Tivoli software

IBM

Certification Study Guide Series: IBM Tivoli Monitoring V6.2

- Helps you achieve IBM Tivoli Monitoring Version 6.2 certification
- Explains the certification path and prerequisites
- Introduces useful tips and best practices

Vasfi Gucer
John M Bubenheim
Raghunandan Hulgundi
Mei Yang-Matteson
Amina Shaheen

Redbooks

ibm.com/redbooks

International Technical Support Organization

Certification Study Guide Series: IBM Tivoli Monitoring V6.2

May 2008

SG24-7456-00

Note: Before using this information and the product it supports, read the information in "Notices" on page ix.

First Edition (May 2008)

This edition applies to IBM Tivoli Monitoring Version 6.2.0.

Contents

Notices ix
Trademarks x

Preface xi
The team that wrote this book xi
Become a published author xiii
Comments welcome xiii

Chapter 1. Certification overview 1
1.1 IBM Professional Certification Program 2
1.1.1 Benefits of certification 3
1.1.2 Tivoli Software Professional Certification 4
1.2 IBM Tivoli Monitoring V6.2 Implementation Certification 7
1.2.1 Test 908 objectives 8
1.3 Recommended resources for study 8
1.3.1 Courses 9
1.3.2 Publications 9

Chapter 2. Planning 11
2.1 IBM Tivoli Monitoring V6.2 components 12
2.1.1 Tivoli Enterprise Monitoring Server (monitoring server) 12
2.1.2 Tivoli Enterprise Portal Server (portal server) 13
2.1.3 Tivoli Enterprise Portal (portal or portal client) 13
2.1.4 Tivoli Enterprise Monitoring agent (monitoring agent) 14
2.1.5 Warehouse Proxy agent (WPA) 14
2.1.6 Warehouse Summarization and Pruning agent (S and P) 14
2.2 IBM Tivoli Open Process Automation Library (OPAL) 15
2.3 What is new in IBM Tivoli Monitoring V6.2 15
2.3.1 Optional IBM Tivoli Monitoring V6.2 components 17
2.4 IBM Tivoli Monitoring V6.2 deployment scenarios 19
2.4.1 A simple medium installation 19
2.4.2 A large installation 21
2.4.3 Determining server placement 23
2.4.4 High availability scenarios 23
2.5 Tivoli Data Warehouse 25
2.6 Communications protocol selection 27
2.7 Scalability 29
2.8 Planning an upgrade from a previous installation 30
2.8.1 Upgrading from Tivoli Distributed Monitoring 30

2.8.2 Planning an upgrade from OMEGAMON Platform V350 and V360 . 34
2.8.3 Planning a data migration from an existing Warehouse database . . 35
2.8.4 Planning the upgrade from IBM Tivoli Monitoring V6.1 36

Chapter 3. Prerequisites 39
3.1 Environmental assessment 40
3.2 Hardware requirements 42
3.2.1 Disk requirements 42
3.2.2 Processor requirements 43
3.2.3 Memory requirements 43
3.2.4 Additional requirements 44
3.3 Software requirements 45
3.3.1 Supported operating systems 45
3.3.2 IBM Global Security Tool Kit requirement 51
3.3.3 Supported databases for Tivoli Enterprise Portal Server and Tivoli Data Warehouse 52
3.3.4 Required software 53

Chapter 4. Installation 57
4.1 IBM Tivoli Monitoring V6.2 new installation 58
4.1.1 Preinstallation steps 58
4.1.2 Tivoli Enterprise Monitoring Server installation 62
4.1.3 Tivoli Enterprise Portal Server installation 64
4.1.4 Tivoli Enterprise Monitoring agent installation 66
4.1.5 Tivoli Enterprise Portal desktop client installation 68
4.1.6 Installing and enabling application support 69
4.1.7 Adding application support to the hub monitoring server 72
4.1.8 Populating the agent depot during installation 74
4.1.9 Manage Tivoli Monitoring Services 75
4.1.10 Configuring IBM Tivoli Monitoring Web Services (SOAP Server) . . 76
4.1.11 Tivoli Data Warehouse installation 79
4.1.12 Performing a silent installation on a Linux or UNIX computer 98
4.2 Upgrading from a previous OMEGAMON version 100
4.2.1 Upgrade procedure 100
4.2.2 Upgrade considerations 105
4.3 IBM Tivoli Monitoring V5.*x* upgrade 105
4.3.1 Product prerequisites 106
4.3.2 Installation procedure 106
4.3.3 Uninstalling the Migration Toolkit 112
4.3.4 Upgrading in phases and steps 112
4.4 Monitoring Agent for IBM Tivoli Monitoring V5.X Endpoint 115
4.4.1 Preinstallation steps 116
4.4.2 Using the Tivoli Enterprise Portal to view resource model data . . . 116

4.4.3 Reconfiguring data logging 116
4.4.4 Installing Monitoring Agent for Tivoli Monitoring V5.X Endpoint . . . 117
4.4.5 Configuring and distributing Monitoring Agent for IBM Tivoli Monitoring 5.X Endpoint 119
4.5 Integration with IBM Tivoli Enterprise Console 122
4.5.1 OMEGAMON IBM Tivoli Enterprise Console Event Adapter (OTEA) . . 123
4.5.2 Installing Tivoli Enterprise Console event synchronization 125
4.5.3 Installing monitoring agent .baroc files on the event server 128
4.5.4 Event severity 129
4.5.5 Starting and stopping the process that sends updates to a monitoring server 130
4.6 Uninstalling IBM Tivoli Monitoring V6.2. 131
4.6.1 Uninstalling the entire IBM Tivoli Monitoring environment 131
4.6.2 Uninstalling an individual IBM Tivoli Monitoring agent or component . . 133
4.6.3 Uninstalling the Warehouse Proxy 135
4.6.4 Uninstalling Tivoli Enterprise Console event synchronization. 136

Chapter 5. Configuration 141
5.1 IBM Tivoli Monitoring upgrade tools 142
5.1.1 The witmscantmr command 143
5.1.2 The witmassess command 145
5.1.3 The witmupgrade command 148
5.1.4 The witmmtk command. 151
5.2 Configuring IBM Tivoli Monitoring components. 154
5.2.1 Starting Manage Tivoli Enterprise Monitoring Services: Windows . 154
5.2.2 Starting Manage Tivoli Enterprise Monitoring Services for Linux and UNIX 155
5.2.3 Changing the configuration of Tivoli Enterprise Monitoring Server . 155
5.2.4 Specifying network interfaces 156
5.2.5 User options 156
5.2.6 Starting and stopping components 156
5.2.7 Configuring user authentication on the hub monitoring server 157
5.2.8 Creating a user on Tivoli Enterprise Portal 160
5.2.9 Configuring failover support 160
5.2.10 Adding application support to backup hub monitoring server 161
5.2.11 Configuring the Hot Standby feature on monitoring servers 161
5.2.12 Configuring agents 163
5.2.13 Verifying that failover support works 163
5.2.14 Using Manage Tivoli Enterprise Monitoring Services to add application support to a monitoring server 163

5.2.15 Using the itmcmd support command to add application support to a Linux or UNIX monitoring server . . . 164
5.3 IBM Tivoli Data Warehouse . . . 165
5.3.1 Configuring the Warehouse Proxy agent . . . 165
5.3.2 Configuring the Warehouse Summarization and Pruning Agent . . . 168
5.4 IBM Tivoli Universal Agent . . . 174
5.5 The tacmd command . . . 176
5.5.1 The tacmd login command . . . 177
5.5.2 The tacmd addBundles command . . . 177
5.5.3 The tacmd viewDepot command . . . 178
5.5.4 Return codes . . . 179
5.5.5 The tacmd editSit command . . . 180
5.5.6 Commands for UNIX only . . . 181
5.5.7 The itmcmd config command . . . 183
5.6 Agent Builder . . . 185
5.6.1 Product code for new agent . . . 186
5.6.2 Starting the Agent Builder . . . 186
5.6.3 Generating the Install Package . . . 186
5.7 IBM Tivoli Monitoring V5.X Endpoint features . . . 187
5.7.1 Configuring and distributing Monitoring Agent for IBM Tivoli Monitoring V5.X Endpoint . . . 187
5.7.2 The wep command . . . 189
5.8 Upgrading from IBM Tivoli Monitoring V6.1 . . . 190

Chapter 6. Troubleshooting and performance tuning . . . 193
6.1 Troubleshooting and tuning the historical database . . . 194
6.1.1 Tivoli Data Warehouse V2.1 overview and architecture . . . 194
6.1.2 Historical data architecture overview . . . 195
6.1.3 Configuring the historical database . . . 195
6.2 IBM Tivoli Monitoring V6.2 trace and log facilities . . . 199
6.2.1 Trace settings . . . 202
6.2.2 Integration Agent . . . 206
6.2.3 Universal Agent . . . 207
6.3 Tivoli Enterprise Portal Server troubleshooting . . . 207
6.3.1 Creating users . . . 208
6.3.2 Authentication . . . 209
6.3.3 Verifying that the user is defined in Tivoli Enterprise Portal Server database . . . 211
6.3.4 Tivoli Enterprise Portal Server logs . . . 212

6.4 Heartbeat 214
6.5 Situations 214
6.6 SOAP interface 219
6.7 Workspaces 230

Chapter 7. Administration 233
7.1 Situation editor 234
7.1.1 Understanding the terms 234
7.1.2 Creating a situation 235
7.1.3 Association 243
7.1.4 Predefined situations 243
7.2 Workspace 244
7.2.1 Workspace administration 244
7.2.2 Views 245
7.2.3 Graphic views 252
7.3 Manage Tivoli Enterprise Monitoring Services 256
7.4 Historical data collection 258
7.4.1 Historical data types 259
7.4.2 Data collection options 260
7.4.3 Starting the Summarization and Pruning Agent 261
7.5 Integration with other Tivoli event systems 266
7.5.1 IBM Tivoli Enterprise Console event viewer 266
7.5.2 IBM Tivoli Enterprise Console event integration 268
7.5.3 IBM Tivoli Netcool/OMNIbus event integration 269
7.5.4 Common Event Console view 269
7.6 IBM Tivoli Monitoring V6.2 command line 270
7.6.1 The tacmd command 270
7.6.2 The itmcmd command 276
7.6.3 The cinfo command (UNIX-only) 277
7.6.4 The kincinfo command (Windows-only) 279
7.6.5 The setperm command (UNIX-only) 279
7.6.6 Backup and restore commands 280

Appendix A. Sample Certification Test questions 285
Questions 286
Answers 295

Related publications 297
IBM Redbooks publications 297
Other publications 297
Online resources 298
How to get IBM Redbooks publications 298
Help from IBM 298

Index 299

Notices

This information was developed for products and services offered in the U.S.A.

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

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to:
IBM Director of Licensing, IBM Corporation, North Castle Drive, Armonk, NY 10504-1785 U.S.A.

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law: INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

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

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

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

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

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

COPYRIGHT LICENSE:

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

Trademarks

IBM, the IBM logo, and ibm.com are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both. If these and other IBM trademarked terms are marked on their first occurrence in this information with a trademark symbol (® or ™), these symbols indicate U.S. registered or common law trademarks owned by IBM at the time this information was published. Such trademarks may also be registered or common law trademarks in other countries. A current list of IBM trademarks is available on the Web at “Copyright and trademark information” at:
http://www.ibm.com/legal/copytrade.shtml

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

Redbooks (logo)  ®	iSeries®	S/390®
AIX 5L™	Netcool/OMNIbus™	System p™
AIX®	OMEGAMON Monitoring Agent®	System z™
Candle®	OMEGAMON®	Tivoli Enterprise Console®
CICS®	OS/390®	Tivoli®
DB2®	OS/400®	WebSphere®
HACMP™	pSeries®	z/OS®
i5/OS®	RACF®	zSeries®
IBM®	Redbooks®	

The following terms are trademarks of other companies:

Oracle, JD Edwards, PeopleSoft, Siebel, and TopLink are registered trademarks of Oracle Corporation and/or its affiliates.

Snapshot, and the NetApp logo are trademarks or registered trademarks of NetApp, Inc. in the U.S. and other countries.

ITIL is a registered trademark, and a registered community trademark of the Office of Government Commerce, and is registered in the U.S. Patent and Trademark Office.

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

Internet Explorer, Microsoft, SQL Server, Windows NT, Windows Server, Windows Vista, Windows, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

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

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

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

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

Preface

This IBM® Redbooks® publication is a study guide for IBM Tivoli® Monitoring Version 6.2 and is aimed at individuals who want to get an IBM Professional Certification for this product.

The IBM Tivoli Monitoring Version 6.2 Certification, offered through the Professional Certification Program from IBM, is designed to validate the skills required of technical professionals who work in the implementation of the IBM Tivoli Monitoring Version 6.2 product.

This book provides a combination of theory and practical experience needed for a general understanding of the subject matter. It also provides sample questions that will help in the evaluation of personal progress and provide familiarity with the types of questions that you will encounter in the exam.

This publication does not replace practical experience, nor is it designed to be a stand-alone guide for any subject. Instead, it is an effective tool that, when combined with educational activities and experience, can be an extremely useful preparation guide for the exam.

For your convenience, we structure the chapters based on the sections of the IBM Tivoli Monitoring V6.2 Implementation Certification test, such as Planning, Prerequisites, Installation, and so on, so studying each chapter will help you prepare for one section of the exam.

The team that wrote this book

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

Vasfi Gucer is a Project Leader at the International Technical Support Organization, Austin Center. He has been with the ITSO since January 1999. He has more than 10 years of experience in the areas of systems management, networking hardware, and software on mainframe and distributed platforms. He has worked on various Tivoli client projects as a systems architect in the U.S. He writes extensively and teaches IBM classes worldwide on Tivoli software. Vasfi is also a IBM Certified Senior IT Specialist.

John M Bubenheim is an IBM Certified Consulting IT Specialist with Americas System z™ Software. He joined IBM in 2000 as a member of the zBlue Software

Migration Project Office and currently leads a team that specializes in OMEGAMON® and IBM Tivoli Monitoring implementations. His background includes 28 years of experience in the IT industry specializing in Systems Programming, Performance and Capacity Management, Automation, and Storage Administration on mainframe and distributed platforms.

Raghunandan Hulgundi is an I/T Architect in Poughkeepsie, New York, supporting both IBM and commercial accounts for the past five years. His primary area of expertise is in providing solutions for distributed platforms for the IBM Tivoli suite. His skills include IBM Tivoli Monitoring V5.1.2, V6.1, IBM Tivoli Distributing Monitoring V3.7, and Tivoli Framework V4.1.1, actively developing best practices for monitoring solutions. He is also a Certified IT Specialist.

Mei Yang-Matteson currently works on the IBM Tivoli Monitoring Level 2 Support team and has been working with IBM Tivoli Monitoring 5.*x* and 6.*x* for two years. She first starting working with Tivoli in 1997 administering Tivoli Framework, Distributed Monitoring, Software Distribution, Inventory, and Remote Control for a Tivoli client. She then joined IBM Brazil in 1999 and continued providing support for Distributed Monitoring 3.7 and IBM Tivoli Monitoring 5.*x* for six years, before joining the IBM Tivoli Monitoring Level 2 team in the U.S.

Amina Shaheen is a Systems Management specialist working in IBM Global Services Division, Southbury, CT. She is an IBM Tivoli Monitoring V5.1.1 and 6.1, Information Technology Infrastructure Library (ITIL®), Lean, and IBM WebSphere® MQ 5.3 System Administrator Certified Professional. She has extensive experience in IBM Tivoli Monitoring for WebSphere Business Integration, including IBM WebSphere MQ, IBM WebSphere MQ Integrator, and IBM WebSphere MQ InterChange Server. She has been leading Tivoli projects for monitoring for IBM Global and other Tivoli commercial accounts. Her areas of expertise include IBM Tivoli Framework, IBM Tivoli Distributed Monitoring, IBM Tivoli Monitoring for Business Integration, IBM Tivoli Monitoring V5.1.2, IBM Tivoli Monitoring V6.1, and various monitoring agent packages.

Thanks to the authors of the previous editions of this book.

- Authors of the first edition, *Certification Study Guide Series: IBM Tivoli Monitoring V6.1*, published in February 2006, were:
  - Charles Beganskas
  - Ana Godoy
  - Dennis A. Perpetua
  - Amina Shaheen
  - Jason Shamroski
  - John Willis

Also, we would like to thank Bryant Bernstein from Senetas Corporation Ltd. for reviewing the book.

Become a published author

Join us for a two- to six-week residency program! Help write a book dealing with specific products or solutions, while getting hands-on experience with leading-edge technologies. You will have the opportunity to team with IBM technical professionals, Business Partners, and Clients.

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

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

ibm.com/redbooks/residencies.html

Comments welcome

Your comments are important to us!

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

- Use the online **Contact us** review IBM Redbooks publications form found at:

  ibm.com/redbooks

- Send your comments in an e-mail to:

  redbooks@us.ibm.com

- Mail your comments to:

  IBM Corporation, International Technical Support Organization
  Dept. HYTD Mail Station P099
  2455 South Road
  Poughkeepsie, NY 12601-5400

1

Certification overview

This chapter provides an overview of the skill requirements needed to obtain an IBM Advanced Technical Expert certification. We designed the following sections to provide a comprehensive review of specific topics that are essential for obtaining the certification:

- IBM Professional Certification Program
- IBM Tivoli Monitoring V6.2 Implementation Certification
- Recommended resources for study

1.1 IBM Professional Certification Program

Having the right skills for the job is critical in the growing global marketplace. IBM Professional Certification, designed to validate skill and proficiency in the latest IBM solution and product technology, can help provide that competitive edge. The IBM Professional Certification Program Web site is available at:

http://www.ibm.com/certify/index.shtml

The Professional Certification Program from IBM offers a business solution for skilled technical professionals seeking to demonstrate their expertise to the world.

The program is designed to validate your skills and demonstrate your proficiency in the latest IBM technology and solutions. In addition, professional certification can help you excel at your job by giving you and your employer confidence that your skills have been tested. You might be able to deliver higher levels of service and technical expertise than non-certified employees and move on a faster career track. Professional certification puts your career in your control.

The certification requirements are difficult, but it is not overwhelming either. It is a rigorous process that differentiates you from everyone else.

The mission of IBM Professional Certification is to:

- Provide a reliable, valid, and fair method of assessing skills and knowledge
- Provide IBM with a method of building and validating the skills of individuals and organizations
- Develop a loyal community of highly skilled certified professionals who recommend, sell, service, support, and use IBM products and solutions

The Professional Certification Program from IBM has developed certification role names to guide you in your professional development. The certification role names include IBM Certified Specialist, IBM Certified Solutions/Systems Expert, and IBM Certified Advanced Technical Expert for technical professionals who sell, service, and support IBM solutions. For technical professionals in application development, the certification roles include IBM Certified Developer Associate and IBM Certified Developer. An IBM Certified Instructor certifies the professional instructor.

The Professional Certification Program from IBM provides you with a structured program leading to an internationally recognized qualification. The program is designed for flexibility by allowing you to select your role, prepare for and take tests at your own pace, and, in some cases, select from a choice of elective tests best suited to your abilities and needs. Certain roles also offer a shortcut by giving credit for a certification obtained in other industry certification programs.

You can be a network administrator, systems integrator, network integrator, solution architect, solution developer, value-added reseller, technical coordinator, sales representative, or educational trainer. Regardless of your role, you can start charting your course through the Professional Certification Program from IBM today.

1.1.1 Benefits of certification

Certification is a tool to help objectively measure the performance of a professional on a given job at a defined skill level. Therefore, it is beneficial for individuals who want to validate their own skills and performance levels, their employees, or both. For optimum benefit, the certification tests must reflect the critical tasks required for a job, the skill levels of each task, and the frequency by which a task needs to be performed. IBM prides itself in designing comprehensive, documented processes that ensure that IBM certification tests remain relevant to the work environment of potential certification candidates.

In addition to assessing job skills and performance levels, professional certification can also provide benefits, such as:

- For employees:
  - Promotes recognition as an IBM certified professional
  - Helps to create advantages in interviews
  - Assists in salary increases, corporate advancement, or both
  - Increases self-esteem
  - Provides continuing professional benefits
- For employers:
  - Measures the effectiveness of training
  - Reduces course redundancy and unnecessary expenses
  - Provides objective benchmarks for validating skills
  - Makes long-range planning easier
  - Helps to manage professional development
  - Aids as a hiring tool
  - Contributes to competitive advantage
  - Increases productivity
  - Increases morale and loyalty
- For IBM Business Partners and consultants:
  - Provides independent validation of technical skills
  - Creates competitive advantage and business opportunities
  - Enhances prestige of the team
  - Contributes to IBM requirements for various IBM Business Partner programs

Specific benefits can vary by country (region) and role. In general, after you become certified, you might receive the following benefits:

- Industry recognition

  Certification might accelerate your career potential by validating your professional competency and increasing your ability to provide solid, capable technical support.

- Program credentials

  As a certified professional, you receive through e-mail your certificate of completion and the certification mark associated with your role for use in advertisements and business literature. You can also request a hardcopy certificate, which includes a wallet-size certificate.

  The Professional Certification Program from IBM acknowledges the individual as a technical professional. The certification mark is for the exclusive use of the certified individual.

- Ongoing technical vitality

  IBM Certified professionals are included in mailings from the Professional Certification Program from IBM.

1.1.2 Tivoli Software Professional Certification

The IBM Tivoli Professional Certification program offers certification testing that sets the standard for qualified product consultants, administrators, architects, and partners.

The program also offers an internationally recognized qualification for technical professionals seeking to apply their expertise in today's complex business environment. The program is designed for those who implement, buy, sell, service, and support IBM Tivoli solutions and want to deliver higher levels of service and technical expertise.

Whether you are a Tivoli client, partner, or technical professional wanting to put your career on the fast track, you can start on the road to becoming a Tivoli Certified Professional today.

Benefits of being Tivoli certified

Tivoli certification can provide the following benefits:

- For the individual:
  - IBM Certified certificate and use of logos on business cards

Note: Certificates are sent by e-mail. However, a paper copy of the certificate along with a laminated wallet card can also be requested by sending an e-mail to mailto:certify@us.ibm.com.

  - Recognition of your technical skills by your peers and management
  - Enhanced career opportunities
  - Focus for your professional development
- For the IBM Business Partner:
  - Confidence in the skills of your employees
  - Enhanced partnership benefits from the IBM Business Partner program
  - Billing your employees out at higher rates
  - Strengthens your proposals to clients
  - Demonstrates the depth of technical skills available to prospective clients
- For the client:
  - Confidence in the services professionals handling your implementation
  - Ease of hiring competent employees to manage your Tivoli environment
  - Enhanced return on investment (ROI) through more thorough integration with Tivoli and third-party products
  - Ease of selecting a Tivoli Business Partner who meets your specific needs

Certification checklist

Here is the certification checklist:

1. Select the certification that you want to pursue.
2. Determine which test or tests are required by reading the certification role description.
3. Prepare for the test, using the following resources provided:
   - Test objectives
   - Recommended educational resources
   - Sample assessment test
   - Other reference materials
   - Opportunities for experience

Note: These resources are available from each certification description page, as well as from the Test information page.

4. Register to take a test by contacting one of our worldwide testing vendors:
   - Thomson Prometric
   - Pearson Virtual University Enterprises (VUE)

   Note: When providing your name and address to the testing vendor, be sure to specify your name exactly as you want it to appear on your certificate.

5. Take the test. Be sure to keep the Examination Score Report provided upon test completion as your record of taking the test.

   Note: After taking a test, your test results and demographic data (including name, address, e-mail, and phone number) are sent from the testing vendor to IBM for processing (allow 2-3 days for transmittal and processing). After all the tests required for a certification are passed and received by IBM, your certificate will be issued.

6. Repeat steps three through five until all required tests are successfully completed for the desired certification role. If additional requirements are needed (such as an “other vendor” certification or exam), follow the instructions on the certification description page to submit these requirements to IBM.
7. After you complete your certification requirements, you will be sent an e-mail asking you to accept the terms of the IBM Certification Agreement before receiving the certificate.
8. Upon acceptance of the terms of the IBM Certification Agreement, an e-mail will be sent containing the following electronic deliverables:
   - A Certification Certificate in PDF format, which can be printed in either color or black and white
   - A set of graphic files of the IBM Professional Certification mark associated with the certification achieved
   - Guidelines for the use of the IBM Professional Certification mark
9. To avoid an unnecessary delay in receiving your certificate, ensure that we have your current e-mail on file by keeping your profile up-to-date. If you do not have an e-mail address on file, your certificate will be sent through postal mail.

After you receive a certificate by e-mail, you can also contact IBM at mailto:certify@us.ibm.com to request that a hardcopy certificate be sent by postal mail.

Note: IBM reserves the right to change or delete any portion of the program, including the terms and conditions of the IBM Certification Agreement, at any time without notice. Certain certification roles offered through the IBM Professional Certification Program require recertification.

1.2 IBM Tivoli Monitoring V6.2 Implementation Certification

We can categorize the certification process as:

- Job role description and target audience:

  A Tivoli Certified Consultant – IBM Tivoli Monitoring V6.2 is a technical professional responsible for planning, installation, configuration, operations, administration, and maintenance of an IBM Tivoli Monitoring V6.2 solution. This individual will be expected to perform these tasks with limited assistance from peers, product documentation, and support resources.

  To attain the IBM Certified Deployment Professional - IBM Tivoli Monitoring V6.2 certification, candidates must pass one test.

- Required prerequisites:
  - Strong working knowledge of IBM Tivoli Monitoring V6.2 infrastructure components
  - Working knowledge of operating system and networking and firewall concepts
  - Working knowledge of upgrading and migration paths available through IBM Tivoli Monitoring V6.2
  - Working knowledge of XML
  - Working knowledge of IBM Tivoli Universal Agent
  - Basic knowledge of IBM Tivoli Management Framework V4.1.1, IBM Tivoli Distributed Monitoring V3.7, IBM Tivoli Monitoring V5.1.X, IBM Tivoli Enterprise Console® V3.9, and IBM OMEGAMON XE and DE
  - Basic knowledge of security (Secure Sockets Layer (SSL), data encryption, IBM Global Security Toolkit, and system user accounts)
  - Basic knowledge of supported databases and Open Database Connectivity (ODBC)
  - Basic knowledge of the enterprise-wide monitoring capabilities of IBM Tivoli Monitoring V6.2
  - Basic knowledge of protocols, including HTTP and SOAP

- Core requirement:

  In order to be certified, you must select Test 908 - IBM Tivoli Monitoring V6.2:

  - Test 908 objectives
  - Test 908 sample test
  - Test 908 recommended educational resources
  - Approximate number of questions: 71
  - Duration in minutes: 120
  - Format: Multiple choice
  - Required passing score: 75% passing score or 53 correct answers

1.2.1 Test 908 objectives

For the most updated objectives of the IBM Tivoli Monitoring V6.2 Implementation Certification Test, refer to the following link:

http://www-03.ibm.com/certify/tests/obj908.shtml

1.3 Recommended resources for study

Courses and publications are offered to help you prepare for the certification tests. The courses are recommended, but not required, before taking a certification test. If you want to purchase Web-based training courses or are unable to locate a Web-based course or classroom course at the time and location that you desire, contact one of our delivery management teams at:

- Americas: mailto:tivamedu@us.ibm.com
- EMEA: mailto:tived@uk.ibm.com
- AP: mailto:tivtrainingap@au1.ibm.com

Note: Course offerings are continuously being added and updated. If you do not see the courses listed in your geography, contact the delivery management team.

