
    through the command line 203
    through the Tivoli Enterprise Portal 203
deploying a Universal Agent 203
deployment planning 13
DEPOTHOME environment variable 199
design process overview 13
desktop client
  adding application support on Linux 176
  adding application support on Windows 174
  configuring on Linux 159
  connecting to an external Web server 246
  creating a shortcut to launch using Web Start 193
  defined 6
  downloading from portal server 191
  external Web server, connecting to 246
desktop client *(continued)*
  installing 156
  installing on Linux from installation media 158
  installing on Windows from installation media 156
  Interoperable Object Reference (IOR) on Linux, updating 246
  Interoperable Object Reference (IOR) on Windows, updating 246
  IOR for Linux, updating 246
  IOR for Windows, updating 246
  launching from IBM Java Control Panel 192
  logs, location of 191
  planning worksheet, Linux 419
  planning worksheet, Windows 418
  starting 188
  using Web Start from the command line 192
detailed data, amount of 20
detailed records per day, number of 20
determining what to monitor 14
  managed systems 15
  organizational perspective 15
  physical perspective 14
digital certificates 239
disk requirements for Tivoli Data Warehouse 24
disk storage requirements 81
documentation
  See publications
downloading the desktop client using Java Web Start 191
DVDs, contents of 9

E

Eclipse Help Server 10
EGG1 encryption scheme 68
EIB
  See Enterprise Information Base (EIB)
EIB tables 439
EIF
  See Tivoli Event Integration Facility (EIF)
EIF probe, configuring 400
enabling application support for non-Base agents 164
enabling event forwarding on the monitoring server 402
enabling tracing for the JRE 191
ENDQUEUE column 356
ENDTIME column 357
Enterprise Information Base (EIB) 5
environment variables
  KDC_FAMILIES 231
  KDE_TRANSPORT 230, 231
  Warehouse Proxy 354
ephemeral keyword 429
ephemeral pipe
  implementing 429
ERRORMSG column 357
estimating warehouse database size 19
  aggregate data, amount of 21
  amount of detailed data 20

estimating warehouse database size *(continued)*
detailed records per day, number of 20
determining the size 22
hard disk drive footprint 20
worksheet 22
event forwarding 10
in a clustering environment 51
event integration scenarios 52
Netcool/OMNIbus 55
with Tivoli Enterprise Console 52
event integration, customizing on Netcool/OMNIbus 403
event synchronization
installation planning 60
installing 388
removing 450
Situation Update Forwarder process 379, 405
uninstalling programmatically 450
event synchronization component 361
changes made to event server 362
changing the configuration 379
changing the TCP/IP timeout setting 380
configuring the Netcool/OMNIbus Objectserver 397
creating a new rule base 375
defining additional monitoring servers 380
importing agent class files and rule set 377
importing class files and rule set 374
installing from the command line 366
Netcool/OMNIbus Objectserver 391
installing on Netcool/OMNIbus Objectserver 388
from a wizard 388
installing with the wizard 363
Netcool/OMNIbus Objectserver 388
methods of installing 362
overview 7
sitconfig.sh command 379
sitconfsvruser.sh command 380
uninstalling manually 451
upgrading to version 2.0.0.0 381
from a wizard 381
from the command line 383
using silent installation 384
using silent installation 371
Netcool/OMNIbus Objectserver 394
verifying installation
Netcool/OMNIbus 404
event synchronization configuration fields
Netcool/OMNIbus 390
event synchronization event class attributes 376
events, forwarding to Netcool/OMNIbus 402
events, forwarding to Tivoli Enterprise Console 378
example environments 27
EXPORTTIME column 356
external Web server
desktop client connection 246
portal client connection 246
portal server configuration 243

F

failback, definition of 42
failover support 221
configuring hub monitoring servers 221
configuring monitoring agents 227
configuring remote monitoring servers 225
verifying 227
failover, definition of 41
file descriptors limit 66
file, Sentry.baroc 376
files
atr 178
cat 178
catalog and attribute 159
seedkpp.log file 179
SQL 159
filter 69
firewall gateway, implementing 434
firewall support 433
editing the partition file
UNIX and Linux 433
Windows 432
sample partition file 434
firewalls
achieving interoperability across 427
and Network Address Translation 428
factors in implementation 427
flow of connection establishment 427
implementing with ephemeral pipe 429
implementing with firewall gateway 434
implementing with partition files 430
multiple network interface cards 247
NAT 247
NIC 247
number of internet zones 428
options for 427
permissions at 427
portal server interface, defining 247, 248
scenarios 249
server address continuity across 428
firewalls, achieving interoperability across 427
fixes, obtaining 459
flexible scheduling 11
forwarding events to Tivoli Enterprise Console 378
forwarding situation events 10, 52
to Netcool/OMNIbus 55
to Tivoli Enterprise Console 52
fsync() 235
fully qualified path names, using 64