1.3.1 Courses

Course names and course numbers vary depending on the education delivery arm used in each geography. Refer to the Tivoli software education Web site to find the appropriate course and education delivery vendor for each geography.

Refer to the following link for a listing of courses related to IBM Tivoli Monitoring V6.2:

http://www-03.ibm.com/certify/tests/edu908.shtml

1.3.2 Publications

Before taking test 908, IBM Tivoli Monitoring V6.2 Implementation, we recommend that you review IBM Tivoli Monitoring V6.2 guides and IBM Redbooks publications.

You might want to refer to the following guides:

- *Introducing IBM Tivoli Monitoring, Version 6.2.0,* GI11-4071
- *IBM Tivoli Monitoring User's Guide, Version 6.2.0*, SC32-9409
- *IBM Tivoli Monitoring Administrator's Guide, Version 6.2.0*, SC32-9408
- *IBM Tivoli Monitoring Installation and Setup Guide, Version 6.2.0*, GC32-9407
- *IBM Tivoli Monitoring Upgrading from Tivoli Distributed Monitoring, Version 6.2.0*, GC32-9462
- *Monitoring Agent for IBM Tivoli Monitoring 5.x Endpoint User's Guide*, SC32-9490

For the online publications of IBM Tivoli Monitoring V6.2, refer to the following link:

http://publib.boulder.ibm.com/infocenter/tivihelp/v15r1/index.jsp?topic=/com.ibm.itm.doc/welcome.htm

IBM Tivoli Monitoring V6.*x* IBM Redbooks publications

IBM Tivoli Monitoring IBM Redbooks publications include:

- *Getting Started with IBM Tivoli Monitoring Version 6.1 on Distributed Environments*, SG24-7143

  This book covers the planning, architecture, tuning, implementation, and troubleshooting of IBM Tivoli Monitoring V6.1. In addition, it provides scenarios about migration from Tivoli Distributed Monitoring V3.7 and IBM Tivoli Monitoring V5.*x* coexistence with IBM Tivoli Monitoring V6.1.

This book targets IT specialists who will be working on new IBM Tivoli Monitoring V6.1 installations or IBM Tivoli Monitoring V5.*x* coexistence or implementing a migration from Tivoli Distributed Monitoring V3.7.

- *Deployment Guide Series: IBM Tivoli Monitoring V6.2*, SG24-7444

  This book focuses on the planning and deployment of IBM Tivoli Monitoring Version 6.2 in small to medium and large environments. This book also covers the Agent Builder, including a 30 minute video that you can launch from the ITSO Web site.

  The target audience for this book is IT specialists who will be working on new IBM Tivoli Monitoring V6.2 installations.

- *IBM Tivoli Monitoring: Implementation and Performance Optimization for Large Scale Environments*, SG24-7443

  This IBM Redbooks publication provides a practical guide to implementing, using, and optimizing IBM Tivoli Monitoring, including best practices for performance tuning, sizing, high availability, scalability, reporting, IBM Change and Configuration Management Database integration, and firewall considerations.

  This book is a reference for IT professionals who implement and use the IBM Tivoli Monitoring solution in large scale environments.

2

Planning

The keys to a successful deployment of IBM Tivoli Monitoring V6.2 are proper architecture planning and requirements collection. This chapter summarizes the various core IBM Tivoli Monitoring V6.2 components and how each component relates to each other component. We examine several common architecture designs based on several factors: number of agents, hardware availability, and network restrictions.

In this chapter, we discuss the following topics:

- IBM Tivoli Monitoring V6.2 components
- IBM Tivoli Monitoring V6.2 deployment scenarios
- Scalability
- Hardware and software requirements
- Upgrade planning from previous versions

2.1 IBM Tivoli Monitoring V6.2 components

An IBM Tivoli Monitoring V6.2 installation consists of various components of the IBM Tivoli Monitoring V6.2 infrastructure. This environment is a combination of several vital components. Additionally, optional components can be installed to extend the monitoring functionality.

Figure 2-1 shows the IBM Tivoli Monitoring V6.2 components.

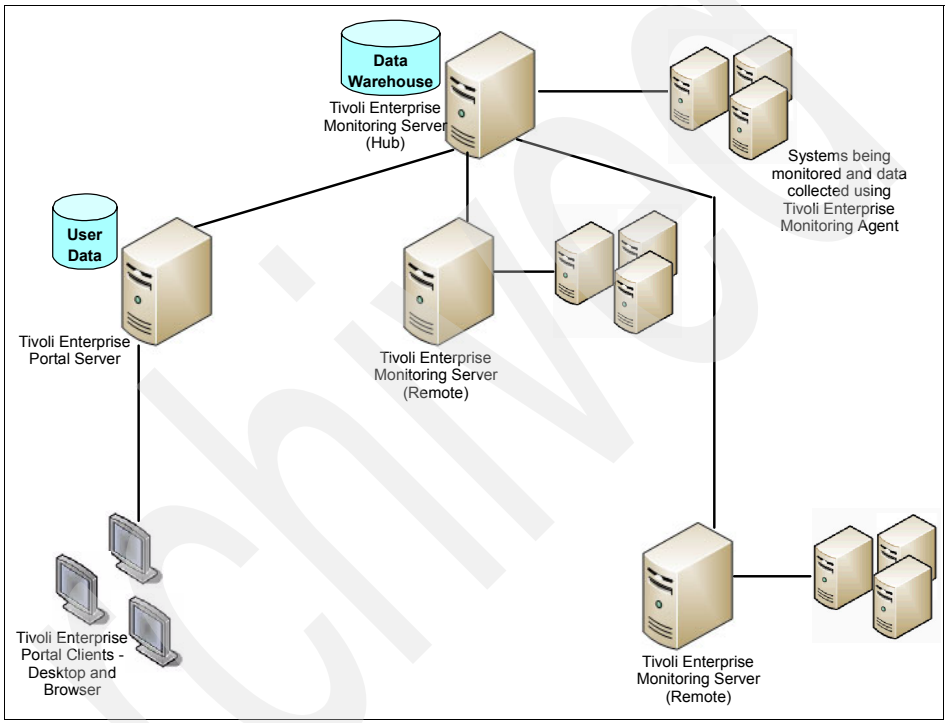


Figure 2-1 IBM Tivoli Monitoring V6.2 components

2.1.1 Tivoli Enterprise Monitoring Server (monitoring server)

The Tivoli Enterprise Monitoring Server (referred to as the *monitoring server*) is the key component on which all other architectural components directly depend. The monitoring server acts as a collection and control point for alerts received from agents and collects their performance and availability data.

The monitoring server is responsible for tracking the heartbeat request interval for all Tivoli Enterprise Monitoring agents connected to it. The monitoring server stores, initiates, and tracks all situations and policies, and it is the central

repository for storing all active conditions on every Tivoli Enterprise Monitoring agent. Additionally, it is responsible for initiating and tracking all generated actions that invoke a script or program on the Tivoli Enterprise Monitoring agent.

The monitoring server storage repository is a proprietary database format (referred to as the Enterprise Information Base (EIB)) that is grouped as a collection of files located on the Tivoli Enterprise Monitoring Server.

The primary monitoring server is configured as a hub (*LOCAL). All IBM Tivoli Monitoring V6.2 installations require at least one monitoring server configured as a hub.

Additional remote (*REMOTE) monitoring servers are introduced as a scalable hub-spoke configuration into the architecture. This hub/remote interconnection provides a hierarchical design that enables the remote monitoring server to control and collect its individual agent status and propagate the agent status up to the hub monitoring server. This mechanism enables the hub monitoring server to maintain infrastructure-wide visibility of the entire environment.

2.1.2 Tivoli Enterprise Portal Server (portal server)

The Tivoli Enterprise Portal Server (referred to as the *portal server*) is a repository for all graphical presentation of monitoring data. The portal server provides the core presentation layer, which allows for retrieval, manipulation, analysis, and reformatting of data. It manages this access through user workspace consoles.

2.1.3 Tivoli Enterprise Portal (portal or portal client)

The Tivoli Enterprise Portal client (referred to as the *portal* or *portal client*) is a Java™-based user interface that connects to the Tivoli Enterprise Portal Server to view all monitoring data collections. It is the user interaction component of the presentation layer. The portal brings all of these views together in a single window so that you can see when any component is not working as expected. The client offers two modes of operation: a Java desktop client and an HTTP browser.

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

IBM Tivoli Monitoring V6.2 uses a Java Web Start capability for administering the desktop client. Java Web Start allows the portal desktop client to be deployed over the network, ensuring that the most current version is used.

2.1.4 Tivoli Enterprise Monitoring agent (monitoring agent)

The Tivoli Enterprise Monitoring agent (also referred to as *monitoring agents* or *managed systems*) are installed on the system or subsystem requiring data collection and monitoring. The agents are responsible for gathering data and distributing attributes to the monitoring servers, including initiating the heartbeat status. These agents test attribute values against a threshold and report these results to the monitoring servers. The Tivoli Enterprise Portal displays an alert icon when a threshold is exceeded or a value is matched. The tests are called *situations*.

Tivoli Enterprise Monitoring agents are grouped into:

- Operating System (OS) Agents: Operating System Agents retrieve and collect all monitoring attribute groups related to specific operating system management conditions and associated data.
- Application Agents: Application Agents are specialized agents coded to retrieve and collect unique monitoring attribute groups related to one specific application. The monitoring groups are designed around an individual software application, and they provide in-depth visibility into the status and conditions of that particular application.
- Universal Agent: The Tivoli Universal Agent is a monitoring agent that you can configure to monitor any data that you collect. It enables you to integrate data from virtually any platform and any source, such as custom applications, databases, systems, and subsystems.

2.1.5 Warehouse Proxy agent (WPA)

The Warehouse Proxy agent is a unique agent that performs the task of receiving and consolidating all historical data collections from the individual agents to store in the Tivoli Data Warehouse. You can also install multiple Warehouse Proxy agents in your environment.

2.1.6 Warehouse Summarization and Pruning agent (S and P)

The Summarization and Pruning agent is a unique agent that performs the aggregation and pruning functions for the historical raw data on the Tivoli Data Warehouse. It has advanced configuration options that enable exceptional customization of the historical data storage. One S and P is recommended to manage the historical data in the Tivoli Data Warehouse. Due to the large amounts of data processing requirements, we recommend that you always install the S&P on the same physical system as the Tivoli Data Warehouse repository.

Note: To know the current supported platforms for above components, refer to the latest support matrix worksheet from the link below:

http://www-1.ibm.com/support/docview.wss?rs=203&uid=swg21067036

2.2 IBM Tivoli Open Process Automation Library (OPAL)

The IBM Tivoli Open Process Automation Library (OPAL) Web site is a catalog of solutions provided by IBM and IBM Business Partners that can be found at:

http://www.ibm.com/software/tivoli/opal

The Web site provides:

- A comprehensive online catalog of more than 300 validated product extensions
- A way for clients and IBM Business Partners to get more value from Tivoli products in a expedited way.
- Product Extensions that facilitate managing or protecting a specific application or type of application. Examples include:
  - Automation packages
  - Integration adapter and agents
  - Technical integration papers
  - Trap definitions
  - Plug-in toolkits or application registration files
- 70+ Universal Agent Solutions
- 209+ IBM Tivoli Availability and Business Service Management (ABSM) solutions

2.3 What is new in IBM Tivoli Monitoring V6.2

Figure 2-2 on page 16 gives an overview of what is new in IBM Tivoli Monitoring V6.2.

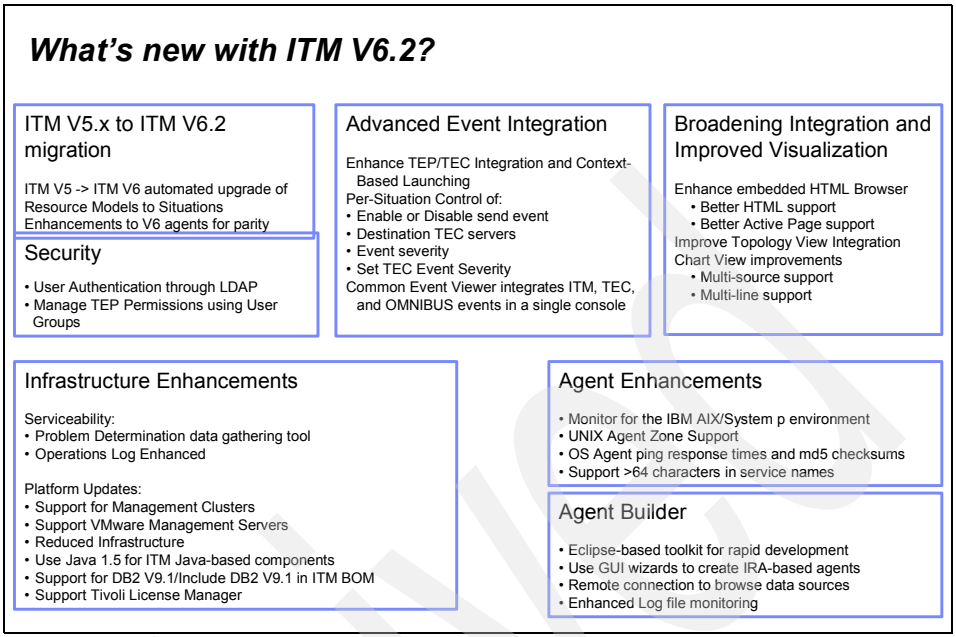


Figure 2-2 IBM Tivoli Monitoring V6.2 new features

IBM Tivoli Monitoring V6.2 incorporates news features in terms of functionality, serviceability, and quality.

Agent Builder

Agent Builder was introduced with IBM Tivoli Monitoring V6.1 Fix Pack 5 and has been enhanced in IBM Tivoli Monitoring V6.2.

Agent Builder is an Eclipse-based wizard that allows you to quickly and easily build a custom monitoring agent. It can use various datasources, such as Windows® Management Instrumentation (WMI), Windows Performance Monitor (Perfmon), Windows Event Log, Simple Network Management Protocol (SNMP), Script, Java Management Extensions (JMX™), and more. The OPAL Best Practice Library contains many downloadable samples of custom agents that were created by Agent Builder.

For more information about Agent Builder, you can refer to *Deployment Guide Series: IBM Tivoli Monitoring V6.2*, SG24-7444. You can also watch a video about Agent Builder at:

`ftp://www.redbooks.ibm.com/redbooks/SG247444/itm62.html`

Agent enhancements

This is a new monitor for the IBM AIX® and IBM System p™ environment. This is full performance management of AIX and System p with IBM Tivoli Monitoring V6.2.

IBM Tivoli Monitoring V6.2 provides visualization and performance management of the entire System p environment with historical data collection for improved troubleshooting, capacity planning, and service level reporting.

Other agent improvements include added capability for client configurable views, situations, and workflows, UNIX® Agent Zone Support, and support for more than 64 characters in service names.

New severities

In IBM Tivoli Monitoring V6.1, only three default event and threshold severities supported by situations and view-level thresholds were assignable: *Critical*, *Warning*, and *Informational*. In IBM Tivoli Monitoring V6.2, this default set is expanded to match Tivoli Enterprise Console: *Fatal*, *Critical*, *Minor*, *Warning*, *Harmless*, *Informational*, and *Unknown*.

2.3.1 Optional IBM Tivoli Monitoring V6.2 components

The following sections discuss optional IBM Tivoli Monitoring V6.2 components.

Monitoring Agent for IBM Tivoli Monitoring 5.x Endpoint

This integration agent enables the collection and visualization of IBM Tivoli Monitoring V5.*x* resource models in Tivoli Enterprise Portal. The visualization is the direct replacement for the Web Health Console. Additionally, the agent provides a rollup function into the Tivoli Data Warehouse.

When using Monitoring Agent for IBM Tivoli Monitoring 5.*x* Endpoint, the portal displays the data for the IBM Tivoli Monitoring V5.1.2 resource models, including their health, indication health, values from the indications, and status. This agent collects and displays the real-time raw data and historical data logged by the IBM Tivoli Monitoring V5.1.2 resource models.

The Monitoring Agent for IBM Tivoli Monitoring 5.*x* Endpoint provides data from IBM Tivoli Monitoring V5.1.2 resource models to IBM Tivoli Monitoring V6.2. This involves mapping the data from each resource model to the appropriate tables in IBM Tivoli Monitoring V6.2.

The Monitoring agent is installed on the Endpoints running IBM Tivoli Monitoring V5.1.2 with the IBM Tivoli Monitoring V5.1.2 Fix Pack 6 and the IBM Tivoli Monitoring Component Services Version 5.1.1 Fix Pack 2 or Version 5.1.3 with a minimum of 16 MB of disk space on Windows and 36 MB on Unix.

Tivoli Enterprise Console event synchronization

IBM Tivoli Monitoring V6.2 enhances the existing Tivoli Enterprise Console integration and allows context-based launching. It allows you to enable or disable send events, setting the destination IBM Tivoli Enterprise Console servers and event severity per situation.

Events can be forwarded to multiple Tivoli Enterprise Console servers. Because clients often have multiple Tivoli Enterprise Console servers in their environments, IBM Tivoli Monitoring V6.2 provides users with the ability to granularly select which events get forwarded to which Tivoli Enterprise Console servers.

This feature also provides multiple Tivoli Enterprise Console destination failover capability, where the user can create an alias that can be an ordered list of failover servers.

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 that you do not have to modify all of 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.

Event integration with Netcool/OMNIbus

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 back to the monitoring server that forwarded them.

Each event server to which events are forwarded must have an EIF probe associated with it and the event synchronization component installed on it. For each situation, the event server to which the situation event is forwarded needs to be specified. (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.

2.4 IBM Tivoli Monitoring V6.2 deployment scenarios

Deployment scenarios attempt to provide a realistic understanding of architectural design. Use these scenarios for guidance to assist in the planning and deployment strategy that you use for a production installation. It is important to recognize that every deployment strategy is unique, and only proper planning can guarantee a successful implementation.

2.4.1 A simple medium installation

The simple medium installation is the fundamental design using only the minimum required components. This scenario is perfect for prototyping IBM Tivoli Monitoring V6.2 or using it within a production installation consisting of up to 1500 agents maximum. In fact, IBM Tivoli Monitoring V6.2 by design excels in superiority for the small or medium installation. The predefined, ready to use monitoring collections, GUI presentation layer, historical data collection, and

robustness provide a full monitoring solution with a modest total cost of ownership (TCO).

It is implemented with the minimum hardware requirements necessary for a production IBM Tivoli Monitoring V6.2 installation.

The installation consists of the following components:

- Tivoli Enterprise Monitoring Server
- Tivoli Enterprise Portal Server
- Tivoli Enterprise Monitoring Server (Remote)
- Tivoli Warehouse Proxy agent
- Tivoli Data Warehouse
- Summarization and Pruning Agent

Figure 2-3 depicts the medium-sized topology. The diagram provides an overview of each IBM Tivoli Monitoring V6.2 connected component.

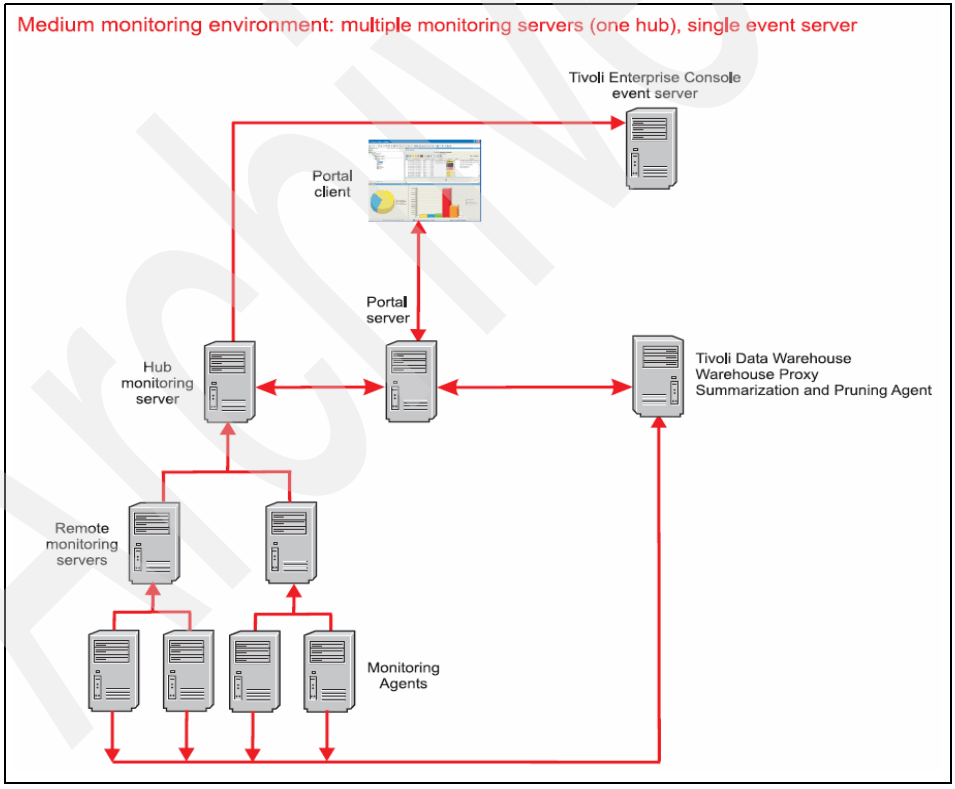


Figure 2-3 Medium installation scenario

2.4.2 A large installation

Figure 2-4 shows a larger monitoring environment for a multiple hub installation, which will be able to work with enterprise-wide historical data collection and event correlation.

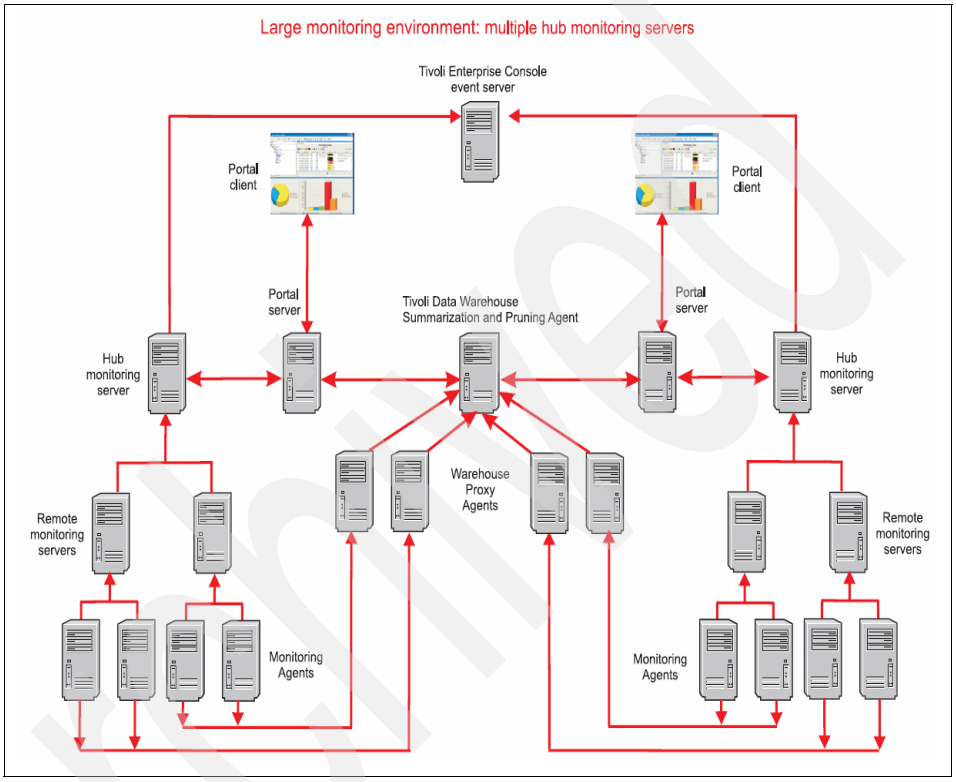


Figure 2-4 Large installation scenario

This implementation can support a large number of agents, because it has more than one hub. Even with more than one hub, you can still correlate events using Tivoli Enterprise Console Server, and you can have historical data collection using only one Tivoli Data Warehouse Server.

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.
- You can scale the Tivoli Data Warehouse server according to how much historical data you plan to collect and retain.

- When installing 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. We 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.
  - 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.

Table 2-1 shows the number and type of monitoring servers based on the number of monitoring agents and the complexity of the environment.

Table 2-1 Number and type of monitoring servers

Number and type of monitoring servers	**Number of agents (simple side of spectrum)**	**Number of agents (complex side of spectrum)**
Hub monitoring server with no remote monitoring servers	< 500 agents	< 250 agents
Hub monitoring server with 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

2.4.3 Determining server placement

Include the following considerations when determining the needs of the monitoring environment:

- Decide where (within the existing network topology or geographically) you want to accumulate data that is generated by the agents. This location is where you will install a monitoring server.
- Determine the amount of data that you expect to collect. Depending on the complexity of your environment, the number of agents that you install, and the amount of data that 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 location is where you install the portal server and portal client.
- Determine your need for a high availability operation in your environment. If you need a 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 that are 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.

2.4.4 High availability scenarios

There are two primary technological approaches to configure resiliency or high availability for the Tivoli monitoring platform components (see Figure 2-5 on page 24). 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 might be applicable for certain sites to make the hub monitoring server resilient to specific failure scenarios. This alternative approach is called *Hot Standby.*

For users who are 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 environmental 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.

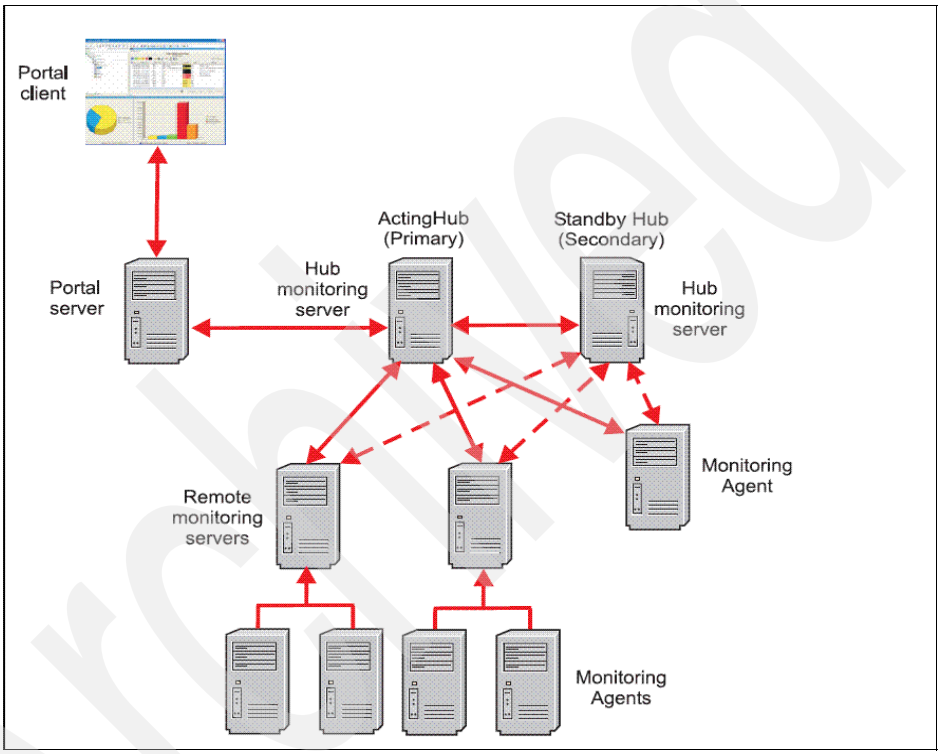


Figure 2-5 High availability scenarios with IBM Tivoli Monitoring

Table 2-2 on page 25 lists the options of Hot Standby.

Table 2-2 Hot Standby options

Component	Is there a potential single point of failure	Is cluster failover available	Is 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

You are permitted to use the hub Tivoli Enterprise Monitoring Server to handle agent tasks directly. However, we do not recommend using the hub Tivoli Enterprise Monitoring Server for this purpose. The hub Tivoli Enterprise Monitoring Server must focus on collecting data and processing tasks between the Tivoli Enterprise Portal Server and itself. If the environment expands, install additional remote Tivoli Enterprise Monitoring Servers to process the additional agent requirement. Additional agent deployments increase the processing requirements for the hub Tivoli Enterprise Monitoring Server, which can degrade if the hub is allowed to handle agent tasks directly.

Tip: Because IBM Tivoli Monitoring V6.2 supports primary and secondary communication paths, we highly recommend that you install several backup remote Tivoli Enterprise Monitoring Servers that exist solely for Tivoli Enterprise Monitoring agent failover capabilities. When a failure of a remote Tivoli Enterprise Monitoring Server occurs, we do not advise that you double the maximum load of a production remote Tivoli Enterprise Monitoring Server. Best practices direct these orphan Tivoli Enterprise Monitoring agents to the idle remote Tivoli Enterprise Monitoring Server.

2.5 Tivoli Data Warehouse

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.

The Tivoli Data Warehouse data requirement will be a substantial amount. We advise separating the Tivoli Warehouse Proxy agent and the Tivoli Data Warehouse repository between two systems. Install the Summarization and Pruning agent on the Tivoli Data Warehouse system. We always recommend that you keep these two components together.

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

The following features are new in V6.2:

- The use of variable length character columns is new. 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®, and VARCHAR or NVARCHAR in SQL Server®) rather than fixed length CHAR or NCHAR columns. This feature significantly reduces disk space requirements for tables and improves the performance and scalability of the warehouse.
- Most key columns in summary tables are 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, because these columns are indexed. Index disk space requirements are significantly reduced when using DB2.
- Improved indexing on summary tables is new. Indexes on summary tables now include all of the key columns needed for SNP processing. This change significantly improves SNP performance, because many tablespace scans have been eliminated.

In planning the size of the database, 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://catalog.lotus.com/wps/portal/topal`

The tool does all of the calculations for you and includes data for nearly all of the V6.*x*-based monitoring agents.

Important: As previous noted, for “Large installations”, make sure that only the required attributed groups are enabled for Tivoli Data Warehousing. Enormous amounts of data can be collected between two large IBM Tivoli Monitoring V6.2 installations. Best practice design is critical to ensure a stable, scalable environment.

The two installations are still built separately from each other. The only deviation is that one IBM Tivoli Monitoring V6.2 installation requires a logical association as the *master* control for the Summarization and Pruning Agent.

Restriction: There can only be one Summarization and Pruning Agent for a single Tivoli Data Warehouse. Because the Summarization and Pruning Agent requires connections to a Tivoli Enterprise Monitoring Server, one of the monitoring installations needs a logical designation as the master. This is not a programmatic assignment, but a logical identification for the configuration and management of the Summarization and Pruning Agent.

2.6 Communications protocol selection

If installing IBM Tivoli Monitoring V6.2 components across firewalls, we recommend that you configure the *IP.SPIPE* (TCP communication) protocol. The *IP* (UDP communication) protocol is insufficient for firewall configurations. The connectionless UDP protocol requires opening up multiple ports across firewalls to allow multiple connections from each IBM Tivoli Monitoring V6.2 component. For example, a Tivoli Enterprise Monitoring agent communicating to the Tivoli Enterprise Monitoring Server using IP (UDP communication) protocol requires multiple ports to operate properly. Secondly, using the IP.SPIPE (TCP communication) protocol will enable the *Ephemeral Pipe Support (EPS)* operation automatically if certain conditions match.

Table 2-3 on page 28 depicts the *default* listening ports for the IBM Tivoli Monitoring V6.2 components. Use this table as a quick reference to understand the standard ports for an installation. *Although modification is supported, we recommend that you do not modify these default values.*

Table 2-3 Default port usage for IBM Tivoli Monitoring V6.2

IBM Tivoli Monitoring V6.2 component	Listening port
Tivoli Enterprise Monitoring Server (*IP.PIPE*)	1918/TCP
Tivoli Enterprise Monitoring Server (*IP.SPIPE*)	3660/TCP
Tivoli Enterprise Monitoring Server (*IP*)	1918/UDP
Tivoli Enterprise Portal Server	1920/TCP 15001/TCP
Tivoli Enterprise Console	5529/TCP
Tivoli Warehouse Proxy agent	6014/TCP

Using IP.SPIPE allows a few well known ports to be open through the firewall. Use Table 2-3 to calculate which port to open. If the firewall is not using network address translation (NAT), the computation is sufficient to have the components connect through the firewall.

Every system that has IBM Tivoli Monitoring V6.2 installed will automatically reserve the well known port (default 1918) for Tivoli Enterprise Monitoring Server communication. It does not matter in which order components start on a system that has several IBM Tivoli Monitoring V6.2 components installed; the default well-known port is only used by Tivoli Enterprise Monitoring Server.

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

Use the KDC_FAMILIES options COUNT and SKIP with all IBM Tivoli Monitoring products running on the Warehouse Proxy agent computer. Only perform this step to guarantee the port on which Warehouse Proxy listens for firewall consideration. The Warehouse Proxy agent uses the KDC_FAMILIES COUNT option to obtain its listening port. All other non-monitoring server processes (agents or portal server) running on the computer with the Warehouse Proxy agent use the KDC_FAMILIES SKIP option to bypass reserved ports.

For all other components except for the Tivoli Enterprise Monitoring Server, the following calculation is used internally by IBM Tivoli Monitoring V6.2 to reserve the listening ports.

"reserved port" = *well-known* port + (*N**4096)

Where:

N= startup sequence

For example, the IBM Tivoli Monitoring V6.2 component startup on the system follows this sequence:

1. The Universal Agent starts first: port 6014 (1918 + 1*4096).
2. The remote Tivoli Enterprise Monitoring Server starts second: port 1918 (always reserved for Tivoli Enterprise Monitoring Server).
3. The Windows OS Agent starts third: port 10110 (1918 + 2*4096).
4. The Warehousing Proxy starts fourth: port 14206 (1918 + 3*4096).

2.7 Scalability

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

You must make this decision carefully, because different sources have their own reasons for providing sizing metrics.

For IBM Tivoli Monitoring V6.2, analysis of all these sources, including an in-depth knowledge of the monitoring environment, will assist in scaling the installation properly. Understanding the limitations of IBM Tivoli Monitoring V6.2 and strategically working through them will facilitate obtainable goals.

From a scalability standpoint, Tivoli Enterprise Monitoring Server plays the key role. As the architect of an IBM Tivoli Monitoring V6.2 implementation, you need to consider the following factors:

- Number of physical hosts and platform types included
- Number and type of applications and operating systems per host
- Geographical topology of the environment, particularly in relation to where the managed systems will reside
- Estimated number of events generated or thresholds that will be deployed, or both
- The degree of automation that is required or planned, both reflex and workflow

- Estimated number of Tivoli Enterprise Portal users and the expected type of usage (heavy reporting, frequent real-time updates, and so on)
- Network topology and firewall considerations

The information generated from these points can then be combined with the scalability guidelines that have been established for the initial release of IBM Tivoli Monitoring V6.2.

Table 2-4 classifies the extensive metrics for IBM Tivoli Monitoring V6.2. These metrics measure the apex for the IBM Tivoli Monitoring V6.2 components with respect to load quantity. All of these metrics represent one installation instance.

Table 2-4 Metrics for IBM Tivoli Monitoring V6.2

IBM Tivoli Monitoring V6.2 component	Verified metric
Remote Tivoli Enterprise Monitoring Servers per hub server	15 (Windows and UNIX)
Total number of managed systems per hub server	10000
Managed systems per remote Tivoli Enterprise Monitoring Server	1500
Consoles per Tivoli Enterprise Portal Server	50

Important: These metric values do not represent actual hard limits in IBM Tivoli Monitoring V6.2. These numbers are derived from what was actually tested, not necessarily a product limitation.

2.8 Planning an upgrade from a previous installation

In this section, we describe planning an upgrade from a previous installation of IBM Tivoli Monitoring.

2.8.1 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. This upgrade tool kit is installed on the Tivoli management region server and every managed node gateway with endpoints that you want to upgrade.

Tivoli Distributed Monitoring operates in a Tivoli Management Framework environment, which in large enterprises consists of a three-tiered architecture of

Tivoli servers and endpoints. IBM Tivoli Monitoring V6.*x* uses a different architecture, where components are organized in a similar hierarchical arrangement.

Comparing the infrastructures from an architectural point

To compare Tivoli Management Framework and Tivoli Monitoring Services:

- Tivoli Management Framework

  Tivoli Management Framework is the systems management framework that provides infrastructure services for many Tivoli products, such as IBM Tivoli Monitoring V5.1.2, Distributed Monitoring V3.7, and IBM Tivoli Enterprise Console.

- Tivoli Monitoring Services

  Tivoli Monitoring Services is the systems management framework that supports the IBM Tivoli Monitoring V6.*x* base product and the products that run on the base product.

  Tivoli Monitoring Services also collectively refers to the V6 product components: hub and remote Tivoli Enterprise Monitoring Servers and Tivoli Enterprise Monitoring agents.

While the implementation details are extremely different from the Tivoli Management Framework, Tivoli Monitoring Services provides similar kinds of infrastructure services.

Unlike the Tivoli Management Framework, Tivoli Monitoring Services does not need to be separately installed. It is part of the V6.*x* installation.

Figure 2-6 on page 32 shows a comparison of the infrastructural elements of the two architectures.

On the left side, you see an IBM Tivoli Monitoring V5.1.2 and Distributed monitoring V3.7 environment based on the Tivoli Management Framework architecture; on the right side, you see the IBM Tivoli Monitoring V6.2 environment that uses the Tivoli Monitoring Services architecture.

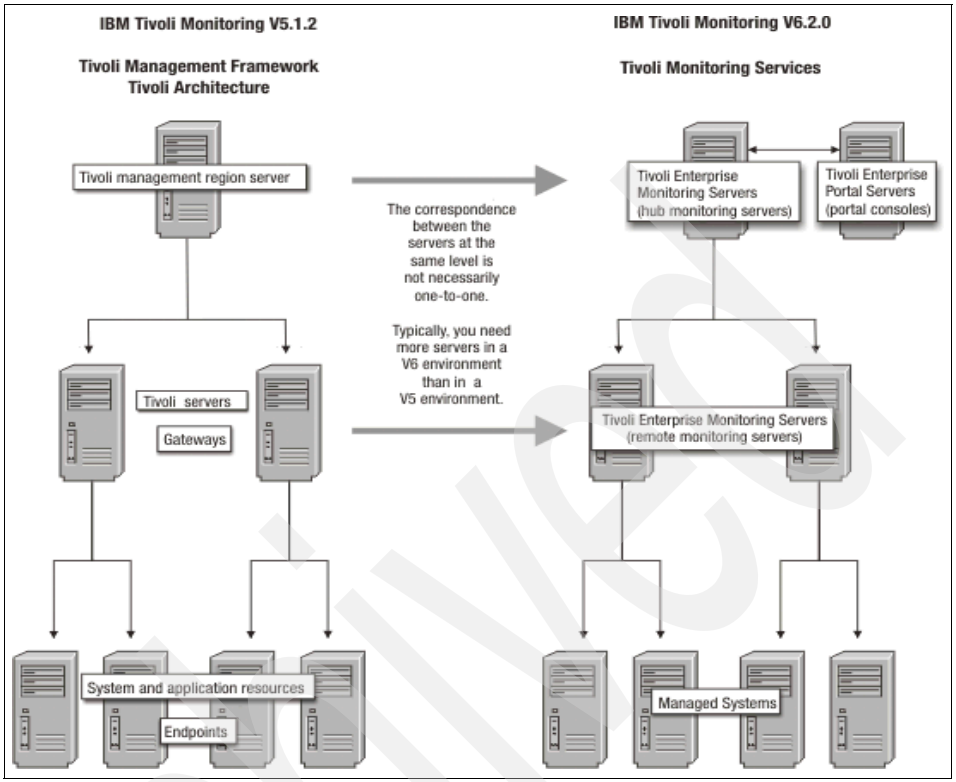


Figure 2-6 Comparison of architectures

Note: Although you can install the upgrade toolkit from either the Tivoli command line or the Tivoli desktop, you can only run the upgrade tools from the command line. There is no equivalent function in the Tivoli desktop.

Table 2-5 on page 33 lists the upgrade tools.

Table 2-5 Upgrade tools

Name of tool	Command	What the tool does
Set Java tool	**witmjavapath**	The *Set Java tool* specifies the location on the Tivoli server of the prerequisite Java software for the upgrade toolkit. The Scan, Assess, and Upgrade tools do not work until you set the Java path.
Scan tool	**witmscantmr**	The *Scan tool* collects information about the Tivoli infrastructure components (Tivoli server, gateways, and endpoints) where Tivoli Distributed Monitoring is installed or running. It uses this information to create an output data file that maps the Tivoli components to a proposed IBM Tivoli Monitoring infrastructure that is capable of handling the same monitoring load. You can use the output data file as a road map for deploying the IBM Tivoli Monitoring infrastructure. Beside creating an initial road map, the Scan tool also creates status reports that show the progress of the infrastructure upgrade.
Assess tool	**witmassess**	The *Assess tool* collects Tivoli Distributed Monitoring data from endpoints, profiles, or profile managers that you want to upgrade. It uses this information to create an output data file or files that map the collected data to the monitoring elements used by IBM Tivoli Monitoring. (For example, the output data file for a profile assessment specifies an equivalent situation for each monitor threshold.) The output data files from the Assess tool are used as input to the Upgrade tool.
Upgrade tool	**witmupgrade**	The *Upgrade tool* deploys the monitoring elements (monitoring agents, situations, or managed system lists) specified in the output file from the Assess tool. You can also use the Upgrade tool to undo (roll back) an upgrade and to disable (clean up) monitors that have been upgraded. All of the custom monitors are also upgraded for which the Universal Agents are installed on the managed system in IBM Tivoli Monitoring V6.2.

The information that needs to be gathered before the upgrade process is:

- The name of the Tivoli server
- The name of the policy region that contains the gateway and the endpoints that need to be migrated

To look up the names (labels) of the Tivoli server and policy region, use the command:

```
wlookup -r ManagedNode -a -L

wlookup -r PolicyRegion -a -L
```

- To see the name of the gateway, use the command **wlookup -ar Gateway**.

- The see the names of all of the endpoints assigned to the gateway, use the command **`wep ls`**.
- To list the names (labels) of all gateways and their assigned endpoints, enter **`wep ls -g <gateway_label>`**.
- You also need the fully qualified host name of the Tivoli server.

2.8.2 Planning an upgrade from OMEGAMON Platform V350 and V360

Here are the considerations for upgrading from OMEGAMON Platform V350 and V360.

Terminology changes

The following terms, which are listed in Table 2-6, have changed with the move from Candle® OMEGAMON to IBM Tivoli Monitoring V6.2.

Table 2-6 Terminology changes

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 Client Support	IBM Software Support

Upgrade considerations

The upgrade process from OMEGAMON Platform V350 or V360 to IBM Tivoli Monitoring V6.2 uses the existing installation directories. If the OMEGAMON Platform was prior to V350 or V360, it needs to be upgraded to V350 or V360 before upgrading to IBM Tivoli Monitoring V6.2. The upgrade process will also

install the required IBM Java Runtime Environment (JRE™) 1.5 for IBM Tivoli Monitoring V6.2.

After upgrading the infrastructure components to IBM Tivoli Monitoring V6.2, you need to install the application support files for the monitoring agents on the monitoring server, the portal server, and the portal desktop client.

When the OMEGAMON Platform V350 or V360 components are upgraded to IBM Tivoli Monitoring V6.2, the configuration settings are lost and all the components require reconfiguration. The upgraded OMEGAMON Platform V350 or V360 agents need to be reconfigured using Manage Candle Services to connect to the Monitoring servers. With OMEGAMON Platform V350 or V360 agents, you can only use protocols: SNA, IP.PIPE, or IP.UDP.

Candle Management Workstation coexistence

Candle Management Workstation in the OMEGAMON monitoring environment is left as it is in the upgrade process and continues to work as it was, although this not officially part of IBM Tivoli Monitoring and no new function has been added.

If Candle Management Workstation was not installed (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 ships 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.

2.8.3 Planning a data migration from an existing Warehouse database

To migrate the existing data in an OMEGAMON Platform V360 data warehouse to the IBM Tivoli Monitoring Tivoli Data Warehouse, use the migration tool provided with IBM Tivoli Monitoring.

The warehouse migration tool is installed during the installation of 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.

2.8.4 Planning the upgrade from IBM Tivoli Monitoring V6.1

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
- Red Hat Enterprise Linux® 3 x86 Warehouse Proxy agent and Summarization and running agent
- Red Hat Enterprise Linux 3 System z® Warehouse Proxy agent and Summarization and Pruning agent
- Solaris™ V8 - SPARC Tivoli Enterprise Monitoring Server and Summarization and Pruning agent
- Red Hat 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 System z Warehouse Proxy agent and Summarization and Pruning agent

Planning the sequence of the upgrade

Upgrade the products in the following order:

- Event synchronization: Upgrade the event synchronization component first if in use
- Warehouse database migration
- Hub Tivoli Enterprise Monitoring Server
- Remote monitoring server (if necessary)
- Tivoli Enterprise Management Agent Framework (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.)
- Tivoli Enterprise Portal Server
- Tivoli Enterprise Portal desktop client

Important: When upgrading from a previous release (into the same installation directory), the following information is migrated into the new version:

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

3

Prerequisites

It is vital to understand IBM Tivoli Monitoring V6.2 prerequisites to ensure that all infrastructure requirements are adequately met. This chapter introduces all of the prerequisite topics necessary to gain working knowledge of the hardware and software requirements.

This chapter covers the following topics:

- Environmental assessment
- Hardware requirements
- Software requirements

3.1 Environmental assessment

All distributed, heterogeneous environments, both existing or new, need to be properly assessed for all hardware and software requirements. A complete high-level understanding of the entire environment enables an accurate deployment of IBM Tivoli Monitoring V6.2 from a physical and organizational perspective. Fully review and document the environment that you plan to monitor. An optimal design can be created 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 varies 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 the available equipment and the 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 relationship between physical factors and IBM Tivoli Monitoring deployment is particularly close.

The organizational perspective includes expectations and limitations derived from the way that 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.

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 a network topology diagram is not already available for your organization. This network

design information is necessary for the design process and, at a minimum, needs to 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 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.
- Identify the number of resources to be monitored at remote locations.
- Determine the network reliability.
- Identify and document the host and IP address naming conventions and schemes that are 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:

- List the hardware configuration of the computers to be monitored. Include the vendor, memory available, CPU speed, and disk space available.
- Document the software configuration of the computers to be monitored. Include the operating systems, patch levels, and network configuration.
- Note the applications on each computer that need to be monitored. Include version levels and patch levels.
- Include the number of each type of computer (operating system) and application.
- Document the maximum failure detection interval needed for each computer and application (for configuring heartbeat intervals).
- Note the computers and applications that are mission critical.
- Create 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:

- Document organizational objective, business processes, IT processes, business needs, and future plans. This aspect has a great impact on the design process and you need to look at this area carefully from a physical perspective.

- Consider the amount of growth anticipated for the environment. The growth can be in terms of an increase in the number of monitored systems within the existing infrastructure or as a result of setting up new offices.
- Include internationalization considerations.
- Document primary risks to this project.
- List the number and responsibilities of existing system administrators.
- Note the major impediments to the IT service that your organization offers.
- Document the immediate problems that you are trying to solve with the deployment of IBM Tivoli Monitoring.
- List your immediate and long-term goals.

3.2 Hardware requirements

In this section, we discuss the hardware requirements for IBM Tivoli Monitoring V6.2.

3.2.1 Disk requirements

The minimum disk requirements for each IBM Tivoli Monitoring component vary depending on the size of the environment and the number of agents in the environment. Table 3-1 shows the memory requirements for IBM Tivoli Monitoring V6.2.

Table 3-1 Disk requirements

Component	Disk storage requirements
Hub monitoring server	650 MB
Remote monitoring server	600 MB
Portal server	800 MB
Portal client (browser or desktop)	150 MB

Component	Disk storage requirements
Tivoli Data Warehouse	Use Warehouse Load Projection tool on the IBM Tivoli Open Process Automation Library (OPAL) Web site: http://catalog.lotus.com/wps/portal/topal/details?catalog.label=1TW10TM1Y
Warehouse Proxy agent	150 MB
Summarization and Pruning agent	150 MB

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

3.2.2 Processor requirements

The requirements for the processor are:

- For best performance, we recommend processor speeds of at least:
  - 1 GHz for RISC architectures
  - 2 GHz for Intel® architectures
    Also, consider using multiprocessor systems if you are planning to use multiple components on the same system, for example.
  - Portal server and hub monitoring server
  - Monitoring server (hub or remote) and Warehouse Proxy agent
  - Warehouse Proxy and Summarization and Pruning agents

3.2.3 Memory requirements

Table 3-2 shows the memory requirements for IBM Tivoli Monitoring V6.2.

Table 3-2 Memory requirements

Component	Small environment	Large environment
Hub monitoring server	70 MB	400 MB
Remote monitoring server	100 MB	400 MB
Portal Server	100 MB	600 MB
Portal client (browser or desktop)	150 MB	300 MB
Tivoli Data Warehouse	2 - 4 GB depending on database configuration parameters	4 - 8 GB depending on database configuration parameters
Warehouse Proxy agent	100 MB	200 MB
Summarization and Pruning agent	100 MB	200 MB

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

3.2.4 Additional requirements

You need the best network connection possible between the hub monitoring server and the portal server and also between the Tivoli Data Warehouse, Warehouse Proxy agent, and Summarization and Pruning agent. The portal client requires a video card supporting 64000 colors and 1024 x 768 resolution.

Notes:

- The memory and disk sizings that are shown in Table 3-2 on page 44 are the amounts that are required for the individual component beyond the needs of the operating system and any concurrently running applications.
- 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.
- 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.
- 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.
- The memory requirement for the portal server does not include the database processes for the portal server database, which require up to 400 MB of additional memory, depending on the configuration settings.

3.3 Software requirements

In this section, we describe the supported operating systems and required software for IBM Tivoli Monitoring V6.2.

3.3.1 Supported operating systems

Table 3-3 on page 46 shows the operating systems that are supported for the various IBM Tivoli Monitoring V6.2 components: Monitoring Server, Portal Server, Portal Client, Tivoli Monitoring Agent (TMA), Warehouse Proxy agent (WPA), and Summarization and Pruning agent (SPA).

Note: This section does not show agent-specific requirements (such as supported application levels or any hardware requirements that are unique to a certain agent). For this information, see the specific *User's Guide* for the agent that you are installing.

Table 3-3 Supported Windows operating systems

Operating system	Monitoring server	Portal server	Portal client[a]	OS TMA[b]	WPA	SPA
Windows 2000 Server (32-bit)	X	X	X	X	X	X
Windows 2000 Advanced Server (32-bit)	X	X	X	X	X	X
Windows XP (32-bit)[c]			X	X	X	X
Windows 2003 Server SE (32-bit) with Service Pack 1 [d]	X	X	X	X	X	X
Windows 2003 Server EE (32-bit) with Service Pack 1[d]	X	X	X	X	X	X
Windows Server® 2003 Data Center (32-bit)				X		
Windows 2003 SE (64-bit)				X		
Windows 2003 EE (64-bit)				X		
Windows Server 2003 Data Center (64-bit)				X		
Windows 2003 Server on Itanium2				X		
Windows 2003 on VMware ESX Server V2.5.2 and V3.0	X	X	X	X	X	X
Windows Vista (32-bit)[c]			X			
Windows Vista (64-bit)[c]			X			

a. 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.

b. The OS Tivoli Monitoring Agent (OS TMA) 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.

c. 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.

d. For Windows 2003 Server: If you do not plan to deploy Service Pack 1 in your environment at this time, you must download and install Microsoft Installer 3.1 (KB893803), which is available from the Microsoft Download Web site (http://www.microsoft.com/downloads).

Note: If Tivoli Enterprise Monitoring Server is running on Linux, it will only support DB2 Universal Database (UDB) as the historical warehouse.