G

get_config_parms procedure 403
Global Location Broker 350
Global Security Tool Kit 68
Global Sign-On Kit (GSKit) 239
Global Zone 65
globalization, installing support 183
GSKit 239
See also Global Security Tool Kit
installation requirements 77

H

HACMP
See High-Availability Cluster Multi-Processing
hard disk drive footprint 20
hardware requirements
distributed systems 80
System z 82
heartbeat interval 232
CTIRA_HEARTBEAT environment variable 233
performance issues 234
setting the interval 233
heartbeat monitoring 232
CTIRA_HEARTBEAT environment variable 233
performance issues 234
setting the interval 233
high availability
clustering technologies 41
high availability scenarios 34
High-Availability Cluster Multi-Processing 41
historical data 7
historical data collection
long-term 51
short-term 51
hot standby 221
configuring hub monitoring servers 221
configuring monitoring agents 227
configuring remote monitoring servers 225
deployment scenario 37
hub monitoring servers in 37
monitoring agents in 38
portal server in 38
remote monitoring servers in 38
verifying 227
HTTPS 239
See Secure Hypertext Transport Protocol (HTTPS)
hub monitoring server
adding application support on Linux 122
adding application support on UNIX 122
configuring on Linux 120
configuring on UNIX 120
configuring user authentication on Linux or UNIX 215
configuring user security on Windows 212
failover support 221

hub monitoring server *(continued)*
hot standby 221
in a clustered environment 49
in hot standby environment 37
installing 114
installing on Linux 119
installing on UNIX 119
installing on Windows 115
planning worksheet, Linux or UNIX 411
planning worksheet, Windows 410

I

IBM Eclipse Help Server 10
IBM HTTP Server on Linux, configuring 245
IBM Java Web Start
using to download the desktop client 189
IBM JRE
installing 189
IBM Redbooks 459
IBM Runtime Environments
installing 189
Linux 190
Windows 189
IBM Support Assistant 459
IBM Tivoli Enterprise Console integration 7
IBM Tivoli License Manager 3
IBM Tivoli License Manager, support for 11
IBM Tivoli Monitoring
agent deployment 195
assessing your needs 14
component status, monitoring 232
configuring components 207
design process 13
heartbeat monitoring 232
Java level, required 97
Manage Tivoli Monitoring Services 207
overview 3
planning deployment 13
remote deployment 195
removing 443
uninstalling 443
upgrading to 87
IBM Tivoli Monitoring for Applications: mySAP Agent 95
IBM Tivoli Monitoring for Databases: DB2 Agent 95, 96
IBM Tivoli Monitoring for Databases: Oracle Agent 96
IBM Tivoli Monitoring for Databases: Sybase Server Agent 96
IBM Tivoli Monitoring V5.1.2
upgrading 87
IBM Tivoli Monitoring V5.x
interoperability 87
IBM Tivoli Monitoring V6.2.0 Base DVD 115
IBM Tivoli Monitoring Web Services 255
adding users 258
defining hubs 255
verifying configuration 260
IBM Tivoli Monitoring: UNIX OS Agent 95, 96
IBM Tivoli Monitoring: Windows OS Agent 95
ICSF
See Integrated Cryptographic Service Facility
IIOP
See Internet Inter-ORB Protocol (IIOP)
iKeyman 239
iKeyMan 68
importing event synchronization class files and rule set 374
information to gather before installing 59
installation
hardware requirements, distributed systems 80
hardware requirements, System z 82
information to gather 59
Linux considerations 62
monitoring server name guidelines 61
operating systems, supported 70
order of install 61
overview of the process 59
required information 59
requirements 70
software requirements 82
UNIX considerations 62
Windows considerations 61
installation media
changes to 9
contents of 9
installation steps 113
installing 113
application support 164
desktop client 156
globalization support 183
hub monitoring server 114
language packs 183
Linux monitoring server 119, 127
monitoring agents 148
monitoring agents on Linux 152
monitoring agents on UNIX 152
monitoring agents on Windows 149
planning worksheets 409
portal server 129
remote monitoring server 123
silent 421
UNIX monitoring server 119, 127
Windows monitoring server 115, 124
installing all components on a single Windows computer 105
installing application support
catalog and attribute files 159
seed data 159
SQL files 159
installing into Solaris zones 65
installing monitoring agent .baroc files on the event server 377
installing the event synchronization component
on Netcool/OMNIbus Objectserver 388
Integrated Cryptographic Service Facility 68
Internet Information Server V5.0, configuring 243
Internet Information Server V6.0, configuring 244
Internet Inter-ORB Protocol (IIOP) 67
interoperability 89
Interoperable Object Reference (IOR)
updating on Linux 246
updating on Windows 246
Interoperable Object Reference (IOR) protocol 67
IOR
See Interoperable Object Reference (IOR) protocol
itm_proc.sql 403
ITMAgents<N> script 62
itmcmd agent command 155, 210
itmcmd config command 425
itmcmd manage command 208
itmcmd server command 122, 210
itmcmd startAgent command 210
itmcmd stopAgent command 210
itmcmd support command 122