Table 3-4 Supported Linux operating systems

Operating system	Monitoring server	Portal server [a]	Portal client	OS TMA[b h]	WPA[c]	SPA
Asianux 2.0 for Intel (32-bit)	X	X	X	X	X	X
Red Flag 4.1 for Intel (32-bit)	X	X	X	X	X	X
Red Flag 5.1 for Intel	X	X	X	X	X	X
Red Hat Enterprise Linux 2.1 Intel (32-bit)				X		
Red Hat Enterprise Linux 3 on Intel (32-bit)				X		
Red Hat Enterprise Linux 3 on System z (31-bit)				(31,64N)		
Red Hat Enterprise Linux 3 on System z (64-bit)				X		
Red Hat Enterprise and Desktop Linux 4 Intel (32-bit)	X	X	X	X	X	X
Red Hat Enterprise Linux 4 on AMD64/EM64T (64-bit)	(32)			(64N)/ (64N)		
Red Hat Enterprise Linux 4 on Itanium® (64-bit)				(64N)/ (64N)		
Red Hat Enterprise Linux 4 on System i® and System p®				(32,64N) (64N)		
Red Hat Enterprise Linux 4 on System z (31-bit)	X	X		(31,64N)/ (31,64N)	X	X
Red Hat Enterprise Linux 4 on System z (64-bit)	X [d]	X [d f]		(31,64N)/ (31,64N)	X	X
Red Hat Enterprise Linux 4 for Intel on VMware ESX Server V2.5.2 and V3.0 (32-bit)	X	X	X	(31,64N)/ (31,64N)	X	X
Red Hat Enterprise and Desktop Linux 5 Intel (32-bit)	X	X	X	X	X	X

Operating system	Monitoring server	Portal server [a]	Portal client	OS TMA[b h]	WPA[c]	SPA
Red Hat Enterprise Linux 5 on AMD64/EM64T	(32)			X		
Red Hat Enterprise Linux 5 on Itanium 64-bit				X		
Red Hat Enterprise Linux 5 on System i and System p				(32,64N)/ (64N)		
Red Hat Enterprise Linux 5 on System z (31-bit)	X	X	X	X	X	X
Red Hat Enterprise Linux 5 on System z (64-bit)	X [e]	X [e g]		(31,64N)/ (31,64N)	X	X
SUSE Linux Enterprise Server 8 Intel (32-bit)				X		
SUSE Linux Enterprise Server 8 for System z (31-bit)				X		
SUSE Linux Enterprise Server 8 for System z (64-bit)				X		
SUSE Linux Enterprise Server 9 Intel (32-bit)	X	X	X	X	X	X
SUSE Linux Enterprise Server 9 on AMD64/EM64T (64-bit)				X		
SUSE Linux Enterprise Server 9 on Itanium (64-bit) [d]				X		
SUSE Linux Enterprise Server 9 for System i and System p				(32,64N)/ (64N)		
SUSE Linux Enterprise Server 9 for System z (31-bit)	X	X	X	X	X	X
SUSE Linux Enterprise Server 9 for System z (64-bit)	X [e]	X [e g]		(31,64N)/ (31,64N)	(31)	(31)
SUSE Linux Enterprise Server 10 Intel (32)	X	X	X	X	X	X
SUSE Linux Enterprise Server 10 on AMD64/EM64T (64-bit) [f]				X		
SUSE Linux Enterprise Server 10 on Itanium (64-bit) [d f]				X		

Operating system	Monitoring server	Portal server [a]	Portal client	OS TMA[b h]	WPA[c]	SPA
SUSE Linux Enterprise Server 10 for System i and System p (64-bit)				(32,64N)/ (64)		
SUSE Linux Enterprise Server 10 for System z (64-bit) [f]	X [e]	X [e g]		(31,64N)/ (31,64N)	(31)	(31)

a. 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.
b. 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.
c. An X11 GUI interface is required to configure the Warehouse Proxy agent.
d. This component supports the operating system in 64-bit tolerance mode.
e. See Technote 1247529 for minor known problems and workarounds for SUSE Linux Enterprise Server 10 on 64-bit operating systems.
f. We must install the Tivoli Enterprise Portal Server and its IBM DB2 UDB database in a 31-bit mode session. Each time that we start the Tivoli Enterprise Portal Server, we 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.
g. The Linux OS Monitoring Agent requires the installation of the latest versions of the following libraries: libstdc++ libgcc compat-libstdc++ libXp. These libraries are available on the Linux operating system installation media and Service Packs. Each library can have multiple packages, and each package must be installed.

Table 3-5 Supported Unix operating systems

Operating system	Monitoring server	Portal server	Portal client	OS monitoring agent[a]	Warehouse Proxy[b]	Warehouse Summarization and Pruning agent
AIXV5.2[c] (32 bit)	X			X		X
AIX V5.2 (64 bit)	(32 bit)			X		(32 bit)
AIX V5.3 (32 bit)	x	x		x	x	x
AIX V5.3 (64 bit)	(32 bit)	(32 bit)		X	X	(32 bit)
Solaris Operating Environment V8 (SPARC) (32/64 bit)[d]				X		
Solaris V9 (SPARC) (32/64bit)[e]	(32 bit)			X		(32 bit)

Operating system	Monitoring server	Portal server	Portal client	OS monitoring agent[a]	Warehouse Proxy[b]	Warehouse Summarization and Pruning agent
Solaris V10 (SPARC) (32/64 bit)	(32 bit)			X		(32 bit)
Solaris V10 (x86-64) (64 bit)	(32 bit)			X		
Solaris Zones	(32 bit)			X		(32 bit)
Hewlett-Packard UNIX (HP-UX) 11i v1 (B.11.11) (32/64) on PA-RISC[f]						
HP-UX 11i v2 (B.11.23) (64 bit) on PA-RISC						
HP-UX 11i v3 (B.11.31) (64 bit) on PA-RISC						
HP-UX 11i v2 (B.11.23) on Integrity (IA64)	X			X	X	X
HP-UX 11i v3(B.11.31) on Integrity (IA64)	X			X	X	X

a. 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. 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.

b. 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.

c. 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++ run time 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 Technology Level (TL) 5.
d. 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.
e. 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.
f. 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 the architecture is at least at PA-RISC2.

3.3.2 IBM Global Security Tool Kit requirement

IBM Tivoli Monitoring includes the IBM Global Security Tool Kit (GSKit) for Secure Sockets Layer (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.

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, which are stored in a key database file.

Table 3-6 lists the operating system patches that are required for GSKit, which is used to provide security between monitoring components. GSKit is installed automatically when you install Tivoli Management Services components.

Table 3-6 GSKit requirements

Operating system	Patch required
Solaris V8	108434-14, 111327-05, 108991, 108993-31, 108528-29, 113648-03, 116602-01, 111317-05, 111023-03, and 115827-01
Solaris V9	111711-08
Solaris V10	None
HP-UX V11i	PHSS_26946 and PHSS_33033

Operating system	Patch required
AIX V5.*x*	xlC.aix50.rte.6.0.0.3 or later
Windows Server 2003	None
Red Hat Enterprise Linux 2.1 Intel	pdksh-5.2.14-13.i386.rpm
Red Hat 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, and compat-libstdc++-33-3.2.3-46.1.i386.rpm
SUSE Linux Enterprise Server 8 Intel	None
SUSE Linux Enterprise Server 9 Intel	None

3.3.3 Supported databases for Tivoli Enterprise Portal Server and Tivoli Data Warehouse

The Tivoli Data Warehouse needs a relational database to store the historical data. DB2 UDB is the preferred database, but Microsoft SQL and Oracle are also supported. The product ships with a copy of DB2 UDB.

Before initiating the Warehouse Proxy agent installation and configuration, you need to create a Windows user with database administration rights (for example, the DB2ADMNS group).

Table 3-2 on page 44 shows the supported database for IBM Tivoli Monitoring V6.2.

Table 3-7 Supported databases

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

Portal server operating system	Portal server database ("TEPS")[a]	
LINUX[c]	V8.1 with Fix Pack 10 or higher fix packs, V8.2 with Fix Pack 3 or higher fix packs, or V9.1 and fix packs	
Windows	V8.1 with Fix Pack 10 or higher fix packs, V8.2 with Fix Pack 3 or higher fix packs, or V9.1 and fix packs	MS SQL 2000 SP3[d]

a. "TEPS" is the default database name for the database used by the portal server.
b. Requires an installation workaround that is described in APAR IY95415. If you are using 64-bit DB2 9.1 on System z 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.
c. On Linux, the portal server database must be installed with the operating system language set to UTF-8.
d. 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.

3.3.4 Required software

Table 3-8 shows the required software for IBM Tivoli Monitoring V6.2.

Table 3-8 Required software for IBM Tivoli Monitoring V6.2

Product	Supported version	Monitoring Server	Portal server	Portal desktop client	Portal browser client
IBM Runtime Environment for Java	JRE V1.4.2 or later	X	X	X	X
For Linux computers: A Korn shell interpreter	pdksh-5.2.14	X	X	X	
AIX 5L™ only: xlC Runtime Environment		X			

Product	Supported version	Monitoring Server	Portal server	Portal desktop client	Portal browser client
Microsoft Internet Explorer	V6.0 with all critical Microsoft updates applied	X			
Database:[a] ► DB2 UDB V8 ► Microsoft SQL Server 2000 ► Oracle V9.2 or V10.1 (for warehousing only, not for Tivoli Enterprise Portal Server)	Fix Pack 10 for DB2 UDB V8		X		
IBM Tivoli Enterprise Console	Version 3.9 with Fix Pack 03				
For TCP/IP communication: ► Windows 2000 Professional or Server with Service Pack 3 or later ► Microsoft Winsock V1.1 or later ► Microsoft TCP/IP protocol stack		X	X	X	X

Product	Supported version	Monitoring Server	Portal server	Portal desktop client	Portal browser client
For SNA communication: ► Windows 2000 Professional or Server with Service Pack 3 or later ► Microsoft SNA Server V3.0 or later ► IBM Communications Server V5.0 or V5.2	► Microsoft SNA Server V4.0 requires Service Pack 1 ► IBM Communications Server V5.0 requires fixes JR10466 and JR103368	X			

a. The only supported database for a Linux portal server is DB2.
Each database requires a driver: JDBC™-DB2 for DB2, MS SQL JDBC for MS SQL, and Oracle JDBC for Oracle.

4

Installation

In this chapter, we discuss the steps that are necessary to perform a new installation of IBM Tivoli Monitoring V6.2, to upgrade from IBM Tivoli Monitoring V5.*x*, and to upgrade from OMEGAMON.

This chapter describes the following topics:

- IBM Tivoli Monitoring V6.2 new installation
- Upgrading from a previous OMEGAMON version
- IBM Tivoli Monitoring V5.x upgrade
- Monitoring Agent for IBM Tivoli Monitoring V5.X Endpoint
- Integration with IBM Tivoli Enterprise Console
- Uninstalling IBM Tivoli Monitoring V6.2

4.1 IBM Tivoli Monitoring V6.2 new installation

For the detailed installation steps for IBM Tivoli Monitoring V6.2, refer to *IBM Tivoli Monitoring Installation and Setup Guide, Version 6.2.0*, GC32-9407, and the *Deployment Guide Series: IBM Tivoli Monitoring 6.2*, SG24-7444. In this chapter, we summarize the IBM Tivoli Monitoring V6.2 preinstallation and installation procedures, focusing only on key installation and customization steps and parameters.

You must install the following components (or they must already be installed) before you implement IBM Tivoli Monitoring V6.2:

- Tivoli Enterprise Monitoring Server
- Tivoli Enterprise Portal Server
- Tivoli Enterprise Monitoring agents
- Tivoli Enterprise Portal desktop client
- Tivoli Data Warehouse (Summarization and Pruning Agent and Warehouse Proxy)

The following sections contain both Microsoft Windows and UNIX procedures for installing the various components. Use the procedure that applies to your environment.

Note: The installation procedures in the following sections provide information for installing a single component (such as the monitoring server) on one computer. But, you can also install multiple components (such as the monitoring server and the portal server) on the same computer simultaneously. You just need to select the components during the installation process.

4.1.1 Preinstallation steps

In this section, we describe details that you must be aware of before starting the installation.

Specific information to have ready

During the installation, you need to supply the following information:

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

- Hub monitoring server host name
- Port number

Naming your monitoring server

You must first decide how to name your monitoring servers. In general, use 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. You cannot use blanks or special characters (.$#@) for the initial character of the name.
- Each name must be between two and 32 characters in length.
- Monitoring server naming is case-sensitive on all platforms.

Required order of installation

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

- Hub Tivoli Enterprise Monitoring Server
- Remote monitoring server (if necessary)
- Tivoli Enterprise Monitoring 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 consideration: 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.

Linux or UNIX installation considerations

The following sections provide information about issues that are unique to Linux and UNIX installations.

IBM Tivoli account

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

- You can use any valid name. If you do not install IBM Tivoli Monitoring V6.2 as root, you must use the following procedure to create the user and correctly set the permission. As example, let us create a user called `itmuser` in the `itmusers` group:

  a. Create the itmusers group using the following procedures:

     For Linux, Solaris, and Hewlett-Packard UNIX (HP-UX) computers, run the following command:

     ```
     groupadd itmusers
     ```

     For an AIX 5L computer, run the following command:

     ```
     mkgroup itmusers
     ```

  b. Create the itmuser user belonging to itmusers group; itmusers will be the primary itmuser group.

     For AIX 5L, Solaris, HP-UX, and Linux computers, run the following command to create the itmuser account:

     ```
     useradd -g itmusers -s /usr/bin/ksh itmuser
     ```

- Use the same user to install all of the components.
- If you are using Network File System (NFS) or a local file system, establish your installation directory according to the guidelines that are used in your environment.

  Notes: This guideline 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.

- After properly creating the user, use the following procedure to set the permissions:

  a. Set the CANDLEHOME directory. Set it in the itmuser user profile.

     ```
     export CANDLEHOME=/opt/IBM/ITM
     ```

  b. Run the following command to ensure that the CANDLEHOME environment variable correctly identifies the IBM Tivoli Monitoring installation directory:

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

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

```
cd $CANDLEHOME
```

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

```
pwd
```

e. Run the following commands:

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

Import the images

Import the IBM Tivoli Monitoring V6.2 images to the server where you will perform the installation.

Host name for TCP/IP network services

Configure the TCP/IP network services, such as Network Information Service (NIS), Domain Name System (DNS), and the /etc/hosts file, 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 file.

Use of fully qualified path names

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

File descriptor (maxfiles) limit

The monitoring server requires a minimum of 256 file descriptors (*maxfiles*) for the operating system.

4.1.2 Tivoli Enterprise Monitoring Server installation

This section provides details about the hub monitoring server and remote monitoring server installation.

Hub monitoring server

Here, we describe the major tasks that are performed during the installation.

Windows

In Microsoft Windows, the tasks include:

1. To launch the installation wizard, run **`setup.exe`** in the \WINDOWS directory in the IBM Tivoli Monitoring V6.2 media. The default installation directory is C:\IBM\ITM.
2. The installation program asks about the encryption key. Type 32 characters for the encryption key or use the default key.

Notes:

- This encryption key is used to establish a secure connection (using Secure Sockets Layer (SSL) protocol) between the hub Tivoli Enterprise Monitoring Server and the other components of the Tivoli Monitoring V6.2 environment, for example, when the remote Tivoli Enterprise Monitoring Server is connected to the hub. Note that the same key must be used on all Tivoli Management Services components in your enterprise. For example, the encryption key that you set for the Tivoli Enterprise Portal must be the same value that you specify for the encryption key for the hub monitoring server, and the key that you set for each of the remote monitoring servers that connect to the hub must also have the same value. If you reset the key for one component, you must reset the key for all of them. Do not use any of the following characters in your key: = ' |
- Ensure that you document the value that you use for the key. Use this key during the installation of any components that communicate with this monitoring server.

3. In addition, you need to select the components that you want to install. Select Tivoli Enterprise Monitoring Server.

Note: If you want to use the Summarization and Pruning Agent to work with data in Data Warehouse, expand **Tivoli Enterprise Monitoring Agent** and select **Windows Summarization and Pruning Agent**. Refer to the *IBM Tivoli Monitoring Administrator's Guide, Version 6.2.0*, SC32-9408, for information about configuring and using this agent.

4. If you want to remotely deploy agent software, select those agents that you want to deploy. This step creates and populates the deployment depot, from which you can deploy agents at a later time.

   Notes:

   - By default, the depot is located in the <*itm_installdir*>/CMS/depot directory on Windows and the <*itm_installdir*>/tables/<*ms_name*>/depot directory on Linux and UNIX. If you want to use a different directory, change the DEPOTHOME value in the kbb.env file.
   - You can also populate the agent depot by using the **`tacmd addBundles`** command.

5. After the components are installed, a configuration window (the Setup Type window) opens, where you select what you want to configure. Perform the following major tasks in this window:
   - Select the type of monitoring server that you are configuring: Hub or Remote. For this procedure, select **Hub**. Verify that the name of this monitoring server is correct in the Tivoli Enterprise Monitoring Server (TEMS) field. The default name is hub_*hostname*.
   - 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, which enables you to set up backup communication methods.

     Note: IP.PIPE protocol uses TCP; thus, a permanent connection is established between the Tivoli Enterprise Monitoring Server and the remote servers. This permanent connection might have an impact on the server performance because of the number of remote procedure calls (RPCs) that it needs to handle. If using User Datagram Protocol (UDP) will not cause security breaches in your environment, we recommend that you set up the first protocol as IP.UDP; otherwise, use IP.PIPE. Note that if you have a firewall between your Tivoli Enterprise Monitoring Server and your agents, you *cannot* use IP.UDP.

– Select whether or not you want Tivoli Monitoring V6.2 to forward events to IBM Tivoli Enterprise Console using the Tivoli Enterprise Console Event Integration Facility.

– Specify the monitoring server location and what data to add to the application support.

– Specify the default communication between any IBM Tivoli Monitoring component and the hub monitoring server.

Linux or UNIX

In Linux or UNIX, the tasks include:

1. To launch the installation wizard, run **./install.sh** in the directory from where the installation files were extracted. The default installation directory is /opt/IBM/ITM.
2. Unlike the Windows installation, the Linux or UNIX installation does not have a graphical user interface (GUI); instead, you are prompted with text menus.
3. As in the Windows installation, you need to enter the encryption key. Use the same instructions that you use for the Windows installation.
4. Select the operating system and components to be installed.

   The name convention for Linux or UNIX is the same, HUB_*hostname.*

Notes:

- When the Tivoli Enterprise Monitoring Server installation service finishes, the installation program will *not* ask whether you want to configure or not. In order to configure, you need to run the **./itmcmd config -S -t tems_name** command from /opt/IBM/ITM/bin.
- In addition, you need to add application support for the monitoring server by running the **./itmcmd support -t tems_name *pc pc pc*** (*pc* is the product code) command. Application support includes the workspaces and situations for agents. For more information, refer to 4.1.6, “Installing and enabling application support” on page 69.

Remote monitoring servers

The steps to install the remote monitoring servers are similar to the hub monitoring server installation. You need to select the monitoring server type as Remote Server. The default name is REMOTE_*hostname*.

4.1.3 Tivoli Enterprise Portal Server installation

This section describes installation considerations for Tivoli Enterprise Portal Server.

Installation

You can install Tivoli Enterprise Portal Server on either a Windows computer or a Linux computer. Note the following considerations about the installation.

Windows

On Windows, the tasks include:

1. To launch the installation wizard, run **`setup.exe`** in the \WINDOWS directory in the IBM Tivoli Monitoring V6.2 media. The default installation directory is C:\IBM\ITM.
2. You need to enter an encryption key to use. Use the same key that you used during the installation of the monitoring server to which this portal server will connect.
3. Select **Tivoli Enterprise Portal Server** from the list of components to install.
4. If you are installing the portal server on a computer that already has a monitoring server installed, you need to populate the depot.

After the installation completes, the installation program prompts you to configure the portal server and the connection to the monitoring server. In order to perform this configuration, you need to know the following information:

- The host name where you are installing the portal server
- The portal server's connection details to the datasource

> **Note:** The datasource is used for historical data reporting. We provide details about this configuration in 4.1.11, "Tivoli Data Warehouse installation" on page 79.

Linux or UNIX

The tasks to install Tivoli Enterprise Portal Server on Linux or UNIX include:

1. To launch the installation wizard, run **`./install.sh`** in the directory from where the installation files were extracted. The default installation directory is /opt/IBM/ITM. The installation runs in text mode.
2. You need to enter an encryption key to use. Use the same key that you used during the installation of the monitoring server to which this portal server will connect.
3. Select the operating system and components to install.

> **Note:** After installation, you need to configure Tivoli Enterprise Portal Server. Change the directory to /opt/IBM/ITM/bin and run **`./itmcmd config -A cq`**.

4. If you have multiple network interface controllers (NICs) on the portal server or a firewall between the portal client and the portal server, you need to configure portal server interfaces.

To configure the portal server interfaces on Windows:

1. Launch the Manage Tivoli Enterprise Monitoring Services (MTEMS) GUI.
2. Go to **Actions** → **Advanced** → **Configure TEPS interfaces** (see Figure 4-1).

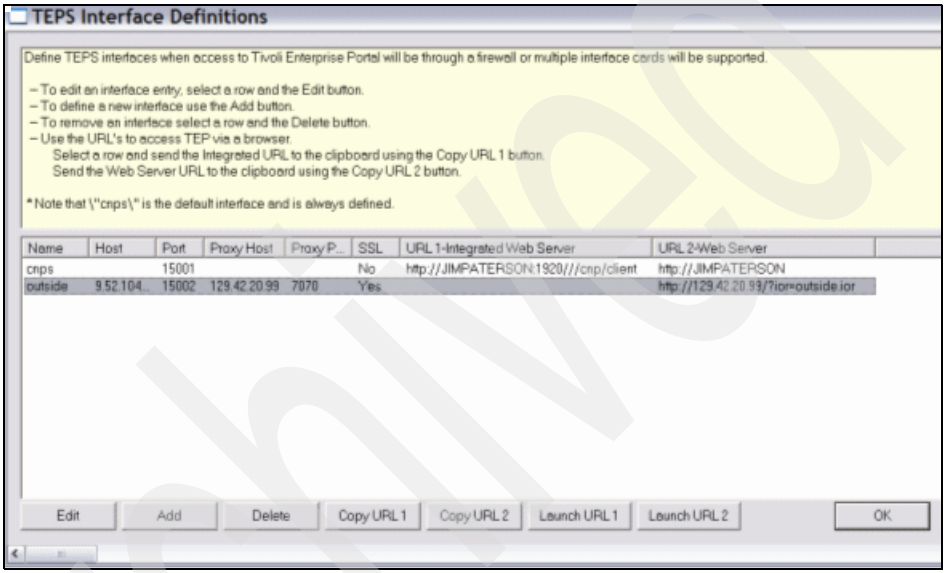


Figure 4-1 TEPS Interface Definitions

To configure the portal server interfaces on UNIX or Linux, you must configure portal server interfaces via the environment variables in <*installDir*>/config/cq.ini.

4.1.4 Tivoli Enterprise Monitoring agent installation

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

You can install the OS agent locally or remotely using the **tacmd createNode** command.

Installing agents locally

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

- IBM Tivoli Monitoring V5.X Endpoint
- Linux OS
- UNIX Logs UNIX OS
- Universal Agent
- Warehouse Proxy
- Warehouse Summarization and Pruning
- Windows OS
- UNIX OS

If you are installing other agents (for example, DB2 or Microsoft Exchange), launch the agent installation using the **setup.exe** or **install.sh** commands that are part of the particular agent installation packages.

The installation steps are similar to the Tivoli Enterprise Monitoring Server and Tivoli Enterprise Portal Server processes.

Windows

To launch the installation of the monitoring agent on Windows, the default installation directory is C:\IBM\ITM. You need to enter an encryption key to use, which controls to which Tivoli Enterprise Monitoring Server the monitoring agent can connect.

After the installation is complete, the configuration window opens, where you can configure the monitoring agent communication with the monitoring server.

Linux or UNIX

To launch the installation of the monitoring agent on Linux or UNIX, the default installation directory is /opt/IBM/ITM. You need to enter an encryption key to use, which controls to which Tivoli Enterprise Monitoring Server the monitoring agent can connect.

Note: After the Linux or UNIX installation completes, the next step is to configure the monitoring agent, which is not automatic as in the Windows installation. You need run **./itmcmd config -A *pc*** (*pc* is the product code) from /opt/IBM/ITM/bin.

Installing agents remotely

To deploy an OS agent from the command line interface, use the **tacmd createNode** command. For the full syntax, including the parameter descriptions, refer to the *IBM Tivoli Monitoring Command Reference,* SC23-6045-01.

For example, the following command deploys the UNIX OS monitoring agent on the server1.ibm.com computer in the /opt/IBM/ITM directory. Perform the installation as the root user:

```
tacmd createNode -h server1.ibm.com -d /opt/IBM/ITM -u root
```

Note: 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 in order for the **tacmd createNode** command to execute correctly. You cannot specify any other user ID.

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), which is used primarily for Windows servers
- Secure Shell (SSH), which is used primarily by UNIX servers, but it is also available on Windows. *Note that only SSH version 2 is supported.*
- Remote Execution (REXEC), which is used primarily by UNIX servers, but it is not very secure
- Remote Shell (RSH), which is used primarily by UNIX servers, but it is not very secure

You can specify a protocol to use; if you do not, the **tacmd createNode** command selects the appropriate protocol dynamically.

4.1.5 Tivoli Enterprise Portal desktop client installation

The following sections provide details about the desktop installation.

Windows

On Windows, the tasks include:

1. To launch the installation wizard, run **`setup.exe`** in the \WINDOWS directory in the IBM Tivoli Monitoring V6.2 media. The default installation directory is C:\IBM\ITM.
2. Enter an encryption key to use. Use the same key that you used during the installation of the portal server to which the client will connect.

After the installation completes, the installation program opens the configuration window, where you can configure the portal server connection with the monitoring server.

Linux or UNIX

On Linux or UNIX, the tasks include:

1. To launch the installation wizard, run **`./install.sh`** in the directory from where the installation files were extracted. The default installation directory is /opt/IBM/ITM. The installation runs in text mode.
2. Enter an encryption key to use. Use the same key that you used during the installation of the portal server to which the client will connect.

Note: After the installation, you need to configure the Tivoli Enterprise Portal desktop client. Change the directory to /opt/IBM/ITM/bin and run **`./itmcmd config -A cj`**.

4.1.6 Installing and enabling application support

Before you can view data that is collected by the monitoring agents, you must install and enable application support for those agents. Application support files provide agent-specific information for workspaces, help, 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 that are maintained by the hub monitoring server. These SQL files are also called *seed data*, and installing them on a monitoring server is 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 is 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 that 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 a non-OS agent remotely through the Tivoli Enterprise Portal, application support for the agent must be installed on the Tivoli Enterprise Portal Server *before* the agent is deployed.

Because application support for certain IBM Tivoli Monitoring 6.*x*-based distributed agents is included on the base installation CD, you might 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 the 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 4-1. On Windows, both installation and the 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, because the enablement step is done separately from the installation.

Table 4-1 Procedures for installing and enabling application support

Operating system	Monitoring servers	Portal server	Desktop clients
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 either the **`itmcmd support`** command or Manage Tivoli Monitoring Services window.	1. Install application support files from installation media. 2. *Configure* the portal server using either the **`itmcmd config`** command or Manage Tivoli Monitoring Services window.	1. Install application support files from installation media. 2. *Configure* the desktop client using either the **`itmcmd config`** command or Manage Tivoli Monitoring Services window.

Note:

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 a non-local monitoring server is not installed on the local computer, by installing the support using option 3, Install TEMS support for remote seeding, and 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 without uninstalling the Tivoli Enterprise Monitoring Server.

4.1.7 Adding application support to the hub monitoring server

All monitoring agents require that application support files are 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, help, predefined situations, and other data.

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 by 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`*

   `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 that are installed on this computer, run the following command:

   `./cinfo`

   You also see the other components that are installed.

Type 1 when prompted to display the product codes for the components that are installed on this computer. Refer to 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 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. Change to the bin directory:

   ```
   cd install_dir/bin
   ```

3. Run the following command using the parameters that are described in Table 4-2:

   ```
   ./itmcmd manage [-h ITMinstall_dir]
   ```

Table 4-2 Parameters for the itmcmd manage command

Parameter	Description
-h	(optional) You can use this parameter to specify the installation directory.
ITMinstall_dir	This parameter is 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.

4. Start the monitoring server if it is not already started. Right-click **Tivoli Enterprise Monitoring Server** and click **Start**.

5. 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**.
6. If you selected the **Advanced** option, the Install Product Support window is displayed. Select the application support packages that you want to install and click **Install**.
7. 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**.

4.1.8 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 that you specified does not exist, you are asked whether to create it. Type `y` to create this directory. The prompt shown in Example 4-1 displayed.

Example 4-1 Prompt

```
Select one of the following:
Install products to the local host.
Install products to depot for remote deployment (requires TEMS).
Install TEMS support for remote seeding
Exit install.
Please enter a valid number:
```

4. Type `2` to start the installation and press Enter.
5. The license agreement is displayed. Press Enter to read through the agreement. 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.

7. When you have specified all of the agents that you want to add to the agent depot, type `E` and press Enter to exit.

Notes:

- You need to have monitoring server installed before a depot can be created.
- You can also populate the agent depot using the **`tacmd addBundles`** command.

4.1.9 Manage Tivoli Monitoring Services

Manage Tivoli Monitoring Services is the administration tool on Windows and Linux systems for configuring and managing IBM Tivoli Monitoring components. This topic provides information about starting Manage Tivoli Monitoring Services and describes the Tivoli Enterprise Portal Server (referred to as the *portal server*) and client setup and maintenance functions.

Use Manage Tivoli Monitoring Services to:

- Supply initial configuration data to Tivoli Management Services components after downloading them to your machine.
- Start and stop IBM Tivoli Monitoring software components that run as Windows NT® services.

You can also use Manage Tivoli Monitoring Services to perform the following tasks:

- Activate or deactivate trace logging for a service, if necessary.
- Edit variables for a service, if necessary.
- Change default Java Settings for IBM Tivoli Monitoring components that use Java, if desired.

Opening the Manage Tivoli Monitoring Services window

To open Manage Tivoli Monitoring Services, on the computer where IBM Tivoli Monitoring is installed, click **Start** → **Programs** → **IBM Tivoli Monitoring** → **Manage Tivoli Monitoring Services**:

- **Starting a service**

  Use these instructions to start any of the services listed. Because the Tivoli Enterprise Monitoring Server (referred to as the *monitoring server*) is the central component of IBM Tivoli Monitoring, it must be started first, followed by the Tivoli Enterprise Portal Server, resource agents, and Tivoli Data Warehouse, if used. Users can then log on to the portal server from their browser or desktop, depending on how the client is configured.

- **Locally**

  To start a service on the local system, double-click the green icon next to its name in the Manage Tivoli Monitoring Services window or anywhere on the row.

- **Remotely**

  You can also start or stop a service on a remote Windows system that has the same version of Manage Tivoli Monitoring Services installed on it as this computer and on which you have Windows Administrator authority. Use the following steps to start a service remotely:

  a. Click **Windows** → **Open Remote View** to open the Manage Remote Services window.

  b. Type the name of the remote computer and click **OK**.

     You must have administrator authority on both computers, because the remote service control manager is opened.

  c. Double-click the service to stop or start.

4.1.10 Configuring IBM Tivoli Monitoring Web Services (SOAP Server)

IBM Tivoli Monitoring Web Services provides 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.

Windows: Defining hubs

Use the following steps to define SOAP hubs on Windows:

1. Start Manage Tivoli Monitoring Services by selecting **Start** → **(All) Programs** → **IBM Tivoli Monitoring** → **Manage Tivoli Monitoring Services**.
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 can choose any alias (for example, HUB2). Alias names can be a minimum of three characters and a maximum of eight characters.
7. Choose one of the following communication types:
   – If you are using TCP/IP or TCP/IP Pipe communications, complete the fields in Table 4-3.

Table 4-3 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 4-4.

Table 4-4 SNA fields in Hub Specification dialog

Field	Description
Network Name	Your site SNA network identifier
LU Name	The LU name for the monitoring server, which 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.

UNIX and Linux: Defining hubs (command-line interface 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>
   ```

   Accept the defaults, which reflect the choices that you made during the last configuration, until you see the following prompt, which is shown in Example 4-2.

   Example 4-2 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:
   ```

2. 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:

```
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):
```

After you enter the alias, the list of hubs with the new hub added is displayed. See Example 4-3.

Example 4-3 List of hubs

```
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 that you have already defined.

4.1.11 Tivoli Data Warehouse installation

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.

With Tivoli Data Warehouse, you can analyze historical trends from monitoring agents. Tivoli Data Warehouse uses an IBM DB2, Oracle, or Microsoft SQL Server database to store historical data that is collected across the environment. You can generate warehouse reports for short-term (file) and long-term data (RDBMS) through Tivoli Enterprise Portal.

Tivoli Data Warehouse uses the Warehouse Proxy agent (WPA) to move data from monitoring agents or the monitoring server to the data warehouse database. The Warehouse Proxy is an Open Database Connectivity (ODBC) export server for warehousing historical data. It is a special agent that uses an ODBC connection to transfer historical data that is collected from agents to a database.

You can then analyze this data using the workspaces in Tivoli Enterprise Portal or any third-party software.

The Warehouse Summarization and Pruning Agent provides the ability to customize the length of time for which to save data (pruning) and how often to compress data (summarization).

Preinstallation configuration

The Tivoli Data Warehouse needs a relational database to store the historical data. DB2 UDB is the preferred database, but Microsoft SQL and Oracle are also supported.

Note: The warehouse database is supported on Microsoft SQL Server only if the Tivoli Enterprise Portal Server (portal server) 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.

Before initiating the Warehouse Proxy agent installation and configuration, you need to create a Windows user with database administration rights (for example, the DB2ADMNS group).

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 that are required for interacting with 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.

Important: A DB2 database is created automatically at install time only if the Warehouse Proxy Agent is installed on Windows and the Tivoli Data Warehouse is also on Windows.

If the Warehouse Proxy Agent is connected to a Tivoli Data Warehouse database on Unix (AIX or Linux), the database needs to be created manually.

If the Warehouse Proxy Agent is on Windows and connected to a Tivoli Data Warehouse database on Unix (AIX or Linux), an ODBC connection is used to connect to the Tivoli Data Warehouse database.

If Warehouse Proxy Agent is on Unix (Linux or AIX) and connected to a Tivoli Data Warehouse database on UNIX (AIX or Linux), a JDBC connection is used to connect to the Tivoli Data Warehouse database.

The Tivoli Data Warehouse database should have UTF8 encoding when it is an ORACLE or a DB2 database.

Installing and configuring the Warehouse Proxy agent

As with other IBM Tivoli Monitoring agents, the Warehouse Proxy agent installation follows the same procedure as the procedure that we described in 4.1.4, “Tivoli Enterprise Monitoring agent installation” on page 66.

After installing the Warehouse Proxy agent, you need to configure it to connect to the database in order to retrieve and insert data. For Warehouse Proxy agent on Windows, you can use the Manage Tivoli Enterprise Monitoring Services console to *reconfigure* it. For Warehouse Proxy agent on UNIX, you must complete the configuration of the Warehouse Proxy agent using the Manage Tivoli Monitoring Services GUI, which requires an X11 GUI interface.

Configuring a Warehouse Proxy agent on Windows (ODBC)

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** to the message regarding connection to a hub monitoring server.
2. The next two windows (titled 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** in response to the message asking if you want to configure the ODBC datasource.
4. Select **DB2** from the list of databases and click **OK**.

   The configuration window that is shown in Figure 4-2 on page 82 is displayed.
5. Click **OK** to accept all default information on this window, or change one or more default values, and then click **OK**.
6. Click **OK**.

You *only* select the “Synchronize TEPS Warehouse Information” check box if you are reconfiguring 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.

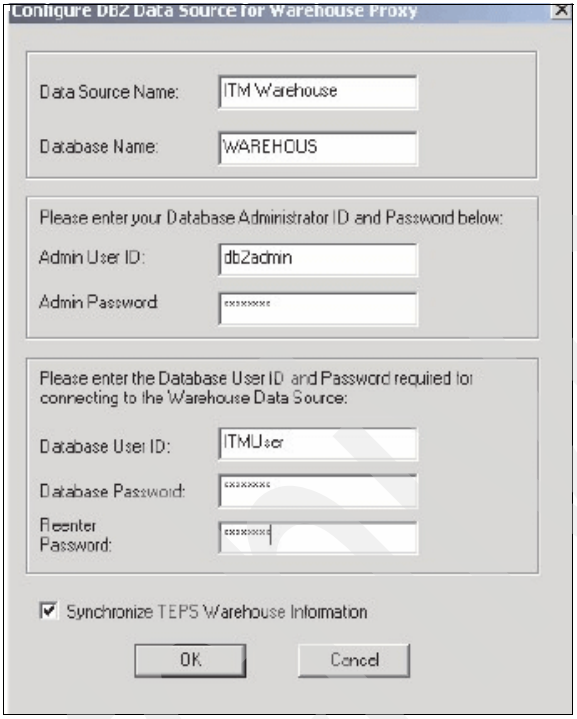


Figure 4-2 Configure DB2 Data Source for Warehouse Proxy window

Configuring a Warehouse Proxy agent on on Linux or AIX (JDBC)

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.

2. On the TEMS Connection tab (Figure 4-3), 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 that are used by the application agents and by the hub monitoring server. If the Warehouse Proxy agent does not have the same protocol as the hub monitoring server, it cannot register with the hub. If the Warehouse Proxy does not have the same protocol as the application agents, the application agents cannot communicate with the proxy when they try to create a route to it.

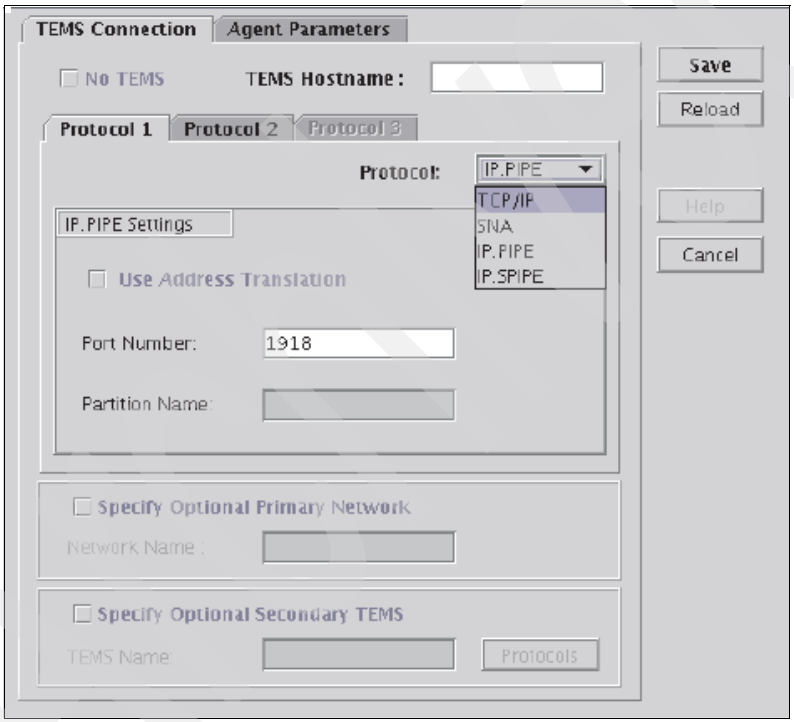


Figure 4-3 Configure Warehouse Proxy window (TEMS Connection tab)

3. Click the **Agent Parameters** tab (Figure 4-4 on page 85) and enter the following information:

   a. In the Database drop-down list, select **DB2**.

   b. Add the names and directory locations of the JDBC driver JAR files to the JDBC Drivers list box:

      i. 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.

      ii. 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

      iii. 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**.

   c. Change the default value that is displayed in the Warehouse URL field if it is incorrect. The default Tivoli Data Warehouse URL for IBM DB2 is:

      ```
      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.

   d. 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:

      com.ibm.db2.jcc.DB2Driver

   e. 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.

f. Select 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 certain 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 application programming interface (API).

g. Click **Test database connection** to ensure that you can communicate with the Tivoli Data Warehouse database.

h. Click **Save** to save your settings and close the window.

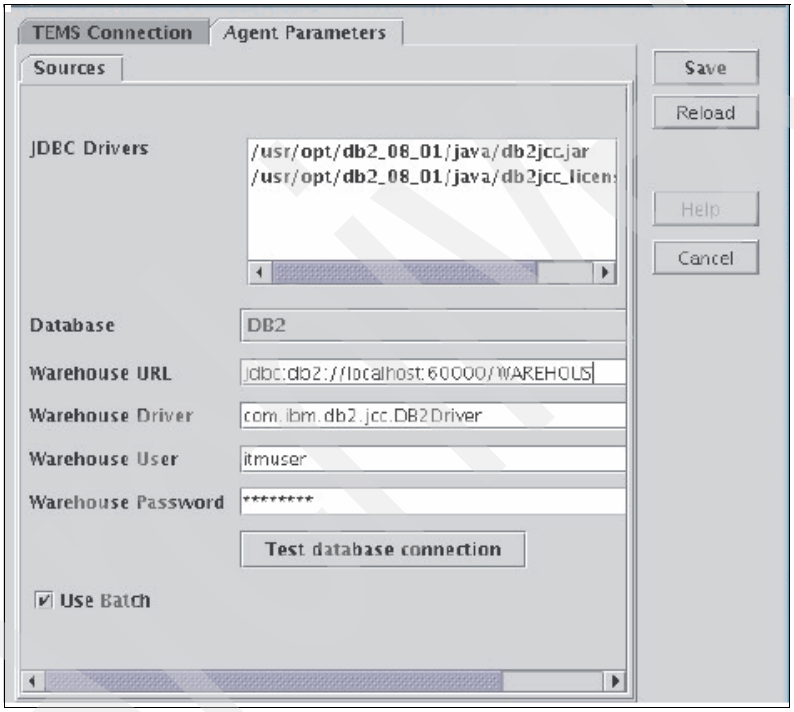


Figure 4-4 Configure Warehouse Proxy window (Agent Parameters tab)

Starting the Warehouse Proxy

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

For 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
```

The parameter ***hd*** is the product code for the Warehouse Proxy agent.

Summarization and Pruning Agent

As with other IBM Tivoli Monitoring agents, the Summarization and Pruning Agent installation follows the same procedure as the procedure that we described in 4.1.4, “Tivoli Enterprise Monitoring agent installation” on page 66.

After installing the Summarization and Pruning Agent, you need to configure how data will be collected, aggregated, and pruned. For the best performance, install the Summarization and Pruning agent on the same computer as the data warehouse.

Configuring the Summarization and Pruning Agent

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:
     i. 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**.
     ii. On the next window, verify the host name and port number of the hub monitoring server. Click **OK**.
   - On Linux or UNIX, select the **TEMS Connection** tab and verify the following information:
     i. The host name of the hub monitoring server in the TEMS Hostname field. (If the field is not active, clear the No TEMS check box.)
     ii. The communications protocol that the hub monitoring server uses in the Protocol drop-down list.
     iii. If you select IP.UDP, IP.PIPE, or IP.SPIPE, enter the port number of the monitoring server in the Port Number field.
     iv. If you select Systems Network Architecture (SNA), enter information in the Net Name, LU Name, and LOG Mode fields.

   d. When you are finished verifying or entering information about the hub monitoring server:
      - On Windows, click **Yes** in response to 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 4-5 on page 89 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.

3. On the configuration window:
   a. Add the names and directory locations of the JDBC driver JAR files to the JDBC Drivers list box.

      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.

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**.

d. In the Database field, select the database platform that 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 that you selected are displayed in the other text fields on the Sources tab.

e. Change the default value that is displayed in the Warehouse URL field if it is not correct:

   - 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.

f. 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.)

g. 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.

h. 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.

i. Click **Test database connection** to ensure that you can communicate with the Tivoli Data Warehouse database.

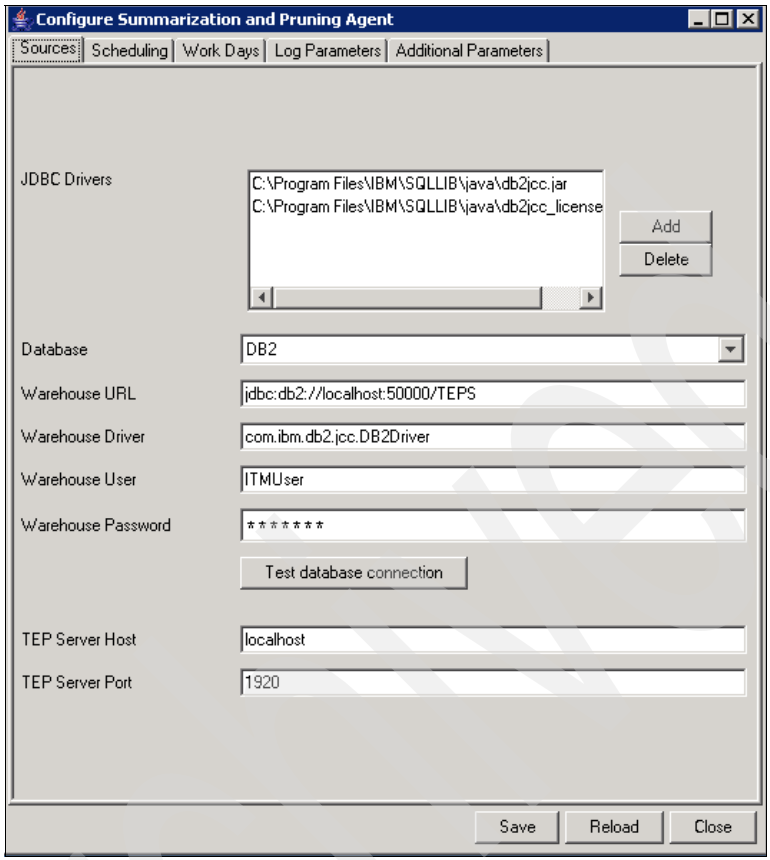


Figure 4-5 Sources tab of Configure Summarization and Pruning Agent window

4. Select the **Scheduling** tab to specify when you want summarization and pruning to take place. You can schedule summarization and pruning to run on a fixed schedule or on a flexible schedule, as shown in Figure 4-6 on page 90:
   - Fixed:
     - Schedule the Summarization and Pruning agent to run every *x* days.
     - Select the time of day that you want the agent to run. Set the time to at least five minutes from the current time if 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 does *not* run, using the format *HH:MM-HH:MM*. Click **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 the start time.

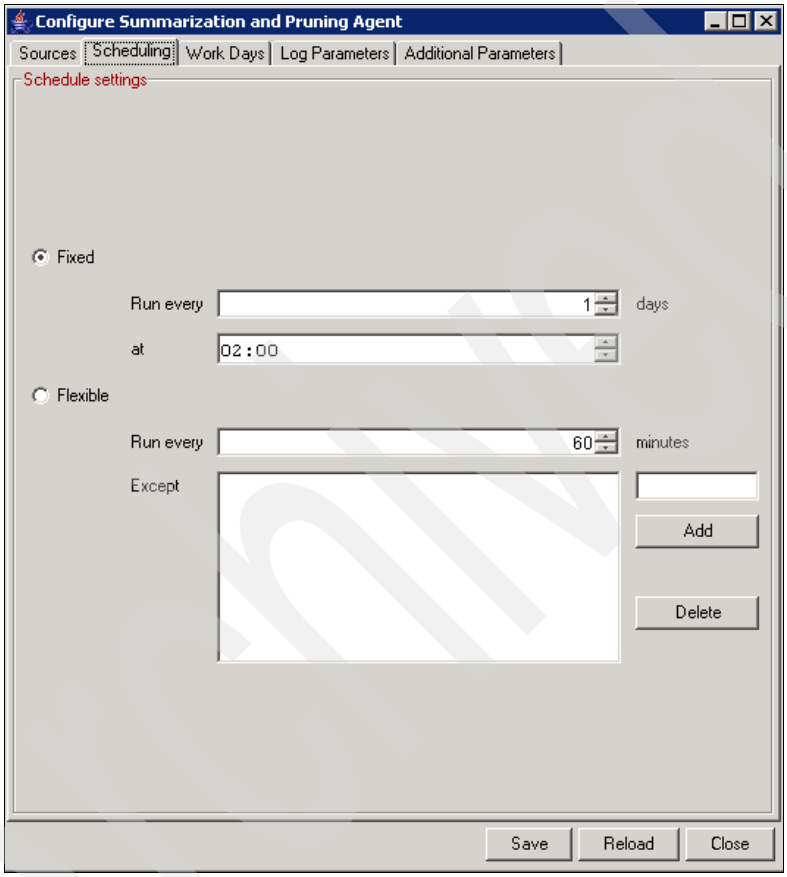


Figure 4-6 Scheduling tab of Configure Summarization and Pruning Agent window

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 that you specify on the Scheduling tab. If you select Flexible, the Summarization and Pruning agent runs one time immediately after it is started and then at the interval that you specified, except during any blackout times.

5. Specify shift and vacation settings in the **Work Days** tab (Figure 4-7 on page 92):

   When you enable and configure shifts, IBM Tivoli Monitoring produces three 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 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:
     - Select **Specify shifts** to enable shifts.
     - 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:
     i. Select **Specify vacation days** to enable vacation days.
     ii. Select **Yes** in the drop-down list if you want to specify weekends as vacation days.
     iii. Select **Add** to add vacation days.
     iv. Select the vacation days that 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 that you select are displayed in the list box.

   If you want to delete any days that you have previously chosen, select them and click **Delete**.

Notes: 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.

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.

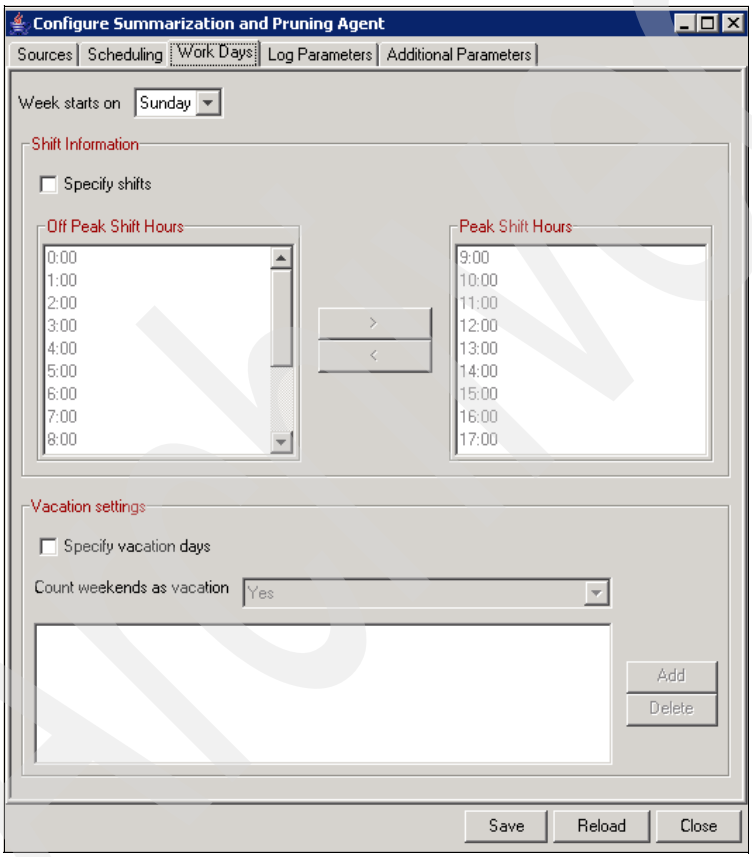


Figure 4-7 Work Days tab of Configure Summarization and Pruning Agent window

6. Select the **Log Parameters** tab to set the intervals for log pruning (Figure 4-8 on page 93):
   - Select **Keep WAREHOUSEAGGREGLOG data for**, select the unit of time (day, month, or year), and select the number of units of data to keep.

– Select **Keep WAREHOUSELOG data for**, select the unit of time (day, month, or year), and select the number of units of data to keep.

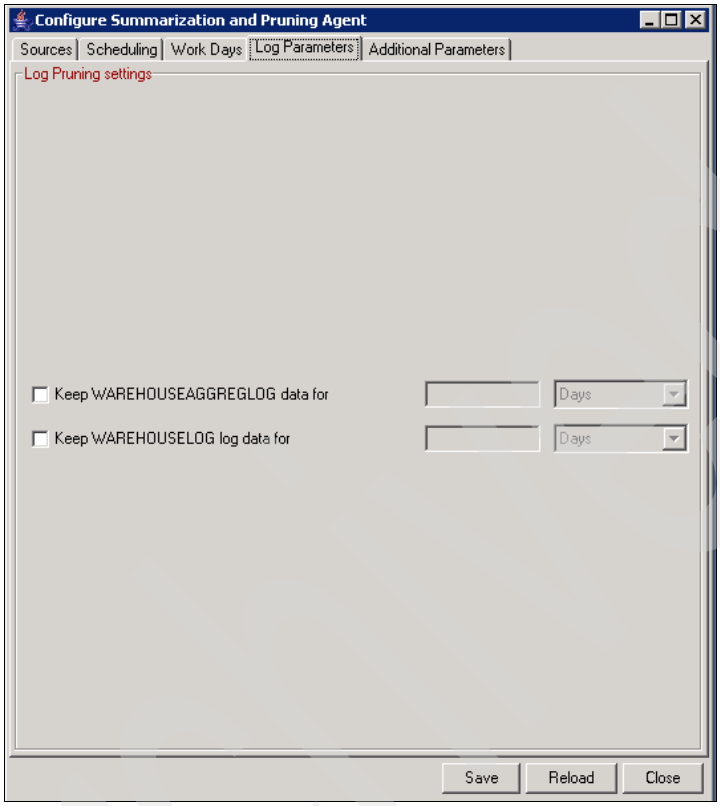


Figure 4-8 Log Parameters tab of Summarization and Pruning Agent configuration window

7. Specify the additional summarization and pruning settings in the **Additional Parameters** tab (Figure 4-9 on page 95):
   a. Enter the number of worker threads to use.
   b. Enter the maximum rows per database transaction.
   c. For the “Use timezone offset from” field, indicate 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.

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**.

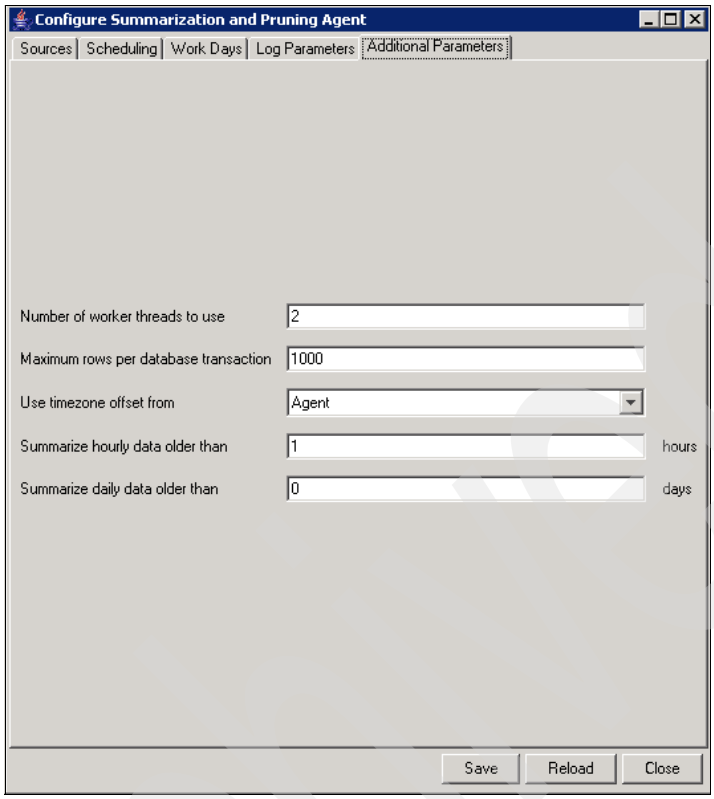


Figure 4-9 Additional Parameters tab of Summarization and Pruning Agent configuration window

Starting the Summarization and Pruning agent

To start 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 where ***sy*** is the product code for the Summarization and Pruning agent.

  ```
  ./itmcmd agent start sy
  ```

Configuring data collection and warehousing

Your user ID must have Configure History permission to open the History Collection Configuration window. If you do not have this permission, you will not see the menu item or tool for historical configuration.