J

Java Web Start
using to download the desktop client 189
JRE
enabling tracing for 191

K

KBB_RAS1 trace setting 351
kcirunas.cfg file 63
KDC_FAMILIES environment variable 231
KDC_FAMILIES variable 429
KDC_PARTITION environment variable 433
KDE_TRANSPORT environment variable 230, 231
KDE_TRANSPORT variable 429
key database 241
key database, creating 241
key, DB2 product license 79
keyword
ephemeral 429
KfwServices 66, 235
KGLCB_FSYNC_ENABLED parameter 235
KHD_CNP_SERVER_HOST 102
KHD_CNP_SERVER_PORT 102
KHD_MAX_ROWS_PER_TRANSACTIONS 102
KHD_MAX_ROWS_SKIPPED_PER_TABLE 102
KHD_SOURCE_DATABASE_PASSWORD 102
KHD_SOURCE_DATABASE_SCHEMA 102
KHD_SOURCE_DATABASE_USER 102
KHD_SOURCE_JDBC_DRIVER 102
KHD_SOURCE_URL 102
KHD_TARGET_DATABASE_PASSWORD 102
KHD_TARGET_DATABASE_SCHEMA 102
KHD_TARGET_DATABASE_USER 102
KHD_TARGET_JDBC_DRIVER 102
KHD_TARGET_URL 102

KHDENV_MIG 101, 102
khdmig.jar 101
KinConfg.exe) utility 93
Kochi fonts
  installing on SUSE 185
KPX_WAREHOUSE_LOCATION 350
KPX_WAREHOUSE_LOCATION
  variable 430

L

language packs, installing 183
large monitoring environment, multiple
  hub example 32
large monitoring environment, single hub
  example 30
LDAP
  not supported on z/OS 69
  using for user authentication 69
LDAP server certificate 69
ldapsearch 219
  sample command (no SSL) 220
  sample command with SSL 220
ldapsearch command-line options 219
ldedit command 235
libraries
  IBM Tivoli Monitoring 455
license key, DB2 product 79
License Manager, IBM Tivoli 3
Linux
  /etc/hosts file 64
  adding application support on
    monitoring server 122
  backing up a current installation 92
  configuring 425
  configuring desktop client 159
  configuring monitoring agents 153
  configuring portal desktop client 159
  configuring the portal server 139,
    143
  EIB tables 439
  file descriptors limit 66
  file permissions for monitoring
    agents 155
  fully qualified path names 64
  host names, setting 64
  hub monitoring server 119, 120
  installation considerations 62
  installation user account 64
  installing as root 64
  installing monitoring agents 152
  installing the desktop client from
    installation media 158
  installing the portal server 137
  maxfiles 66
  monitoring agents 152
  network interface cards 64
  NFS environment 64
  planning 62
  portal server installation 136
  remote monitoring server 127, 128
  response file configuration 425
  response file installation 423
  silent configuration 425
  silent installation 423
  starting monitoring agents 155
  starting portal server 148
Linux *(continued)*
  TCP/IP network services 64
Linux monitoring server
  advanced configuration 235
  firewall support 433
  KDC_PARTITION 433
  NAT 433
  network address translation
    (NAT) 433
Local Location Broker 350
location broker 428
Location Broker
  Global 350
  Local 350
logs
  for desktop client 189
LOGTMZDIFF column 357

M

maintenance
  in a clustered environment 52
Manage Tivoli Monitoring Services 207
  adding application support 178, 179
  agents, configuring 209
  application support, adding 178, 179
  configuring user authentication 211
  defining SOAP hubs 255
  editing the partition file
    UNIX and Linux 433
    Windows 432
  itmcmd manage command 208
  monitoring agents, configuring 209
  monitoring server, configuring 208
  starting components 210
  starting on Linux 208
  starting on UNIX 208
  starting on Windows 207
  stopping components 210
managed system factors 15
maxfiles 66
MAXWRITETIME column 357
medium monitoring environment
  example 29
memory
  allocating for browser client 185
memory requirements 81
Method, Network Access 69
Microsoft Cluster Server 41
Microsoft SQL data warehouse
  ODBC connection 306
Microsoft Windows Terminal
  Services 61
migrated information 91
migratewarehouse.bat 101
MINWRITETIME column 357
monitoring agent
  planning worksheet, Linux or
    UNIX 417
  planning worksheet, Windows 416
  removing through the portal 449
  uninstalling on Linux 447
  uninstalling on UNIX 447
  uninstalling on Windows 446
monitoring agent .baroc files, installing
  on the event server 377
monitoring agent deployment
  determining when to use 19
monitoring agents
  configuring 209
  configuring failover support 227
  configuring hot standby 227
  configuring on Linux 153
  configuring on UNIX 153
  definition 6
  deploying 195
  deploying OS agents 200
  file permissions, changing 155
  in a hot standby environment 38
  installing 148
  installing on Linux 152
  installing on UNIX 152
  installing on Windows 149
  monitoring agents on Linux 152
  product codes 437
  starting 210
  stopping 210
monitoring agents, base 3
monitoring environment
  agent deployment 19
  assessing needs 14
  design process 13
  determining what you need 14
  environment examples 27
  network diagram 15
  number of monitoring servers 16
  planning 13
  planning steps 13
  planning the design 16
  remote deployment 19
  sample deployments 27
  security considerations 18
  server placement 18
monitoring server
  adding application support on
    Linux 122, 168
  adding application support on
    UNIX 122
  adding application support on
    Windows 166
  agent depot, location 199
  agent depot, populating 195
  communications protocol planning
    worksheet 420
  configuring 208
  configuring failover support 221
  configuring hot standby 221
  configuring on Linux 120, 128
  configuring on UNIX 120, 128
  defined 5
  defining additional to the event server
    Netcool/OMNIbus 403
  DEPOTHOME environment
    variable 199
  determining the number needed 16
  EIB tables 439
  failover support 221
  file descriptor limit on UNIX 66
  forwarding events to
    Netcool/OMNIbus 402
  forwarding events to Tivoli Enterprise
    Console 378
  heartbeat interval, configuring 232

monitoring server *(continued)*
hot standby 221
installing on Linux 119, 127
installing on UNIX 119, 127
installing on Windows 115, 124
naming 61
starting 122, 210
stopping 122, 210
Tivoli Event Integration Facility 378, 402
user authentication, configuring 211
multiple network interface cards 64, 247
portal server interface, defining 247, 248
multiprocessor systems 80

N

naming the monitoring server 61
NAT 247, 433
See Network Address Translation (NAT)
Netcool/OMNIbus
information required for event forwarding 60
integration 55
planning 55
verifying installation of event synchronization component 404
Netcool/OMNIbus configuration, customizing 403
Netcool/OMNIbus event synchronization configuration fields 390
Netcool/OMNIbus Objectserver
configuring for event integration 397
configuring for program execution from scripts 398
configuring the EIF probe 400
configuring the error event flow 402
updating the db schema 398
Network Access Method 69
network address translation (NAT) 247, 433
portal server interface, defining 247, 248
Network Address Translation (NAT)
and firewalls 428
network diagram 15
network factors 15
network interface cards
specifying 64
NFS environment, installing into 64
NIC 247
portal server interface, defining 247, 248
node ID 181
node, definition of 41
non-NIS Solaris monitoring server, configuring permissions for 235
non-OS agents 6
deploying 202
nonsupported operating systems 88