On the Tivoli Enterprise Portal, take the following steps to configure historical data collection:

1. Click **History Configuration** (calendar icon) to open the History Collection Configuration window.
2. Select the product (agent type) for which you want to collect data from the Select a product drop-down list.

   The attribute groups for which you can collect historical data are displayed in the Select Attribute Groups list box. Note that when you select a product type, you are configuring collection for all monitoring agents of that type that report to the selected monitoring server. If your monitored environment is a large scale environment with many hundreds of agents of a certain type, there might be a delay when you select the product.
3. Select one or more attribute groups. You can also click **Show Default Groups** to automatically select the attribute groups that have predefined historical workspaces.

   When you first open the window, the controls show the default settings. As you select attribute groups from the list, the controls do not change for the selected group but remain static. If you change the settings for a group, those changes continue to display no matter which group you select while the window is open. This function enables you to adjust the configuration controls one time and apply the same settings to any number of attribute groups (select one attribute group after the other, use Ctrl+click to select multiple attribute groups, or Shift+click to select all groups from the first group selected to this point). The true configuration settings are shown in the Select Attribute Groups table.

   If you have configurations that you want to populate to several attribute groups, click the attribute group that has the configurations that you want to see reflected in the Configuration Controls area and highlight the other attribute groups that you want configured and click **Configure Group**. All of the selected attribute groups will reflect the same configurations. If collection has been started for any of the attribute groups that you have selected, stop collection before attempting to change the configurations.
4. Specify the following collection options:
   - **Collection Interval**

     Specify the frequency of data sample transmission to the history file. The options are: every 1, 5, 15, or 30 minutes, every hour, or every day. The

default interval is 15 minutes. The shorter the interval, the faster and larger the history file grows at the collection location. This history file can overload the database, warehouse proxy, and summarization and pruning agent. For example, if you set a 1-minute collection interval for Process data, expect the summarization and pruning for that attribute group to take a long time. Only enable an extremely short interval for an attribute group if it is critical in your work.

– **Collection Location**

  Specify where the historical data files will reside: at the Tivoli Enterprise Monitoring agent (TEMA) or the Tivoli Enterprise Monitoring Server (TEMS). The default location is the monitoring agent, which minimizes the performance impact on the monitoring server from historical data management. Note, however, that the Tivoli Enterprise Monitoring Server might be a better choice for certain environments. Also, the OMEGAMON XE on z/OS product requires that the data is stored at the monitoring server.

– **Warehouse Interval**

  Specify whether or not data is warehoused, and how often. The options are: **`hourly`**, **`daily`**, or **`Off`**. If you choose to warehouse historical data, you can also schedule summarization and pruning of the data. If you select Off, these options are disabled.

The collection options for an attribute group apply on all monitoring servers on which collection for those attributes is currently enabled. For certain sets of attribute groups, the configuration is hard-coded by the product. These attribute groups will display “fixed” in the Collection and Warehouse Interval cells of the Select Attribute Groups table.

5. If warehousing is enabled, specify the time periods for which data in the warehouse is summarized (aggregated).

   When you select a particular time period, any time period within the time period that you select is automatically selected, too. For example, if you select yearly summarized data, quarterly, monthly, weekly, daily, and hourly data are also selected, by default. If you do not want to keep data for all of the selected time periods, deselect the time periods that you do not want.

6. If summarization is scheduled, specify how long to keep data for each category of summarized data (hourly, monthly, and so on) before being pruned (deleted).

Click **Configure Groups** to apply the configuration selections to the attribute group or groups. If you currently have configuration controls selected for this product group, click **Stop Collection** first. Apply the new configuration selections and then click **Start Collection** to start the collection of data again.

For information regarding unconfiguring historical data collection and starting data collection, refer to *IBM Tivoli Monitoring User's Guide, Version 6.2.0,* SC32-9409.

4.1.12 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 exist 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.

Installing components with a response file

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 (Table 4-5 on page 98) as appropriate for your environment.

Table 4-5 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: ► $ ► = ► |

Parameter	Definition
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. 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.
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 a 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

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:

   `./itmcmd config -A -p <response_file> pc`

   where:

   – *<response_file>* is the name of the configuration response file. Use an absolute path to this file.
   – *<ms_name>* is the name of the monitoring server that you want to configure.
   – *pc* is the product code for the component or agent that you want to configure.

4.2 Upgrading from a previous OMEGAMON version

This section provides information for upgrading from IBM Tivoli OMEGAMON Platform Version 350 or 360 to IBM Tivoli Monitoring V6.2.

4.2.1 Upgrade procedure

Upgrading from Tivoli OMEGAMON XE to Tivoli Monitoring V6.2 can be simple and easy if carefully planned and implemented. The next sections provide details for performing a successful upgrade. Table 4-6 on page 100 introduces the new terminology used in IBM Tivoli Monitoring V6.2.

Table 4-6 OMEGAMON to Tivoli Monitoring V6.2 terminology

OMEGAMON term	IBM Tivoli Monitoring V6.2 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 Monitoring Services

OMEGAMON term	IBM Tivoli Monitoring V6.2 term
Manage Candle Services	Manage Tivoli Enterprise Monitoring Services
Event	Situation event
Seeding	Adding application support
OMEGAMON Web Services	Tivoli Monitoring Web Services
Candle Client Support	IBM Software Support

What to do before performing the upgrade

Before upgrading your environment, you need to perform the following tasks:

1. Gather information: Verify the previous OMEGAMON XE version. IBM Tivoli Monitoring V6.2 can only be upgrade from OMEGAMON Version 350 or 360.
2. Hardware and OS: Verify that your environment complies with *IBM Tivoli Monitoring Installation and Setup Guide, Version 6.2.0,* GC32-9407.
3. Database: Verify that the RDBMS being used is supported.
4. User: Verify that the user performing the upgrade has administrator privileges.
5. Backup: Perform a backup of the file system where the OMEGAMON is installed, perform a backup of the CMS database (QA1*.db and QA1*.idx), CMS data (situations and policies), and CNPS database (migrate-export.bat tool).
6. Services startup: Before initiating the upgrade procedure, stop all the components in the Candle environment. Configure the component startup to be manual and reboot the computer to unlock any locked files.

What you need to know before starting the upgrade process

Note the following considerations before you attempt to upgrade your OMEGAMON Platform Version 350 or 360 to IBM Tivoli Monitoring V6.2.

ODBC and database

Before you start the upgrade, you need to know the configuration of the various components in order to have proper communication. This information includes the configuration of the Tivoli Enterprise Portal Server, Warehouse Proxy agent, and the Summarization and Pruning Agent. This communication is needed to insert and retrieve data from the various databases in the Tivoli Enterprise Portal Server and in the Warehouse Proxy agent. To perform the database access, those components use Open Database Connectivity (ODBC) and JDBC for the Summarization and Pruning Agent. The correct configuration of those interfaces or gateways is crucial to the success of the upgrade.

Installation directory

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.

Agent configuration

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 Candle Management Workstation (CMW) is used in the OMEGAMON monitoring environment, the installed CMW continues to function after the migration, although it is not officially part of IBM Tivoli Monitoring and no new functionality will be added.

If the OMEGAMON XE for CICS V3.1.0 product is used, CMW must still be used to configure workloads for Service Level Analysis. After configuring the workloads, use the Tivoli Enterprise Portal client for all other tasks.

If Candle Management Workstation is not currently installed (for example, if OMEGAMON XE for CICS V3.1.0 is being installed for the first time into an IBM Tivoli Monitoring V6.2 environment), the CMW that ships with the OMEGAMON XE for CICS 3.1.0 product must first be installed. However, if it is needed, be sure to install CMW on a different computer than Tivoli Enterprise Portal. Otherwise, the CMW attempts to uninstall Tivoli Enterprise Portal.

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 conversion 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 JRE

CandleNet Portal requires the Sun™ Java™ Runtime Environment (JRE). However, Tivoli Enterprise Portal requires the IBM JRE 1.5. You do not need to install this JRE prior to the upgrade; it is installed automatically when you install an IBM Tivoli Monitoring component that requires it.

Migrated information when upgrading from a previous version

If the software is installed over a previous release (into the same IBM directory), the following information is migrated into the new version:

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

Upgrading components

This section provides an overview of upgrading the components and describes the basic operations to migrate the components.

Perform the upgrade operation in the following order:

1. Upgrade the CMS, CNPS, CNP, and OMAs.
2. Install the Summarization and Pruning Agent.
3. Migrate the existing data for the Candle Warehouse Proxy.

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

- Hub Tivoli Enterprise Monitoring Server
- Remote monitoring server (if necessary)
- Tivoli Enterprise Monitoring 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.

Candle Management Server (CMS)

Run the IBM Tivoli Monitoring installation program and use the existing installation directory as the IBM Tivoli Monitoring directory.

CandleNet Portal Server (CNPS)

Upgrading the CNPS is the next step after successfully upgrading your hub and remote CMS servers. Remember to make a backup of your CNPS data before

proceeding. Run the IBM Tivoli Monitoring installation program, as you did when upgrading your Candle Management Server.

CandleNet Portal (CNP)

The CandleNet Portal will not work until you upgrade it to Tivoli Enterprise Portal. You also need migrate objects from Candle Management Workstation to Tivoli Enterprise Portal. Table 4-7 shows the scripts used to migrate users and managed objects.

Table 4-7 Scripts to migrate OMEGAMON objects

Objects	Scripts
User IDs	**migrate-new-users-ibmdb2.bat** UDB **migrate-new-users-mssql.bat** Microsoft SQL Version 7 or Microsoft Database Engines
Managed objects	**migrate-cmw-navigator-ibmdb2.bat** UDB **migrate-cmw-navigator-mssql.bat** Microsoft SQL Version 7 or Microsoft Database Engines

OMEGAMON Monitoring Agent (OMA)

Upgrade OMA, also known as the Candle Monitoring Agent (CMA), to Tivoli Enterprise Monitoring agent by running the installation program.

Candle Warehouse Proxy

You can migrate existing data in an OMEGAMON V360 Data Warehouse to the IBM Tivoli Monitoring Tivoli Data Warehouse by using a migration tool provided with IBM Tivoli Monitoring.

Before migrating to the new Data Warehouse, you need to create a new ODBC datasource for the 6.2.0 version of the Warehouse Proxy agent and connect that datasource to a new database. The migration tool (**migratewarehouse.bat**) moves your data from the existing database to the new database. The warehouse migration tool is installed when you install the Warehouse Summarization and Pruning Agent. Therefore, before performing the Warehouse Proxy upgrade, first install the Summarization and Pruning Agent.

Summarization and Pruning Agent installation

Refer to *IBM Tivoli Monitoring Installation and Setup Guide, Version 6.2.0*, GC32-9407, for information about how to install the Summarization and Pruning Agent.

4.2.2 Upgrade considerations

Note the following considerations when upgrading from a previous OMEGAMON environment to IBM Tivoli Monitoring V6.2.

Using existing OMEGAMON agents with IBM Tivoli Monitoring

Existing installed OMEGAMON Version 350 and 360 agents are supported using Tivoli Enterprise Monitoring Server. However, the following restrictions apply:

- New features in IBM Tivoli Monitoring (such as remote deployment) are not supported on these 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.
- An OMEGAMON agent cannot be installed 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.

To monitor the OMEGAMON agent, use Manage Candle Services to change the monitoring server to the agent that sends data. To enable Tivoli Data Warehouse to collect data from these agents (through the Warehouse Proxy), copy the product attribute file to the ATTRLIB directory on the Warehouse Proxy agent.

For full interoperability between OMEGAMON agents and IBM Tivoli Monitoring, you need to install the application support files for these agents on the Tivoli Enterprise Monitoring Server, Tivoli Monitoring Portal Server, and Tivoli Monitoring Portal desktop client.

4.3 IBM Tivoli Monitoring V5.*x* upgrade

IBM provides a toolkit to facilitate migrating your existing IBM Tivoli Monitoring (ITM) 5.*x* environment to IBM Tivoli Monitoring V6.2.

The Migration Toolkit is a Tivoli Management Framework-based application that is required to scan and provide snapshots of the IBM Tivoli Monitoring V5 world.

This section provides details about this tool.

4.3.1 Product prerequisites

The following sections discusses the installation requirements and supported platforms for IBM Tivoli Monitoring V5.*x* upgrade toolkit.

Installation requirements

The requirements are:

- Tivoli Management Framework Version 3.7 or higher
- IBM Tivoli Monitoring 5.1.2 Fix Pack 10 or higher
- IBM Runtime Environment for Java, Version 1.4.2 or higher

Supported platforms

For TMR Servers:

- Solaris
- AIX
- HP-UX
- Linux
- Linux S/390®
- Windows

For endpoint interps:

- Aix4-r1
- Hpux10
- Linux-ix86
- Linux-s390
- Linux-ppc
- Solaris2
- W32-ix86
- OS/400® (Only for Profile assess and migrate)

4.3.2 Installation procedure

You can install the toolkit either with the Tivoli command line or the Tivoli desktop.

The toolkit must be installed on every Tivoli management region (TMR) and gateway to be migrated or that is in the Tivoli Management Framework structure of endpoints to be migrated. The toolkit installation is required even if toolkit commands are only run from the TMR Server.

Installing the toolkit from the Tivoli command line

This section describes how to install the toolkit using Tivoli commands:

1. Log on to the Tivoli server or gateway and invoke the Tivoli environment.

2. If you are installing from the physical CD, insert or mount the CD titled IBM Tivoli Monitoring 6.2 Tools.
3. Locate the itm5_upgrade/IBM-Tivoli-Monitoring-Migration-Toolkit/MTK.IND file.
4. Use the Tivoli **winstall** command to install the toolkit:

   ```
   winstall [–c source_dir] –i MTK [–n | managed_node ...] [–y]
   [MtkJavaDir=jre_bin_dir] [ScanValue=0 | 1 ]
   ```

   where:

   -c *source_dir*

   Specify the complete path of the directory that contains the MTK.IND file. If you are running the command from a Tivoli server on a Windows system, enclose the path name in double quotation marks.

   -i MTK

   This parameter specifies the file name of the product index file MTK.IND (without the extension) from which the toolkit is installed.

   [–n | *managed_node* ...]

   –n

   Specify **-n** to install the toolkit on all managed nodes that do not currently have the toolkit installed. This option is ignored when ***managed_node*** is specified.

   You might not want to use this option, because your Tivoli management region might have:

   - Gateways that manage only endpoints that are *not* monitored by V5.1.2
   - Gateways that manage endpoints monitored by V5.1.2, but you do not want to or cannot migrate those endpoints (perhaps the migration of the resource models that they run is not supported)

   In these cases, this option will unnecessarily install the toolkit on those gateways.

   managed_node ...

   Specify the managed nodes on which to install the toolkit. Provide the names of all servers and managed node gateways with endpoints that you want to migrate from V5.1.2, and separate the names by a space.

   If you do not specify either **–n** or ***managed_node***, the toolkit is installed on all managed nodes in the Tivoli region, including the server.

   -y

   Installs the toolkit without requesting confirmation

MtkJavaDir=*jre_bin_dir*

Specifies the full path location of the Java binary files on the Tivoli server. On Windows systems, enclose the path name in double quotation marks. The upgrade tools requires IBM Runtime Environment for Java, Version 1.4.2 or higher. See 4.3.1, “Product prerequisites” on page 106 for more information about Java requirements.

Note: The option name **MtkJavaDir** is case-sensitive.

If you do not specify the location of the JRE with this command, use the **witmmtk javapath** command after you install the migration toolkit to specify the location.

ScanValue=0 | 1

Indicate whether to run (**1**) or not run (**0**) the Scantmr tool (**witmmtk scantmr** command) during the installation of the migration toolkit. The default is not to run the tool. The output from the Scantmr tool is a baseline data file that maps your V5.1.2 environment to a proposed V6.2 infrastructure. A scan can take considerable time in a large environment. If you do not perform a scan during installation of the toolkit, you can use the Scantmr tool after installation.

Note: The option name **ScanValue** is case-sensitive.

If you specify **ScanValue=1**, you must also specify the location of the Java binary files using the ***MtkJavaDir*** variable. The Scantmr tool must have access to the Java location in order to run.

Example

The following example installs the migration toolkit on a Tivoli server on a Windows server and to the managed nodes `dan`, `don`, and `brooks`. The Scantmr tool is not run. The tar file containing the toolkit was unzipped to the C:\toolkit directory:

```
winstall –c
"C:\toolkit\itm5_upgrade/IBM-Tivoli-Monitoring-Migration-Toolkit/" –i
MTK dan don brooks -y MtkJavaDir="C:\Program
Files\Tivoli\bin\w32-ix86\JRE\1.3.0\jre\bin"
```

Installing the toolkit from the Tivoli desktop

This section describes how to install the toolkit using the Tivoli desktop:

1. Log on to the Tivoli server and invoke the Tivoli environment.

2. If you are installing from a physical CD, insert or mount the CD titled *IBM Tivoli Monitoring V6.2 Tools.*
3. Locate the itm5_upgrade/IBM-Tivoli-Monitoring-Migration-Toolkit/MTK.IND file.
4. Access the Tivoli desktop.
5. Select **Install** from the Desktop menu.
6. Select **Install Product** in the menu to display the Install Product window (Figure 4-10 on page 109).

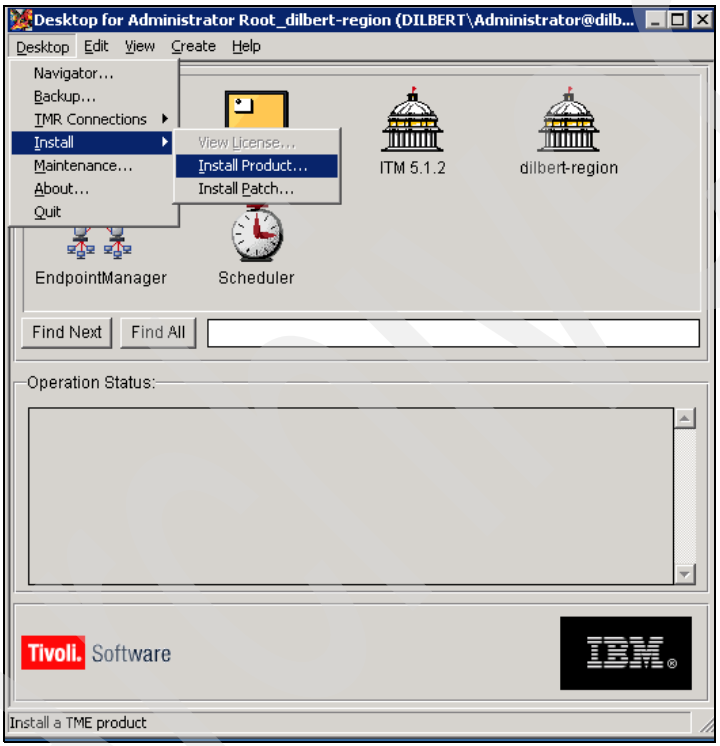


Figure 4-10 Install Migration Tookit via Tivoli Desktop

7. If necessary, click **OK** to ignore an error message about the media settings.
8. Click **Select Media** to display the File Browser window.
9. In the Path Name text field, type the full path to the MTK.IND file.
10. Click **Set Path**. The File Browser window displays the contents of the specified media in the Files list box.
11. Click **Set Media & Close**. The Install Product window reopens.

12. Select **IBM Tivoli Monitoring Migration Toolkit: V5.1.2 to V6.2** from the Select Product to Install list box as shown in Figure 4-11 on page 110. The Install Options window opens.

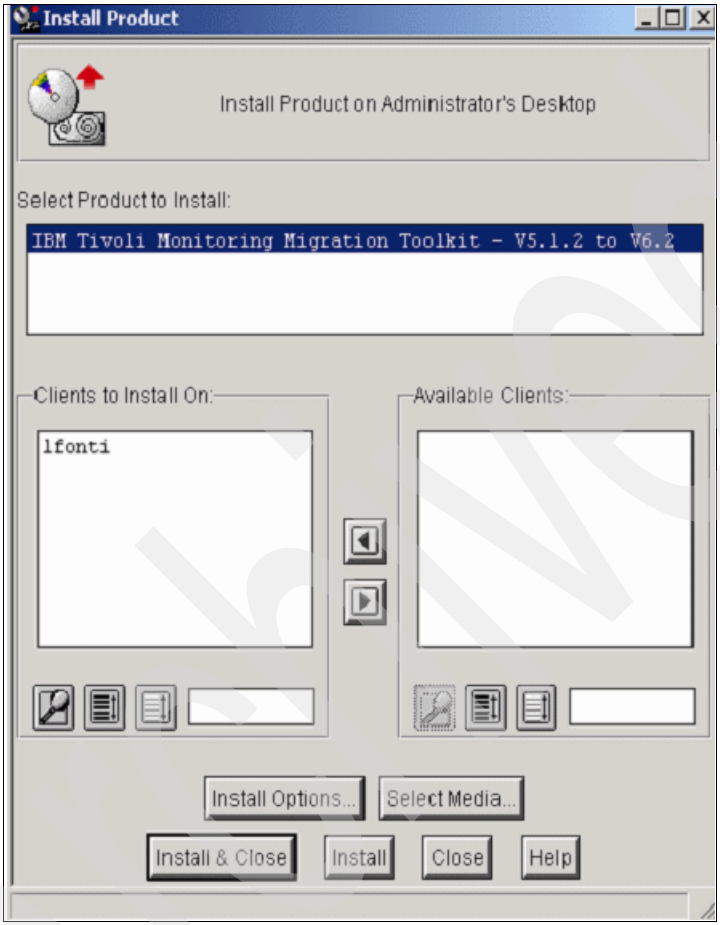


Figure 4-11 IBM Tivoli Monitoring Migration Toolkit: V5.1.2 to V6.2

13. Optionally, in the Install Options window, type the full path location of the Java binary files in the Java Runtime Environment path field, as shown in Figure 4-12 on page 111. Do not use double quotation mark characters (“ ”) around the path, even if it contains spaces.

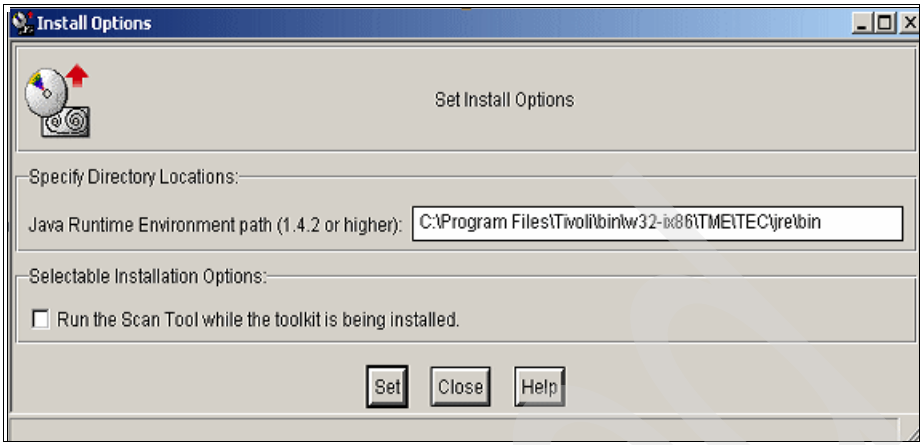


Figure 4-12 Java Runtime Environment path field

> **Note:** The upgrade tools require that you install IBM JRE Version 1.4.2 or higher on the Tivoli server. If you leave the Java Runtime Environment path field empty, you must use the **`witmmtk javapath`** command after you install the migration toolkit to specify the location of the Java binary files.

14. Optionally select the check box if you want to run the Scantmr tool (**`witmmtk scantmr`** command) during the installation of the migration toolkit.

> **Note:** The output from the Scantmr tool is a baseline data file that maps your V5.1.2 environment to a proposed V6.2 infrastructure. A scan can take considerable time in a large environment. If you do not perform a scan during the installation of the toolkit, you can use the Scantmr tool after installation. If you select the check box, you must also specify the location of the Java binary files in the “Specify Directory Locations” field. The Scantmr tool must have access to the Java location in order to run.

15. Click **Close** to close the Install Options window.

16. In the “Clients to Install On” list, you will see that all of the managed nodes are preselected, including those managed nodes that are gateways only to endpoints that are *not* monitored by V5.1.2. You need to install the toolkit only on gateways that manage endpoints running resource models that you are going to migrate. Follow these steps:

    a. Use the arrow keys to move all of those gateways that do not manage endpoints monitored by V5.1.2 from the “Clients to Install On” list to the

Available Clients list. If you move the wrong managed node by mistake, you can reverse the operation.

b. Your migration plans might determine that you do not need to, or cannot, migrate some endpoints monitored by V5.1.2 (for example, the endpoints might be running only those resource models for which the migration is not supported). In this case, if the gateway of these endpoints does not manage *any* endpoints that need to be migrated, you do not need to install the toolkit on that gateway. Move these endpoints also from the "Clients to Install On" list to the Available Clients list.

17. Click **Install** to display the Product Install window and a list of pending installation actions.
18. Click **Continue Install** to begin the installation process.

    The Product Install window displays the progress of the installation. View the messages in the task output window to determine whether the product installation was successful.
19. Click **Close** to close the Product Install window
20. Select **Refresh** from the **View** menu bar. The desktop displays the icon for the migration toolkit.

4.3.3 Uninstalling the Migration Toolkit

The format of the uninstall command is:

```
wuninst product_name <Tivoli_server> -rmfiles
```

where ***product_name*** **= mtk**

- The command must be issued for each gateway server first and then finally for the TMR.
- A **wchkdb –u** command is issued to ensure that the database is clean.

4.3.4 Upgrading in phases and steps

The upgrade tools and procedures are designed to transfer control to V6.2 while preserving the monitoring activity and monitored resources that are already in place. To enable V6.2 to take over from V5.1.2, the first requirement is to install a sufficient number of V6.2 servers (hub and remote Tivoli Enterprise Monitoring Servers and Tivoli Enterprise Portal Servers) to handle current monitoring requirements. The existing Tivoli endpoint systems, which host the monitored resources, can then be connected to the Tivoli Enterprise Monitoring Servers. Endpoints are connected to monitoring servers by deploying OS monitoring agents to the endpoints. The final result is that the endpoints become part of the V6.2 environment. At the same time, however, the endpoints remain connected

to the V5.1.2 environment so that monitoring can continue until the V5.1.2 resource models are no longer needed.

The next step is to replace the resource models in the V5.1.2 profiles with V6.2 *situations*. Situations are associated with appropriate monitoring agents and with lists of managed systems to be monitored. The managed system lists are created from the subscriber lists of profile managers.

Figure 4-13 shows a diagram of the phases and steps.