O

OBJECT column 356, 357
ODBC connection
DB2 data warehouse 285
Microsoft SQL data warehouse 306
Oracle data warehouse 324
ODBC data source connection, removing 450
OMEGAMON
uninstalling agents 447
OMEGAMON Platform V350 and V360
agents, configuration settings 99
Candle Management Workstation coexistence 100
CandleNet Portal database 100
installation directory 99
Java level, required 100
migrating Warehouse Proxy data 101
OMEGAMON XE for CICS 100
terminology 99
unsupported functions 100
upgrading 87
using existing agents 103
when to run the upgrade 99
OMEGAMON XE for CICS 100
omegamon.baroc class file 362
omegamon.rls file 381
omegamon.rls rule set file 362
OPAL documentation 26, 457
operating system (OS) agents 6
operating systems
nonsupported 88
operating systems, supported 70
Optional Primary Network Name option 64
options
Security: Validate User 68
Oracle data warehouse
ODBC connection 324
organizational planning perspective 15
ORIGINNODE column 356, 357
OS agents 6
overview 3

P

partition file
creating 432
editing 432
UNIX and Linux 433
Windows 432
modifying 432
sample 434
partition files
implementing 430
sample scenarios 430
password authentication, configuring 68
password encryption 67
password, saving to stash file 243
physical planning perspective 14
managed systems factors 15
network factors 15
planning 13, 16
hardware requirements, distributed systems 80
hardware requirements, System z 82
installation 59
Linux considerations 62
managed system factors 15
planning *(continued)*
network diagram 15
number of monitoring servers 16
operating systems, supported 70
remote deployment 19
requirements 70
sample deployments 27
security considerations 18
server placement 18
software requirements 82
Tivoli Data Warehouse 19
UNIX considerations 62
where to put your servers 18
Windows considerations 61
worksheets 409
planning, upgrade 88
port number assignments
configuring client connections for the portal server 228
configuring for monitoring agents 230
configuring for the monitoring server 228
controlling 228
portal browser client
starting 188, 189
portal client 6
browser 185
connecting to an external Web server 246
external Web server, connecting to 246
planning considerations 26
portal desktop client
adding application support on Linux 176
adding application support on Windows 174
configuring on Linux 159
downloading with IBM Java Web Start 189
installing on Linux from installation media 158
installing on Windows from installation media 156
planning worksheet, Linux 419
planning worksheet, Windows 418
starting 188
portal server
adding application support on Linux 172
adding application support on Windows 171
backing up the database 94
configuring 239
configuring on Linux or AIX 139, 143
configuring SSL 239
configuring user authentication 211
defined 5
enabling SSL 240
external Web server 243
firewall scenarios 249
IBM HTTP Server on Linux 245
in a clustered environment 50
installing 129
installing on Linux or AIX 136, 137

portal server *(continued)*
installing on Windows 130
interface, defining 247, 248
Internet Information Server V5.0, configuring 243
Internet Information Server V6.0, configuring 244
planning worksheet, Linux 415
planning worksheet, Windows 414
reconfiguring in a hot standby environment 38
Secure Socket Layer (SSL) 239
SSL, configuring 239
starting 210
starting on Linux 148
stopping 210
supported databases 77
testing connection to the Tivoli Data Warehouse 351
portal server database
backing up 94
portal server interface
defining on Linux or UNIX 248
defining on Windows 247
prerequisites
for upgrading 89
primary hub monitoring server 37
problem determination
describing problems 462
determining business impact 461
submitting problems 462
problem resolution 459
processor requirements 80
proddsc.tbl 66, 424
product codes 437
Linux 66
UNIX 66
product license key, DB2 79
product overview 3
protocols
validation 11
public key certificates 69
public-private key pair 239
creating 241
publications
OPAL 26, 457
Redbooks 457
related 457
Technotes 457
types 455

R

RACF 69
rc.itm<N> script 62
Redbooks 457, 459
remote deployment 195
deploying OS agents 200
determining when to use 19
managing agent depot 199
OS agents, deploying 200
populating agent depot 195
sharing an agent depot 199
tacmd createNode command 200
Universal Agent 203
remote monitoring server
configuring failover support 225
remote monitoring server *(continued)*
configuring hot standby 225
configuring on Linux 128
configuring on UNIX 128
in hot standby environment 38
installing 123
installing on Linux 127
installing on UNIX 127
installing on Windows 124
planning worksheet, Linux or UNIX 413
planning worksheet, Windows 412
removing 443
agents 449
component 446
Linux 447
UNIX 447
Warehouse Proxy 449
Windows 446
event synchronization 450
from the portal 449
monitoring component 446
Linux 447
UNIX 447
Warehouse Proxy 449
Windows 446
monitoring environment 443
Linux 445
UNIX 445
Windows 443
OMEGAMON agents 447
reporting software 7
Reports, Crystal 7
required hardware
distributed systems 80
System z 82
required information for installation 59
required software 82
requirements
disk storage 81
memory 81
processor 80
resiliency 34
characteristics 35
options 34
resource groups, definition of 41
resource, definition of 41
reverse synchronization 10
ROWSINSERTED column 356
ROWSREAD column 357
ROWSRECEIVED column 356
ROWSSKIPPED column 357
rule base
creating new 375
importing existing rule base into 375
modifying 376

S

sample deployment scenarios 27
by size 27
event integration 52
high availability 34
large environment, multiple hub 32
large environment, single hub 30
medium environment 29
small environment 27
scale planning 13
scenarios
event integration 52
high availability 34
partition files 430
secureMain 442
upgrade 87
scripts
autostart 62
secondary hub monitoring server 37
SECRET, CA-TOP 69
Secure Hypertext Transport Protocol (HTTPS) 67, 68, 239
secure protocols
Internet Inter-ORB Protocol (IIOP) 67
Interoperable Object Reference (IOR) protocol 67
Secure Hypertext Transport Protocol (HTTPS) 67
Secure Socket Layer (SSL) 68, 239
secureMain utility 441
examples 442
scenarios 442
usage 441
securing a Linux or UNIX installation 441
securing communication between components 67
securing the SOAP server 70
security
configuring user authentication 211
firewall scenarios 249
HTTPS 239
Secure Hypertext Transport Protocol (HTTPS) 239
SSL 239
security considerations 18
security options
for communications 67
for SOAP Server 67
for user authentication 67
Security: Validate User option 68
seed data 159
seeding 159
seedkpp.log file 179
self-signed certificate 242
Sentry.baroc class file 362
Sentry.baroc file 376
Sentry2_0_Base class 61, 362
setting, KBB_RAS1 trace 351
shortcut for launching desktop client 193
silent installation 421
Linux 423
UNIX 423
Windows 421
from command line 422
using SMS 422
single-computer installation order 61
sit_ack_expired_def_action variable 403
sit_resurface_def_action variable 403
sitconfig.sh command 379
sitconfsvruser.sh command 380
sitconfuser command 403
Situation Event Console 7
situation events, forwarding 52

Situation Update Forwarder
process 362, 379
starting and stopping 405
situations
in a clustered environment 51
situpdate_conf_file variable 403
Small Local Zone 65
Small Local Zone with /opt directory
share 66
small monitoring environment
example 27
SOAP server 255
adding users 258
defining hubs 255
verifying configuration 260
SOAP Server
security options for 67
SOAP server, securing 70
software requirements 82
Software Support
contacting 461
describing problems 462
determining business impact 461
overview 459
receiving weekly updates 460
submitting problems 462
software, reporting 7
Solaris local zones
support for 11
Solaris zones
installing into 65
types of 65
SPIPE 68
SPIPE protocol 67
SQL files 159
SQL query 351
assigning to a workspace 353
creating 351
WAREHOUSELOG 353
SSl
See Secure Socket Layer (SSL)
SSL 239
asymmetric cryptography 239
CA certificate request, creating 241
CA certificate, receiving 242
digital certificates 239
enabling 240
Global Sign-On Kit (GSKit) 239
iKeyman 239
key database, creating 241
password, saving to stash file 243
public-private key pair 239
public-private key pair, creating 241
self-signed certificate, using 242
setting up asymmetric
encryption 240
stash file 243
standby hub monitoring server 37
STARTEXPORT column 356
starting
Situation Update Forwarder
process 405
starting Manage Tivoli Monitoring
Services
itmcmd manage command 208
on Linux 208
on UNIX 208
starting Manage Tivoli Monitoring
Services *(continued)*
on Windows 207
starting monitoring agents
itmcmd agent command 155
starting the monitoring server
itmcmd server command 122
starting the portal server 148
STARTQUEUE column 356
startSUF command 405
STARTTIME column 357
stash file 68, 243
status tables for warehouse
migration 103
stopping
Situation Update Forwarder
process 405
stopping the monitoring server
itmcmd server command 122
stopSUF command 405
Summarization and Pruning agent 7, 95
configuring communications for
DB2 297
configuring for hot standby 227
configuring JDBC connection 337
deployment in large monitoring
environments (multiple hubs) 33
deployment in large monitoring
environments (single hub) 32
deployment in medium monitoring
environments 30
deployment in small monitoring
environments 29
description of 270
flexible scheduling 11
in a clustered environment 50
in high availability scenarios 34
installing (DB2) 297
log trimming 11
product code 437
role in Tivoli Data Warehouse 7
starting 347
support assistant 459
supported databases
portal server 77
Tivoli Data Warehouse 77
supported operating systems 70
sysadmin user account 68, 69
System z
required hardware 82
systems, multiprocessor 80