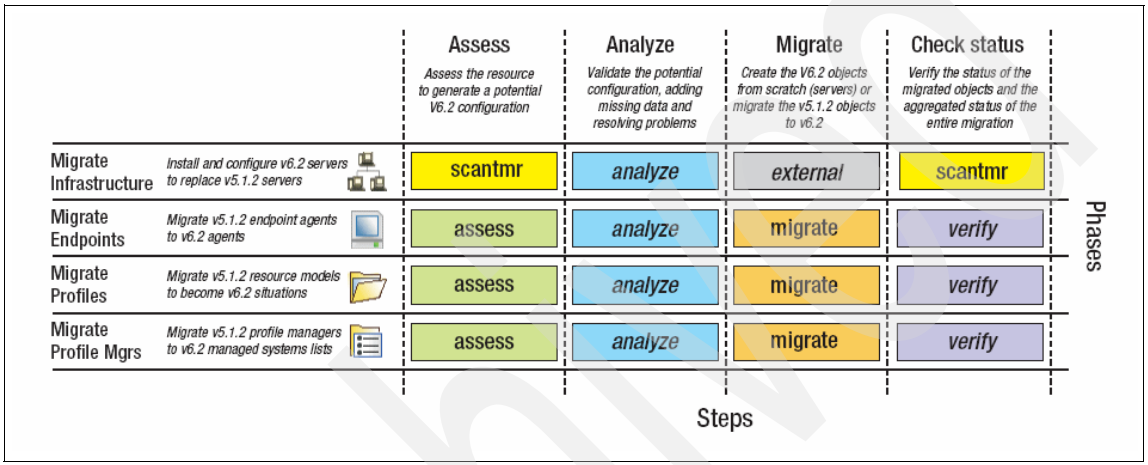


Figure 4-13 Migration by phase and step

Next, we summarize what is included in an upgrade and how to upgrade the elements.

The phases

We will now discuss the phases of upgrading to V6.2:

- **Phase A: Migrate infrastructure**

  Install V6.2 servers to provide the infrastructure support required for monitoring. They replace the infrastructure function of Tivoli servers and gateways.

  The migration of all interconnected infrastructure must take place before any of the other phases can begin.

  If you have Tivoli management regions that are not in any way connected, the migration of each region can be treated as a completely separate activity.

  This phase is described in detail in Chapter 6 of *Upgrading from IBM Tivoli Monitoring V5.1.2, Version 6.2.0,* GC32-1976.

- **Determine the strategy for the other phases**

  Before starting to upgrade endpoints, profiles, and profile managers, you must determine a strategy for the upgrade.

  At this point, the upgrade process becomes incremental, because it is not necessary to complete migrating all of the resources at each phase before moving on to the next phase. For example, you do not need to deploy all monitoring agents to all endpoints before starting to migrate profiles (although you must have migrated all endpoints subscribed to any profile that you want to migrate).

  You thus need to determine how to continue, either migrating all endpoints, all profiles, and then all profile managers, or by dividing your V5.1.2 environment into discrete segments and migrating each segment separately. These options are described more fully in Chapter 7 of *Upgrading from IBM Tivoli Monitoring V5.1.2, Version 6.2.0,* GC32-1976.

- **Phase B: Migrate endpoints**

  Deploy monitoring agents to endpoints, starting with OS monitoring agents. After an OS monitoring agent is deployed to an endpoint, the endpoint is able to communicate with its assigned monitoring server. When an agent is deployed, its target operating system or application becomes a managed system.

  This phase is described in detail in Chapter 8 of *Upgrading from IBM Tivoli Monitoring V5.1.2, Version 6.2.0,* GC32-1976.

- **Phase C: Migrate profiles**

  Deploy situations to replace the resource models in the profiles. At least one situation is created for each resource model indication.

  This phase is described in detail in Chapter 9 of *Upgrading from IBM Tivoli Monitoring V5.1.2, Version 6.2.0,* GC32-1976.

- **Phase D: Migrate profile managers**

  Create managed system lists that correspond to Tivoli subscriber lists. Situations that correspond to the resource models associated with a profile manager are activated after the profile manager is migrated.

  This phase is described in detail in Chapter 10 of *Upgrading from IBM Tivoli Monitoring V5.1.2, Version 6.2.0,* GC32-1976.

Review and cleanup

Review the results and clean up V5.1.2 resource models that have been successfully migrated.

This phase is described in detail in Chapter 11of *Upgrading from IBM Tivoli Monitoring V5.1.2, Version 6.2.0,* GC32-1976

The steps

Each of the phases in the upgrade is an iterative process that follows these workflow steps:

- ***Assess*:** For a set of V5.1.2 resources, request upgrade status and migration settings.
- ***Analyze*:** For a set of V5.1.2 resources that have not yet been migrated, inspect the proposed migration settings.
- ***Migrate*:** Migrate a set of non-migrated V5.1.2 resources to V6.2.
- ***Review results and check status*:** Review the outcome of the object migration and monitor the overall status of the upgrade.

  Each of the phase descriptions explains how the steps are performed. The following section describes the tools that you can use to perform many parts of the upgrade.

4.4 Monitoring Agent for IBM Tivoli Monitoring V5.X Endpoint

The Monitoring Agent for IBM Tivoli Monitoring V5.X Endpoint extends the capability of IBM Tivoli Monitoring V5.1.2 Fix Pack 6. This agent enables data collected by deployed IBM Tivoli Monitoring V5.1.2 Fix Pack 6 endpoints to be displayed in the IBM Tivoli Monitoring V6.2 Tivoli Enterprise Portal and stored in the IBM Tivoli Monitoring V6.2 Tivoli Data Warehouse component.

Notes:

- The Monitoring Agent for IBM Tivoli Monitoring V5.X Endpoint is also called the *integration agent*. It enables the collection and visualization of IBM Tivoli Monitoring V5.1.x resource models in Tivoli Enterprise Portal.
- The integration agent receives data from the IBM Tivoli Monitoring V5.1.2 engine using local pipes and sends the data to IBM Tivoli Monitoring V6.2 components.

This section contains the following information about the installation and configuration of the Monitoring Agent for IBM Tivoli Monitoring V5.X Endpoint:

- Preinstallation steps
- Reconfiguring data logging
- Installing Monitoring Agent for Tivoli Monitoring V5.X Endpoint
- Configuring and distributing Monitoring Agent for IBM Tivoli Monitoring 5.X Endpoint

4.4.1 Preinstallation steps

Before installing Monitoring Agent for IBM Tivoli Monitoring V5.X Endpoint, you need to verify that the IBM Tivoli Monitoring environment has the following software installed:

- IBM Tivoli Monitoring V5.1.2 Fix Pack 6
- IBM Tivoli Monitoring Component Services Version 5.1.1 Fix Pack 2 or Version 5.1.3

In addition, if IBM Tivoli Monitoring V6.2 was installed, verify that the following components that are required to use Tivoli Enterprise Portal to view IBM Tivoli Monitoring V5.1.2 Fix Pack 6 data and store it in the Tivoli Data Warehouse component are installed:

- Tivoli Enterprise Monitoring Server
- Tivoli Enterprise Portal Server
- Tivoli Enterprise Portal
- Warehouse Proxy

4.4.2 Using the Tivoli Enterprise Portal to view resource model data

The data that is available in the Web Health Console is also available in the Tivoli Enterprise Portal. The organization is similar, but the specific views and their contents differ, because of differences in how information is displayed in the user interfaces.

The Web Health Console has two top-level views: the Endpoint view and the Resource Model view. The Tivoli Enterprise Portal displays data similarly to the Web Health Console Endpoint view. (There is no equivalent of the Resource Model view in the Tivoli Enterprise Portal.)

The following information is displayed on the Tivoli Enterprise Portal console when viewing resource model overview workspace:

- ProfileName
- RMName
- Status

4.4.3 Reconfiguring data logging

This is an optional procedure that enables you to determine which kind of data you can collect from your Monitoring Agent for IBM Tivoli Monitoring 5.X Endpoint.

A new IBM Tivoli Monitoring command-line interface (CLI) can be used to perform this configuration:

```
wdmepconfig
```

You can configure the seeding information to let the agent log data of **ITM5**, **ITM6**, or **BOTH** with the following results:

- **ITM5**: The data is written in the earlier Tivoli Data Warehouse V1.*x*.
- **ITM6**: The data is written in the new Tivoli Data Warehouse V2.1.
- **BOTH**: The data is both written in Tivoli Data Warehouse V1.*x* and V2.1.

This is an example:

```
wdmepconfig -e endpoint -D DataSeeding=ITM6
```

If you choose to collect data only for IBM Tivoli Monitoring V6.2 (**ITM6**), you get a request to stop the roll-up of the XML files that contain the aggregated warehouse data from the endpoints to the RDBMS Interface Module (RIM) and to change the IBM Tivoli Monitoring profile collection options to disable the Tivoli Data Warehouse logging.

To stop the collection, you can use this command:

```
wdmcollect -m all -t
```

To change the Tmw2kProfile logging configuration, clear the **TEDW Data** check box in Resource Model.

4.4.4 Installing Monitoring Agent for Tivoli Monitoring V5.X Endpoint

The installation of this component requires IBM Tivoli Monitoring V5.1.2 Fix Pack 6, which enables the full compatibility between the IBM Tivoli Monitoring, V5.1.2 Agent, and the Monitoring Agent for IBM Tivoli Monitoring 5.X Endpoint.

The installation can either be performed using the **winstall** command or from the Tivoli Desktop.

Tivoli Desktop

To install using the Tivoli desktop, complete the following steps:

1. Select **Install** → **Install Product** from the Desktop menu.

> **Note:** If the last installation directory is no longer current, you might receive an error message about the media settings. Just click **OK**.

2. Click **Select Media**, which opens the File Browser window. Locate the directory containing the ITM61AGT.IND file, and then click **Set Path** → **Set Media and Close**.
3. Select the software name from the Select Product to Install list and select the targets of your installation from the Clients to Install On list.

> **Note:** The ITM61AGT product must be installed on the Tivoli server and all gateways in the environment that have the Tmw2kProfile distributed and on which we want to install the Monitoring Agent for IBM Tivoli Monitoring 5.X Endpoint code.

4. Click **Install & Close** when you complete the Clients to Install On selection. The Product Install opens. Click **Continue Install** to start the installation process.

When the installation completes, you see the message "`Finished product installation`" at the bottom of the Product Install window.

Command-line interface using winstall

Run the following command from the command prompt:

```
winstall -c source_dir [-s server] -i product [-y] [-n | managed_node...]
```

Where:

-c *source_dir*	Specifies the complete path to the directory containing the installation image.
-s *server*	Specifies the name of the managed node to use as the installation server. By default, the installation server is the Tivoli server.
-i *product*	Specifies the product index file (ITM61AGT.IND file) from which the product is installed. You can omit the .IND in the command.
-y	Installs the product without requesting confirmation.
-n	Installs the product on all managed nodes that do not currently have the product installed. This option is ignored when ***managed_node*** is specified.

managed_node Specifies the managed nodes on which to install this Tivoli Enterprise product. You can specify multiple managed nodes. If you do not specify a managed node, the product is installed on all managed nodes in your Tivoli region.

Refer to *Tivoli Management Framework Reference Manual, Version 4.1.1*, SC32-0806, for more information about this command.

4.4.5 Configuring and distributing Monitoring Agent for IBM Tivoli Monitoring 5.X Endpoint

You must perform this last step in order to enable data collection from the managed systems that you want to monitor.

You can perform this procedure in two ways:

- Distribution
- Manual distribution

The Monitoring Agent for IBM Tivoli Monitoring 5.X Endpoint is started and stopped by the IBM Tivoli Monitoring V5.1.2 engine and installed in the IBM Tivoli Monitoring V5.1.2 environment. To facilitate the installation, configuration, and operation, it is installed using traditional Tivoli endpoint distribution mechanisms through the new **witm61agt** command-line interface.

Distribution

Perform the following steps:

1. Use the following command on each targeted system:

   ```
   witm61agt -c CMSAddress[:BackupCMSAddress] [-f] [-n] [-i seeding]
   [-o outfile] [[-D Variable=Value] ... ] [ -P protocol ] [-p port]
   {-a | endpoint [endpoint ...] | @filename}
   ```

   Where:

   -f Forces the distribution to proceed even if the operating system version check fails.

   -n No distribution of binaries, just performs the configuration.

   -r Removes files from endpoints, rather than distributing.

   -i The IBM Tivoli Monitoring **wdmepconfig** command is also invoked on each endpoint. ***seeding*** specifies where data will go. Valid values are **ITM5**, **ITM6**, or **BOTH**.

   -o Does not distribute binaries or configure, just dumps the endpoint list to ***outfile***.

-D Adds the setting **Variable=Value** to the environment file for the agent.

-P Specifies the network protocol to use: **TCP** or **UDP**. The default is **TCP**.

-c Specifies the network name of the monitoring server. Optionally, you can specify a backup server, separated by a colon (**:**).

-p Specifies the TCP/IP port number on which the monitoring server listens.

-a All endpoints that have IBM Tivoli Monitoring profiles distributed to them will receive the distribution.

endpoint Distributes to the named endpoints.

@filename Distributes to all endpoints named in the specified file.

2. If you have not set the logging behavior of the IBM Tivoli Monitoring engine using the **-i** option in the previous step, you can use the following command, which only sets that logging behavior:

   ```
   wdmepconfig {-e endpoint | @endpoint_file} {-D DataSeeding=ITM5 |
   ITM6 | BOTH}
   ```

   Where:

   -e *endpoint* For IBM Tivoli Monitoring V5.1.2, a list of one or more names of the endpoints.

   -e @*endpoints_file* For IBM Tivoli Monitoring V5.1.2, the file that contains the list of endpoints.

   -D DataSeeding Application to which to log data, with the following possible values:

   ITM5 IBM Tivoli Monitoring V5.1.2. This is the default value. The data is logged in Tivoli Data Warehouse and Web Health Console, but not Tivoli Enterprise Portal.

   ITM6 IBM Tivoli Monitoring V6.2. The data is logged in Tivoli Enterprise Portal, but not in Tivoli Data Warehouse and Web Health Console.

   BOTH IBM Tivoli Monitoring V5.1.2 and IBM Tivoli Monitoring V6.2. This is the preferred setting. You can start with this option, decide which option you prefer, and then reconfigure accordingly.

Note: Both the **wdmepconfig** and the **witm61agent** (if the **-i** flag is specified during its execution, it will recall the **wdmepconfig** command) commands generate a MDist 2 distribution. Make sure that you have configured the MDist 2 database and can successfully open your MDist 2 GUI from the Tivoli desktop before executing any of these commands.

Manual distribution

Use the following command to manually copy the files on an endpoint and push only the configuration for both IBM Tivoli Monitoring V5.1.2 (**ITM5**) and IBM Tivoli Monitoring V6.2 (**ITM6**) data logging on a Tivoli Enterprise Monitoring Server called mytems that uses the default port 1918:

```
witm61agt endpoint -n -i BOTH -c mytems
```

The **-n** option is for no dependency push.

Distribute the code as follows:

1. Insert the CD into the computer with the endpoint.
2. Install the agent code, which is located in the /AGENT directory on the CD:
   a. Open the top level directory of the lcf installation directory where the endpoint is installed, for example, $LCFROOT.
   b. Extract the operating system-specific binary files from the /AGENT directory.
3. Extract the selected files using the following command:

   ```
   [root@istanbul][/]-> cd /opt/Tivoli/lcf/dat/1
   [root@istanbul][/opt/Tivoli/lcf/dat/1]-> . ./lcf_env.sh
   [root@istanbul][/opt/Tivoli/lcf/dat/1]-> cd $LCFROOT
   [root@istanbul][/opt/Tivoli/lcf]-> zcat <filename> | tar xvf -
   ```

   Where ***<filename>*** is the file name for the operating system.
4. Extract the following metadata files from the $LCF_DATDIR/LCFNEW/KTM directory. This file was created by the **witm61agt** command when it was run to configure the endpoint. The file exists, even if the **-n** option was used so that the main bulk of code was not distributed on the endpoint.
   – For UNIX systems: metadata.tar.Z
   – For Windows systems: metadata.zip

4.5 Integration with IBM Tivoli Enterprise Console

IBM Tivoli Monitoring V6.2 can be configured to send events to IBM Tivoli Enterprise Console. This section provides details about how to install the components used to integrate IBM Tivoli Monitoring V6.2 with IBM Tivoli Enterprise Console.

Note: Note that IBM Tivoli Monitoring V6.2 also supports Netcool/OMNIbus integration. See “Event integration with Netcool/OMNIbus” on page 19 for more details.

We use the following components in this integration:

- OMEGAMON Tivoli Event Adapter (OTEA):

  This is supplied as part of the Tivoli Enterprise Monitoring Server (monitoring server), and the Event Integration Facility (EIF) is the communication method used to send the IBM Tivoli Enterprise Console events.

- Tivoli Enterprise Console event synchronization:

  This component is installed on each IBM Tivoli Enterprise Console server to receive events from IBM Tivoli Monitoring V6.2. The underlying component is called the *Situation Update Forwarder (SUF)*, and SOAP is used as the communication method to send updates to Tivoli Enterprise Monitoring Server.

- Event and rule definitions:

  omegamon.rls Contains event specific synchronization rules.

  omegamon.baroc Contains the new IBM Tivoli Monitoring V6.2 base event definitions.

  Sentry.baroc Contains an updated version of Sentry2_0_Base to support Tivoli Distributed Monitoring V3.*x* environments.

  k<*TAG*>.baroc Each IBM Tivoli Monitoring V6.2 monitoring component provides separate files containing specific monitoring components. The <*TAG*> is 3z, a4, ex, ib, nt, oq, or, oy, ud, ul, ux. For example, the Windows events will be defined in knt.baroc. Note that these files need to be imported into your rule base manually after the installation.

4.5.1 OMEGAMON IBM Tivoli Enterprise Console Event Adapter (OTEA)

This section discusses installing and configuring OMEGAMON IBM Tivoli Enterprise Console Event Adapter (OTEA).

Installing the OTEA

To install the OTEA:

1. Enable the **TEC Event Integration Facility** option during the installation of the Tivoli Enterprise Monitoring Server, as shown in Figure 4-14.
2. When you click **OK**, you will configure the hub monitoring server. Then, you are prompted to enter the host name and port number of your IBM Tivoli Enterprise Console server to which events will be forwarded (The default port is 5529 on Windows. For UNIX Tivoli Enterprise Console, the default is 0).

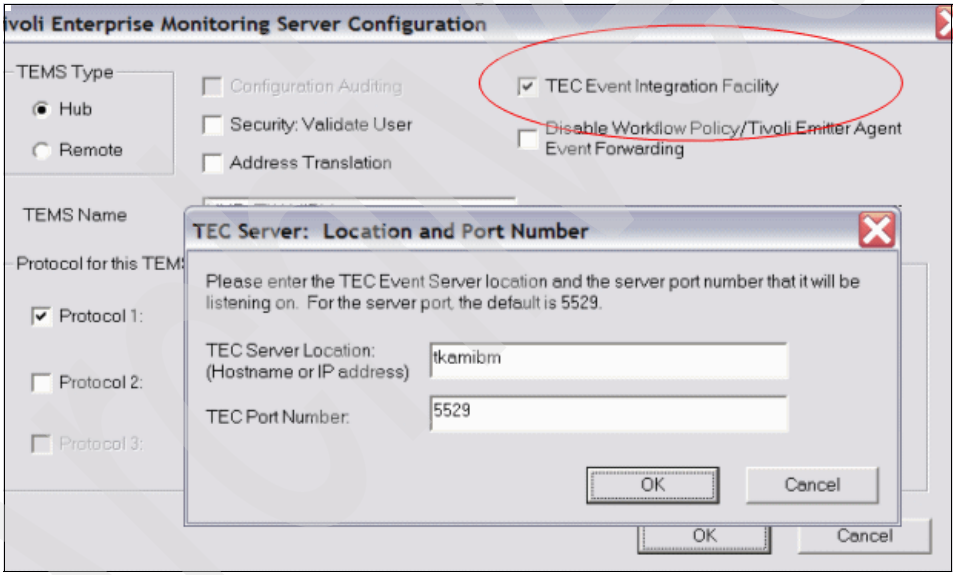


Figure 4-14 TEC Event Integration Facility

Note: The event forwarding uses the non-Tivoli-based transport mechanism.

Configuring the OTEA

The configuration files for the OTEA are in different locations, depending on the platform type of your monitoring server:

- **Windows** <*itm install dir*>\tems\TECLIB
- **UNIX** <*itm install dir*>/ tables/<*tems host name*>/TECLIB

Figure 4-15 shows the files contained in this location.

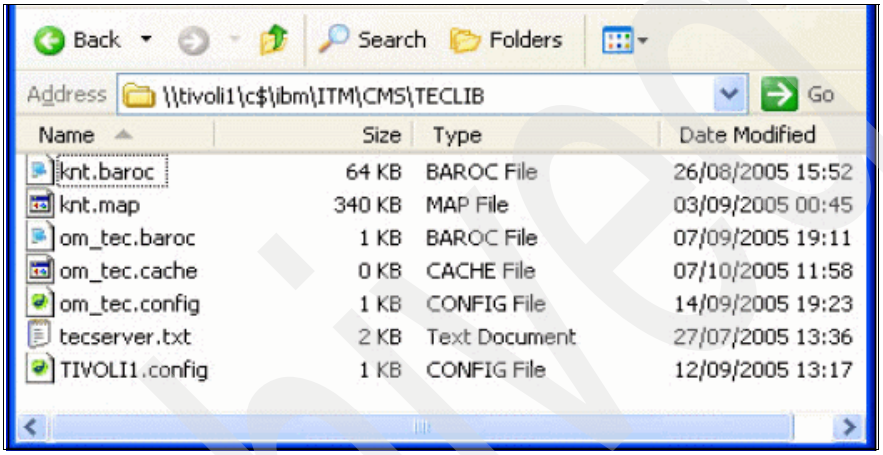


Figure 4-15 OMEGAMON TEC Adapter configuration files

EIF configuration

The EIF configuration file is om_tec.config. It contains several Tivoli Enterprise Console Adapter keywords, as shown in Example 4-4.

Example 4-4 om_tec.config file

```
ServerLocation=TIVOLI1
ServerPort=5529
EventMaxSize=4096
NO_UTF8_CONVERSION=YES
ConnectionMode=co
BufferEvents=YES
BufEvtMaxSize=4096
BufEvtPath=./TECLIB/om_tec.cache
FilterMode=OUT
Filter:Class=ITM_Generic;master_reset_flag=''
```

4.5.2 Installing Tivoli Enterprise Console event synchronization

The Tivoli Enterprise Console event synchronization component must be installed on the IBM Tivoli Enterprise Console (TEC) server. There are three methods for installing the event synchronization:

- From a wizard
- From the command line
- From the command line using a silent install

Installing from a wizard

Use the following steps to install event synchronization from the installation wizard:

1. On the event server, launch the event synchronization installation:
   - On Windows, double-click the **setupwin32.exe** file in the \TEC subdirectory on the IBM Tivoli Monitoring installation media.
   - On Linux or UNIX, change to the /<*os_type*>/tec subdirectory of the IBM Tivoli Monitoring installation media, and run the following command:

     `setup<operating_system>.bin`

     Where <*operating_system*> is the operating system on which you are installing.
2. Click **Next** in the Welcome window.
3. Select **I accept the terms in the license agreement** and click **Next**.
4. Complete the fields in Table 4-8 on page 126 and click **Next**.

Table 4-8 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.
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 that it processes. This value must be an integer. The minimum (and default) is 50.
URL of the Conversational Monitor System (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 Tivoli Enterprise Console sends event information.
Rate for sending SOAP requests to CMS from TEC via web services	Rate for sending SOAP requests to CMS from Tivoli Enterprise Console through Web services.
Level of debug detail for log	The level of information for event synchronization that will be logged.

5. Complete the information shown in Table 4-9 about the files where events will be written and click **Next**.

Table 4-9 Tivoli Enterprise Console event synchronization configuration fields

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.
Maximum number of cache files	The maximum number of event cache files at any given time. The minimum value is 2, and 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 reside	The location of event cache files.

6. Enter the following information for each monitoring server 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 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.

7. After providing information about all the monitoring servers, click **Next**.
8. Specify the rule base to use to synchronize events. You have two choices:
   - Create a new rulebase
   - Use the existing rulebase
9. If you are using an existing rule base, enter the name of the rule base.
10. If you want to import an existing rule base into a new rule base, enter 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.

11. Click **Next**.
12. Click **Next** on the preinstallation summary window.
13. When the installation and configuration steps are finished, a message telling you to stop and restart the event server is displayed. Click **OK**.
14. Click **Finish** in the Summary Information window.

> **Note:** You must stop and restart the event server for these changes to take effect.

Installing from the command line

The installation from the command line is similar to the wizard installation; it differs in how to launch the installation.

Run the following command to launch the installation:

- On Windows: **`setupwin32.exe -console`**
- On UNIX: **`setup<operating_system>.bin -console`**

Notes:

- Because the other steps are similar to wizard installation, we do not show them here.
- You can also install IBM Tivoli Monitoring Tivoli Enterprise Console event synchronization using the command line with silent installation.