T

tacmd addBundles command 198
tacmd createNode command 200
requirements 201
using 202
TCP/IP timeout setting, changing on
event server 380
TEC_Generic class 376
tec.baroc file 376
Technotes 457
TEMS name 181
Terminal Services 61
Tivoli Data Warehouse 7
backing up the database 95
Tivoli Data Warehouse *(continued)*
creating a Windows user 279
DB2 database, increasing 25
disk requirements, understanding 24
estimating database size 19
in a clustered environment 50
planning 19
supported databases 77
uninstalling the Warehouse
Proxy 449
upgrading 95
Windows user, creating 279
worksheet 22
Tivoli Data Warehouse database
backing up 95
Tivoli Distributed Monitoring, upgrading
from 87
Tivoli Enterprise Console
changing the TCP/IP timeout
setting 380
event forwarding 361
event integration 361
event synchronization 7
forwarding events to 378
information required for event
forwarding 60
integration 7, 52
planning 52
Tivoli Event Integration Facility 378
Tivoli Enterprise Console event view 7
Tivoli Enterprise Monitoring Agent
See monitoring agents
Tivoli Enterprise Monitoring Agents
configuring port number
assignments 230
Tivoli Enterprise Monitoring Server
See also monitoring server
configuring port number 228
Tivoli Enterprise Monitoring Server
certificate 70
Tivoli Enterprise Portal 5
authorizing users 68
browser client 6
desktop client 6
Tivoli Enterprise Portal client 6
planning considerations 26
Tivoli Enterprise Portal Server
See also portal server
configuring port number assignments
for client connections 228
Tivoli Event Integration Facility 378, 402
Tivoli Event Integration Facility (EIF) 55
Netcool/OMNIbus
configuring error event flow 402
configuring the EIF probe 400
updating the db schema 398
Tivoli Management Services 3
Tivoli System Automation
Multiplatform 41
topology view 90
trace setting, KBB_RAS1 351
Trusted Root certificate 69
type 437

U

uninstallation 443
  agents 449
  component 446
    Linux 447
    UNIX 447
    Warehouse Proxy 449
    Windows 446
  from the portal 449
  monitoring component 446
    Linux 447
    UNIX 447
    Warehouse Proxy 449
    Windows 446
  monitoring environment 443
    Linux 445
    UNIX 445
    Windows 443
  Warehouse Proxy 449
uninstalling
  event synchronization 450
  event synchronization component manually 451
  IBM Tivoli Monitoring environment 443
  ODBC data source 450
  OMEGAMON agents 447
  Warehouse Proxy agent 449
Universal Agent 6
  definition 6
Universal Agent, deploying 203
UNIX
  /etc/hosts file 64
  adding application support on monitoring server 122
  backing up a current installation 92
  configuring 425
  configuring monitoring agents 153
  EIB tables 439
  file descriptors limit 66
  file permissions for configuring monitoring agents 155
  fully qualified path names 64
  host names, setting 64
  hub monitoring server 119, 120
  installation considerations 62
  installation user account 64
  installing as root 64
  installing monitoring agents 152
  maxfiles 66
  monitoring agents 152
  monitoring server parameter 235
  network interface cards 64
  NFS environment 64
  planning 62
  remote monitoring server 127, 128
  response file configuration 425
  response file installation 423
  silent configuration 425
  silent installation 423
  Solaris zones
    installing into 65
  starting monitoring agents 155
  TCP/IP network services 64
UNIX monitoring server
  advanced configuration 235
UNIX monitoring server *(continued)*
  configuring permissions for non-NIS Solaris 235
  firewall support 433
  KDC_PARTITION 433
  NAT 433
  network address translation (NAT) 433
  non-NIS Solaris monitoring server 235
updating the Netcool/OMNIbus db schema 398
upgrade
  order 61
  Tivoli Distributed Monitoring 87
upgrade planning 88
upgrade scenarios 87
upgrading
  agents, configuration settings 99
  Candle Management Workstation coexistence 100
  CandleNet Portal database 100
  deciding which components 90
  from IBM Tivoli Monitoring V6.1 96
    overview 96
  from V350 and V360 98
  IBM Tivoli Monitoring V5.1.2 to V6.2 87
  IBM Tivoli Monitoring V6.1 to V6.2 87
  installation directory 99
  Java level, required 97, 100
  migrated information 91
  OMEGAMON Platform V350 and V360 87
  order 61
  required order 91
  terminology 99
  Tivoli Data Warehouse 95
  unsupported OMEGAMON functions 100
  Warehouse Proxy database 101
  when to run 99
upgrading the Tivoli Data Warehouse 95
upgrading to IBM Tivoli Monitoring 87
upgrading to V6.2
  required order 91
upgrading to version 6.2
  planning 88
user accounts 68
user authentication 211
  LDAP 69
  options for 67
user authority when installing on Linux or UNIX 64
user security
  configuring for a hub monitoring server on Linux or UNIX 215
  configuring for a hub monitoring server on Windows 212
user validation
  See user authentication
using Java Web Start to download the desktop client 191
utilities
  KinConfg.exe) 93

V

validation
  configuration values 11
  protocols 11
variables
  KDC_FAMILIES 429
  KDE_TRANSPORT 429
  KPX_WAREHOUSE_LOCATION 430
view
  topology 90
virtual memory
  increasing for large environments on AIX 235

W

warehouse migration tool 101
  configuring 101
  planning 101
  running 103
  status tables 103
Warehouse Proxy
  migrating OMEGAMON database 101
  removing 449
  tuning performance 354
  uninstalling 449
Warehouse Proxy agent 7, 95
  configuring 347
  deployment in large monitoring environments (multiple hubs) 33
  deployment in large monitoring environments (single hub) 32
  deployment in medium monitoring environments 30
  deployment in small monitoring environments 29
  in a clustered environment 51
  in high availability scenarios 34
  installing 347
  product code 437
  role in Tivoli Data Warehouse 7
  support for multiple 347
  uninstalling 449
  verifying configuration 350
Warehouse Summarization and Pruning agent
  See Summarization and Pruning agent
WAREHOUSEAGGRLOG table 357
WAREHOUSEID table 103
WAREHOUSELOG query 353
WAREHOUSELOG table 356
WAREHOUSELOG workspace 353
WAREHOUSEMIGLOG table 103
Web browser
  changing locations on UNIX or Linux 186
Web Health Console 87
Web Start
  launching from IBM Java Control Panel 192
  launching the desktop client from a browser 191
  launching the desktop client from the command line 192

Windows
backing up a current installation 93
hub monitoring server 115
installing the desktop client 156
monitoring agents 149
portal server 130
remote monitoring server 124
response file 421
silent installation 421
Windows Terminal Services 61
workflow policies
in a clustered environment 51
worksheets 409
communications protocol 420
desktop client on Linux 419
desktop client on Windows 418
Linux or UNIX hub monitoring server 411
Linux or UNIX remote monitoring server 413
Linux portal server 415
monitoring agent on Linux or UNIX 417
monitoring agent on Windows 416
monitoring server communications protocol 420
portal desktop client on Linux 419
portal desktop client on Windows 418
Windows hub monitoring server 410
Windows portal server 414
Windows remote monitoring server 412
workspace, WAREHOUSELOG 353
workspaces, creating 352
WPSYSNAME column 357
writetime column 103

Z

z/OS
authenticating users on 69



Printed in USA

GC32-9407-01