4.5.3 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 add application support for each agent to the monitoring server, the monitoring agent .baroc files are in the following directory:

- On Windows: <*itm_installdir*>\cms\TECLIB
- On Linux and UNIX: <*itm_installdir*>/tables/<*ms_name*>/TECLIB

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). 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 previous example 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
```

After you load each of the agent .baroc files into the rule base and restart the event server, the event server is ready to receive and correctly parse any events that it receives from the monitoring server from one of the installed monitoring agents.

4.5.4 Event severity

The tec_server.txt file contains the non-default event severity mapping. By default, the IBM Tivoli Monitoring 6.2 severity of `Informational` is mapped to a Tivoli Enterprise Console severity of HARMLESS, and the IBM Tivoli Monitoring severities of WARNING and CRITICAL are preserved in the Tivoli Enterprise Console severity. The resulting Tivoli Enterprise Console severities of specific IBM Tivoli Monitoring situations can be controlled by modifying this tec_server.txt file.

In this file, lines starting with an asterisk (*) in column one are treated as comments. Each line specifies a destination IBM Tivoli Enterprise Console server and optionally a Tivoli Enterprise Console severity level for a situation name.

The syntax of each line is as follows:*

```
sitname=tecservername[:port]|*[,SEVERITY=severitylevel]
```

In this syntax:

- ***tecservername*** is the target IBM Tivoli Enterprise Console server name, address or “*” that denotes the default IBM Tivoli Enterprise Console server.
- ***port*** is the port on which the IBM Tivoli Enterprise Console server is listening or 0 if the IBM Tivoli Enterprise Console server is using port mapping (UNIX servers). If no port is specified, the default will be **0** (use port mapping).
- ***severitylevel*** is one of the valid severity levels supported by the IBM Tivoli Enterprise Console server (**FATAL** | **CRITICAL** | **MINOR** | **WARNING** | **HARMLESS** | **UNKNOWN**).

New in the IBM Tivoli Monitoring V6.2 release

Table 4-10 shows the enhancements to IBM Tivoli Enterprise Portal since the release of Version 6.1.0.

Table 4-10 New in IBM Tivoli Monitoring V6.2

Feature	Description
Event severities	The state of an event that opens for a true situation can be set to informational, warning, or critical. Now you have four additional states from which to choose for associated situations, table view thresholds, and for filtering an event console view: Unknown, Harmless, Minor, and Fatal.
Situation editor	The "EIF" (Event Integration Facility) tab enables you to forward events that open for the situation to one or more EIF receivers and to specify the severity.

For more information about new enhancements in IBM Tivoli Monitoring V6.2, refer to the *IBM Tivoli Monitoring 6.2, User's Guide,* SC32-9409.

4.5.5 Starting and stopping the process that sends updates to a monitoring server

To send event updates to a monitoring server, you must start a long-running process called Situation Update Forwarder. This process is started automatically when the event server starts. To stop the process manually, change to the $BINDIR/TME/TEC/OM_TEC/bin directory (where $BINDIR is the location of the IBM Tivoli Enterprise Console installation) and run the following command:

On Windows:

```
stopSUF.cmd
```

On UNIX:

```
stopSUF.sh
```

On Windows, you can also use the Tivoli Situation Update Forwarder service to start or stop the forwarding of event updates. You can start and stop this service either from the Windows Service Manager utility or with the following commands:

- `net start situpdate`
- `net stop situpdate`

To start the process, run the following command:

On Windows:

```
startSUF.exe config_file
```

On UNIX:

```
startSUF.sh config_file
```

Note: config_file is the name of the file where IBM Tivoli Enterprise Console configuration information is stored. The default name is /etc/TME/TEC/OM_TEC/situpdate.conf.

After changing the configuration file (situpdate.conf), you need to stop and start the process.

4.6 Uninstalling IBM Tivoli Monitoring V6.2

This section provides details about uninstalling IBM Tivoli Monitoring V6.2. We divide this section into the following parts:

- Uninstalling the entire IBM Tivoli Monitoring environment
- Uninstalling an individual IBM Tivoli Monitoring agent or component
- Uninstalling the Warehouse Proxy
- Uninstalling Tivoli Enterprise Console event synchronization

4.6.1 Uninstalling the entire IBM Tivoli Monitoring environment

You can use the following procedure to remove the entire IBM Tivoli Monitoring environment from your computer.

Note: To remove just one component, such as an agent, see 4.6.2, “Uninstalling an individual IBM Tivoli Monitoring agent or component” on page 133.

Uninstalling the environment on Windows

Perform the following steps:

1. From the desktop, click **Start** → **Settings** → **Control Panel** (for Microsoft Windows 2000 Server) or **Start** → **Control Panel** (for Windows Server 2003).
2. Click **Add/Remove Programs**.

3. Select **IBM Tivoli Monitoring** and click **Change/Remove**.
4. Select **Remove** and click **Next**.
5. The Confirm Uninstall window opens. Click **OK**.
6. After stopping Tivoli Enterprise Services, click **Yes** to remove the Tivoli Enterprise Portal database.
7. Inform database administrator credentials, type the password for the database administrator in the **Admin Password** field, and click **OK**.
8. Click **Finish** when the Product Remove Complete window opens.

Uninstalling the environment on Linux or UNIX

Perform the following steps:

1. From a command prompt, run the following command to change to the appropriate /bin directory:

   ```
   cd install_dir/bin
   ```

2. Run the following command:

   ```
   ./uninstall.sh
   ```

   A numbered list of product codes, architecture codes, version and release numbers, and product titles opens for all installed products.

3. You need to type the number for the installed product that you want to uninstall. Repeat this step for each additional installed product.
4. After removing all installed components, you are asked if you want to remove the installation directory. Type `y` and press Enter.
5. After the command completes, you can manually remove the IBM Tivoli Monitoring installation directory.

Notes:

- 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. You need to delete that database manually.
- You can also run the following command to remove all installed components from the command line:

  ```
  ./uninstall.sh REMOVE EVERYTHING
  ```

4.6.2 Uninstalling an individual IBM Tivoli Monitoring agent or component

Use the following procedure to remove an agent or other individual IBM Tivoli Monitoring component from your computer.

Uninstalling a component on Windows

Perform the following steps:

1. From the desktop, click **Start** → **Settings** → **Control Panel** (for Windows 2000 Server) or **Start** → **Control Panel** (for Windows Server 2003).
2. Click **Add/Remove Programs**.
3. Either:
   - To uninstall a single IBM Tivoli Monitoring component, such as the portal server or portal client (but not all components), select **IBM Tivoli Monitoring**.
   - To uninstall an agent bundle or a specific agent, select the agent bundle.
4. Click **Change/Remove**.
5. Either:
   - To uninstall a specific agent or component, select **Modify**.
   - 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, you need to:
   - For an agent, expand **Tivoli Enterprise Monitoring Agents**, and select the agent that you want to uninstall.
   - For a component, select the component (such as Tivoli Enterprise Portal Desktop Client).
     a. Click **Next**.
     b. Click **Next** on the confirmation window.
     c. Depending on the remaining components on the computer, there might be a series of configuration panels. Click **Next** on each of these panels.
9. Click **Finish** to complete the uninstall.

Uninstalling a component on Linux or UNIX

Perform the following steps:

1. From a command prompt, run the following command to change to the appropriate /bin directory:

   ```
   cd install_dir/bin
   ```

2. Run the following command:

   ```
   ./uninstall.sh
   ```

   A numbered list of product codes, architecture codes, version and release numbers, and product titles opens 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.

Uninstalling OMEGAMON agents

Perform the following steps:

1. Launch Manage Candle Services (Version 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 Agent column.
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 of the instances identified in step 4.
6. Open Windows Explorer and navigate to the installation directory for OMEGAMON V350 or V360 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 3-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 do not appear 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. The other steps are the same.

Removing an agent through Tivoli Enterprise Portal

You can also uninstall non-operating system monitoring agents from Tivoli Enterprise Portal by stopping the agent and removing its configuration settings. After removing 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 on which it was listed, and any custom Navigator view items to which it was assigned.

Notes:

- You cannot use Tivoli Enterprise Portal to remove or uninstall OS agents.
- If the Manage Tivoli Enterprise Monitoring Services utility is running when you uninstall the agent, it is shut down automatically by the uninstallation process.

Perform the following steps:

1. In Tivoli Enterprise Portal, right-click the agent Navigator item and click **Remove**.
2. Click **Yes** to confirm the removal of the agent.
3. When you are asked to confirm whether you want to permanently uninstall the agent, click **Yes** to uninstall or **No** to leave the agent installed on the computer.

4.6.3 Uninstalling the Warehouse Proxy

When you uninstall the Warehouse Proxy, the warehouse database is not dropped and historical situations on the agent are not stopped. Perform the following steps before uninstalling the Warehouse Proxy:

1. Stop the historical situations.
2. Drop the warehouse database.
3. Remove the ODBC datasource.
4. Remove the Windows user, ITMUser, that was created to connect to a DB2 database.

Removing the ODBC datasource connection

When you uninstall IBM Tivoli Monitoring, the ODBC datasource created for the Warehouse Proxy agent is not removed automatically, which can cause problems when you reinstall IBM Tivoli Monitoring. To prevent these problems, you need manually remove the ODBC datasource after uninstalling IBM Tivoli Monitoring.

For example, to remove the DB2 datasource from the DB2 command line, run the following command:

```
UNCATALOG SYSTEM ODBC DATA SOURCE <datasource_name>
```

If you are using a Microsoft SQL or Oracle database, use the Windows ODBC Datasource Administrator utility to remove the ODBC datasource.

4.6.4 Uninstalling Tivoli Enterprise Console event synchronization

Use the following steps to uninstall the event synchronization feature from the event server:

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, such as 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 UNIX:

     ```
     $BINDIR/TME/TEC/OM_TEC/_uninst/uninstaller.bin
     ```

3. Follow the prompts in the uninstallation program.

When the uninstallation is completed, you can tell the installer what rule base to load. 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 that you want to load.

You can also tell the uninstaller to stop and restart the event server.

Notes:

- You can also run this uninstallation program in silent mode (by running the program from the command line with the **`-silent`** parameter) or in console mode (by using the **`-console`** parameter).
- You must stop and restart the event server for these changes to take effect.
- If the 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.

Extra problem determination tips for installation and configuration

Additional tips:

1. If the Oracle agent is started and running but not displaying data in the Tivoli Enterprise Portal, check the following issues:
   a. Check the UNIX agent log files to see whether there are connection problems.
   b. Execute KORGRANT.SQL against the user account that you want to use for IBM Tivoli Monitoring.
   c. If there are no connection problems, check whether the agent has terminated. (Search for the word “terminated” in the log.)
   d. If the agent is not terminated, confirm that you have added application support for the Monitoring Agent in the Tivoli Enterprise Monitoring Server as described in *IBM Tivoli Monitoring Installation and Setup Guide, Version 6.2.0*, GC32-9407.
   e. Ensure that the database is up and is accessible on the network.
2. If you do not uninstall the TEPS database when uninstalling IIBM Tivoli Monitoring V6.2 on Windows, you need to perform the following steps to remove the TEPS database before reinstalling it:
   a. Drop the TEPS database.
   b. Remove the ODBC system Datasource Name (DSN) defined for the TEPS database.
3. If a Windows OS agent was installed off-line with a wrong Tivoli Enterprise Monitoring Server (monitoring server) name, you can use the following procedure to connect the OS agent to the correct monitoring server:
   a. Modify the windows registry on the OS agent machine.

b. Configure the Windows OS agent via Manage Tivoli Enterprise Monitoring Services (MTEMS).

4. Use the following steps to remove a partially installed IBM Tivoli Monitoring installation on Windows:

   a. Ensure that there is no entry in the Add and Remove Programs tool for the component that you attempted to install. If there is an entry, use that entry to uninstall the product. If there is no entry, proceed to the next step.

   b. Open the Windows Explorer and navigate to the IBM Tivoli Monitoring installation directory (C:\IBM\ITM by default).

   c. Launch the Manage Tivoli Enterprise Monitoring Services utility by double-clicking the KinConfg.exe file located in either the Install or InstallITM subdirectory.

   d. If any agents, the portal server, or the monitoring server are listed in the Manage Tivoli Enterprise Monitoring Services window, right-click each and click **Advanced** → **Unconfigure**. Repeat this step for all components that are listed. Close the Manage Tivoli Enterprise Monitoring Services utility.

   e. Open the Windows Control Panel.

   f. Double-click **Administrative Tools** and then double-click **Services**.

   g. Verify that all related IBM Tivoli Monitoring services have been removed. These services match those services listed in the Manage Tivoli Enterprise Monitoring Services window.

   h. Open the Registry Editor by clicking **Start** → **Run** and typing `regedt32`. Click **OK**.

   i. Expand the key HKEY_LOCAL_MACHINE registry key.

   j. Expand the SOFTWARE registry key.

   k. Expand the Candle registry key and record any sub-keys that are present. If the Candle key does not exist, proceed to step o on page 138.

   l. Expand the OMEGAMON registry key under the Candle key and record the content of the OMEGAMON key values.

   m. Delete the Candle registry key and all sub-keys. On Windows XP, you can right-click the Candle registry key and click **Delete**.

   n. Close the Registry Editor.

   o. Open Windows Explorer and find the IBM Tivoli Monitoring installation location on your system. The default value is C:\IBM\ITM.

   p. Delete this directory and all subdirectories.

   q. Remove the IBM Tivoli Monitoring bookmark from the Start menu:

      i. Click **Start** from the Windows desktop to display the Start menu items.

ii. Click **Programs.**

iii. Right-click **IBM Tivoli Monitoring** to display the bookmark menu options.

iv. Click **Delete** to remove the IBM Tivoli Monitoring bookmark from the Windows desktop start menu.

5

Configuration

In this chapter, we discuss the configuration process for IBM Tivoli Monitoring V6.2. We describe various ways to configure IBM Tivoli Monitoring in the Tivoli environment and the IBM Tivoli Monitoring features and interactions with other Tivoli products.

We discuss the following topics in this chapter:

- IBM Tivoli Monitoring upgrade tools
- Configuring IBM Tivoli Monitoring components
- IBM Tivoli Data Warehouse
- IBM Tivoli Universal Agent
- The tacmd command
- Agent Builder
- IBM Tivoli Monitoring V5.X Endpoint features

5.1 IBM Tivoli Monitoring upgrade tools

IBM Tivoli Monitoring provides an upgrade toolkit to assist with the upgrade of Tivoli Distributed Monitoring. The upgrade toolkit is contained in a compressed file (upgradetools.zip or upgradetools.tar) that you download and install on the Tivoli server. Each tool is a Tivoli command that you can run from any directory on the Tivoli server after you install the toolkit and set up the Tivoli environment variables.

Although you can install the upgrade toolkit from either the Tivoli command line or the Tivoli desktop, the upgrade tools can be run only from the command line. There is no equivalent function for the Tivoli desktop.

Table 5-1 shows the common names that are used to refer to each tool, each tool's command name, and a description of what the tool does. For more information you can refer to *IBM Tivoli Monitoring Version 6.2.0, Upgrading from Tivoli Distributed Monitoring*, GC32-9463.

Table 5-1 The upgrade tools for upgrading from Tivoli Distributed Monitoring

Name of tool	Command	What the tool does
Scan tool	**witmscantmr**	The *Scan tool* collects information about the Tivoli infrastructure components (Tivoli server, gateways, and endpoints) where Tivoli Distributed Monitoring is installed or running. It uses this information to create an output data file that maps the Tivoli components to a proposed IBM Tivoli Monitoring infrastructure that is capable of handling the same monitoring load. You can use the output data file as a road map for deploying the IBM Tivoli Monitoring infrastructure. Besides creating an initial road map, the Scan tool also creates status reports that show the progress of the infrastructure upgrade.
Assess tool	**witmassess**	The *Assess tool* collects Tivoli Distributed Monitoring data from endpoints, profiles, or profile managers that you want to upgrade. It uses this information to create an output data file or files that map the collected data to the monitoring elements used by IBM Tivoli Monitoring. (For example, the output data file for a profile assessment specifies an equivalent situation for each monitor threshold.) The output data files from the Assess tool are used as input to the Upgrade tool.

Name of tool	Command	What the tool does
Upgrade tool	**witmupgrade**	The *Upgrade tool* deploys the monitoring elements (monitoring agents, situations, or managed system lists) specified in the output file from the Assess tool. You can also use the Upgrade tool to undo (roll back) an upgrade and to disable (clean up) monitors that have been upgraded.

5.1.1 The witmscantmr command

The **witmscantmr** command creates either a baseline file or a status report. The baseline file maps the infrastructure components of a Tivoli management region to a proposed equivalent Tivoli Monitoring Services infrastructure. The status report validates the upgrade of Tivoli infrastructure components. The command syntax is:

```
witmscantmr { –c | –v [ –f baseline ] | –? }
```

You can use the **witmscantmr** command for two purposes:

- At the beginning of the upgrade process, run the **witmscantmr** command with the **–c** option to create a baseline file. The baseline file is an XML output file that maps the infrastructure elements of a Tivoli management region to a proposed equivalent IBM Tivoli Monitoring infrastructure layout. For example, the Tivoli server is mapped to one or more hub Tivoli Enterprise Monitoring Servers, Tivoli gateways are mapped to remote monitoring servers, and so on. Edit the baseline file to specify and change details of the IBM Tivoli Monitoring deployment.
- Run the **witmscantmr** command with the **–v** option after you have deployed some or all of the IBM Tivoli Monitoring components to validate the deployment. Each time that you run the **witmscantmr** command with the **–v** option, the edited baseline file is used as input. The **witmscantmr** command does not change the baseline file, but instead, it produces a separate output file. The output file is identical to the baseline file except that attributes within the file are updated to show the status of the deployment. You can think of the output file as a status report.

Table 5-2 on page 144 shows the options for the **witmscantmr** command.

Table 5-2 Options for the witmscantmr command

Option	Description
-c	Creates a default baseline file named *tmroid.xml*, where tmroid is the object identifier of the Tivoli management region (for example, 1505093874.xml). The baseline file is created in the following directory on the Tivoli server: *$DBDIR*/AMX/shared/analyze/scans where *$DBDIR* is the path name of the Tivoli object database directory.
-v	Creates a data file that shows the status of the infrastructure upgrade, using either the default baseline file or a specified baseline file as input. If the **–f** option is omitted, the command uses the default baseline file as input. The default baseline file is the file that was created with the **–c** option. Use the **–f** option to specify a different baseline file. For example, if you renamed the default baseline file, use the **–f** option to specify the renamed file. The output file that shows the status of the infrastructure upgrade is named baseline_timestamp.xml, where baseline is the name of the baseline file used as input and timestamp is a time stamp that indicates when the output file was created. The time stamp specifies the year, month, day, hour, minute, and second in that order in the following format: *yyyy_mm_dd_hh_mm_ss* The output file is written to the following directory on the Tivoli server: *$DBDIR*/AMX/shared/analyze/scans where *$DBDIR* is the path name of the Tivoli object database directory.
–f *baseline*	Specifies the baseline file to use with the **–v** option. If you do not specify the **–f** option with the **–v** option, the command uses the default baseline file.
–?	Prints the usage description for this command.
-c	Creates a default baseline file named tmroid.xml, where tmroid is the object identifier of the Tivoli management region (for example, 1505093874.xml). The baseline file is created in the following directory on the Tivoli server: *$DBDIR*/AMX/shared/analyze/scans Where *$DBDIR* is the path name of the Tivoli object database directory.

Examples of using the **witmscantmr** command include:

- The following example creates the default baseline file:

```
witmscantmr -c
```

- The following example creates a status report using the default baseline file as input:

```
witmscantmr -v
```

- The following example creates a status report using a baseline file, which is named baseline.xml, as input. In this example, the command is issued one directory higher than the scans directory:

```
witmscantmr -v -f scans/baseline.xml
```

5.1.2 The witmassess command

The **witmassess** command prepares for an upgrade by collecting data about Tivoli-managed resources to be upgraded (endpoints, profiles, and profile managers) and mapping the Tivoli resources to equivalent resources for the IBM Tivoli Monitoring environment.

The **witmassess** command (also referred to as the *Assess tool*) collects Tivoli Distributed Monitoring data from endpoints, profiles, or profile managers that you want to upgrade. It uses this information to create an output data file or files that map the collected data to the monitoring elements used by IBM Tivoli Monitoring. The output data files from the **witmassess** command are used as input to the **witmupgrade** command (also referred to as the *Upgrade tool*). The **witmupgrade** command deploys the monitoring elements (monitoring agents, situations, or managed system lists) specified in the output files from the **witmassess** command. You can edit the output from an assessment before proceeding to upgrade.

The **–e**, **–p**, and **–pm** options specify the Tivoli Distributed Monitoring resources to be assessed: **–e** for endpoints, **–p** for profiles, and **–pm** for profile managers. Use the **–a** option in combination with any of these options to limit the assessment to specific applications.

The **witmassess** command performs assessments that are independent of any previous assessments. For example, an assessment of a profile manager (using the **–pm** option) includes an assessment of the endpoints that subscribe to the profile manager and the profiles that are contained in the profile manager. However, the assessment does not obtain data from any previous assessments of endpoints or profiles.

The syntax of the **witmassess** command follows, with the options in Table 5-3 on page 146:

```
witmassess { [–pm pm –pm . . . ] [ –p prf –p . . . ] [ –e ep –e . . . ]
| –r resfile } [ –a app –a . . . ] [ –f baseline –f . . . ] [ –o flags
] | [ –? ]
```

Table 5-3 Options for the witmassess command

Option	Description
–e ***ep*** **–e ...**	Specifies the endpoints to assess. For each endpoint, specify the **–e** option with the name (label) of the endpoint. In an assessment of endpoints, the **witmassess** command determines which monitoring agents are needed for the applications (including the operating system) that reside on the specified endpoints. The labels of the monitoring agents for supported applications are written to the output files from the assessment. (There is one output file for each specified endpoint.) When you upgrade the endpoints, the **witmupgrade** command deploys the monitoring agents listed in the output files. Use the **–a** option in combination with the **–e** option to limit the assessment to specific types of applications.
–p ***prf*** **–p ...**	Specifies the profiles to assess. For each profile, specify the **–p** option with the name of the profile. In an assessment of profiles, the **witmassess** command creates output files that map the Tivoli Distributed Monitoring monitors in a profile to IBM Tivoli Monitoring situations. (There is one output file for each specified profile.) A separate situation is defined for each monitor threshold. When you upgrade the profiles, the **witmupgrade** command creates the situations listed in the output files from the assessment. Use the **–a** option in combination with the **–p** option to limit the assessment to monitors for specific applications.
–pm ***pm*** **–pm ...**	Specifies the profile managers to assess. For each profile manager, specify the **–pm** option with the name of the profile manager. In an assessment of profile managers, the **witmassess** command assesses the following managed resources for each profile manager: ► The endpoints that subscribe to the profile manager: The assessment of endpoints determines the required monitoring agents for each endpoint (in the same way as described for the **–e** option). ► The profiles that are contained in the profile manager: The assessment of profiles maps Tivoli Distributed Monitoring monitors to IBM Tivoli Monitoring situations (in the same way as described for the **–p** option). ► The subscriber list for the profile manager: The assessment of the Tivoli Distributed Monitoring subscriber list maps the subscriber list to an IBM Tivoli Monitoring managed system list. The results of the assessment are written to output files, and there is one output file for each specified profile manager. The output data defines the relationship among the monitoring agents, situations, applications (managed systems), and managed system list. When you upgrade the profile managers, the **witmupgrade** command deploys the resources listed in the output files from the assessment. The **–p** and **–e** options act as filters when specified with the **–pm** option. Only the resources specified by the **–p** and **–e** options are included in the final results. Use the **–a** option in combination with the **–pm** option to limit the assessment to specific types of applications.

Option	Description
–r ***resfile***	Specifies a text file that lists the resources to assess. Only the endpoint, Tivoli Distributed Monitoring profile, and profile manager resource types are allowed. Each entry in the file must be on a separate line. Each entry has the following format: *@Class:Instance#region* Where *Class* specifies the resource type. The choices are: ► *Instance*: Specifies the name or label of a particular resource. ► *region*: Specifies the object identifier (OID) of the Tivoli management region where the resource resides.
–a ***app*** **–a ...**	Limits the assessment to the specified operating systems or applications. For each operating system or application, specify the **–a** option with the name of the monitoring collection for that operating system or application. The **–a** option is used in conjunction with at least one of the assessment options (**–e**, **–p**, **–pm**, or **–r**) and acts as a filter on those options. If the **–a** option is omitted, all operating systems and applications are assessed for the resources specified with the assessment options.
–f ***baseline*** **–f ...**	Specifies the infrastructure data files to use as input. If the **–f** option is omitted, the **witmassess** command uses the default baseline file named tmroid.xml, where tmroid is the object identifier of the Tivoli management region (for example, 1505093874.xml). The default baseline file is located in the following directory on the Tivoli server: *$DBDIR*/AMX/shared/analyze/scans where *$DBDIR* is the path name of the Tivoli object database directory.
–o ***flags***	Specifies flags that affect the behavior of the **witmassess** command. You can use the **flatten** flags.
–?	Prints the usage description for this command.

The **witmassess** command creates a separate XML output file for each specified resource to be assessed. The name of the output file is the name of the endpoint, profile, or profile manager with an .xml extension. The output files are created in the following directories on the Tivoli server:

- *$DBDIR*/AMX/shared/analyze/endpoints
- *$DBDIR*/AMX/shared/analyze/profiles
- *$DBDIR*/AMX/shared/analyze/profilemanagers

where *$DBDIR* is the path name of the Tivoli object database directory.

Examples of using the **witmassess** command include:

- The following example assesses the endpoints named EP1 and EP2 and uses the default baseline file as input:

  ```
  witmassess -e EP1 -e EP2
  ```

  The **witmassess** command determines the operating system and supported applications on each endpoint. The output files from this command, EP1.xml and EP2.xml, specify the monitoring agents to be deployed to the endpoints when they are upgraded (using the **witmupgrade** command).

- The following example assesses the endpoints listed in the resource file named endpoint_list.txt:

  ```
  witmassess -r endpoint_list.txt -a Unix_Sentry
  ```

  The **-a** option in this example specifies the Unix_Sentry monitoring collection, which limits the assessment to the UNIX endpoints listed in the ep_list.txt file.

5.1.3 The witmupgrade command

The **witmupgrade** command deploys IBM Tivoli Monitoring resources based on specifications in the data output files from the **witmassess** command. The **witmupgrade** command (also referred to as the *Upgrade tool*) deploys the monitoring agents, situations, or managed system lists specified in the output files from the **witmassess** command. You can also use the Upgrade tool to undo (roll back) an upgrade and to disable (clean up) monitors that have been upgraded.

Unlike the **witmassess** command, which has no knowledge of previous assessments, the **witmupgrade** command does not attempt to redeploy any resources that have already been deployed.

The syntax of the **witmupgrade** command follows with the options in Table 5-4 on page 149:

```
witmupgrade { [–x datafile –x . . . | –d directory ] {–u | –r | –c } [
–f baseline ] | –? }
```

Table 5-4 Options for the witmupgrade command

Option	Description
–x ***datafile*** **–x ...**	Specifies the output data files from the **witmassess** command to use as input to the **witmupgrade** command. If the **–x** option and the **–d** option are both omitted, the command uses files contained in the following default locations: *$DBDIR*/AMX/shared/analyze/endpoints *$DBDIR*/AMX/shared/analyze/profiles *$DBDIR*/AMX/shared/analyze/profilemanagers *$DBDIR* is the path name of the Tivoli object database directory.
–d ***directory***	Specifies a directory that contains the output data files from the **witmassess** command to use as input to the **witmupgrade** command. If the **–x** option and the **–d** option are both omitted, the command uses files contained in the following default locations: *$DBDIR*/AMX/shared/analyze/endpoints *$DBDIR*/AMX/shared/analyze/profiles *$DBDIR*/AMX/shared/analyze/profilemanagers *$DBDIR* is the path name of the Tivoli object database directory.
-u	Upgrades the resources that are defined in the data files specified with the **–x** or **–d** option, or if neither option is specified, upgrades the resources in all data files that reside in the default locations.
-r	Rolls back the upgrade of resources defined in the data files specified with the **–x** or **–d** option.
-c	Disables the monitors defined in the data files specified with the **–x** or **–d** option: ► For each data file that resulted from the assessment of an endpoint, the **–c** option disables all monitors on the endpoint. ► For each data file that resulted from the assessment of a profile, the **–c** option disables all monitors in the profile. ► For each data file that resulted from the assessment of a profile manager, the **–c** option disables all monitors in each profile that is contained in the profile manager, and it disables all monitors running on all endpoints that subscribe to the profile manager. If you want to enable the monitors again, use the **wenblprb** command to enable the monitors and then redistribute the profiles that contain the monitors.
–f ***baseline ...***	Specifies one or more baseline files to use as input. (A baseline file is the output file from using the **witmscantmr** command with the **–c** option.) The baseline file identifies the Tivoli Enterprise Monitoring Server to which the upgraded monitoring elements are assigned. If the **–f** option is omitted, the **witmassess** command uses the default baseline file named tmroid.xml, where tmroid is the object identifier of the Tivoli management region (for example, 1505093874.xml). The default baseline file is located in the following directory on the Tivoli server: *$DBDIR*/AMX/shared/analyze/scans *$DBDIR* is the path name of the Tivoli object database directory.
–?	Prints the usage description for this command.

The output files from the **witmassess** command are used as input files to the **witmupgrade** command. For each input file, the **witmupgrade** command creates a corresponding output file. Each input and output file pair represents an endpoint, profile, or profile manager to be upgraded. View the output files from the **witmupgrade** command to verify that the mapped IBM Tivoli Monitoring resources (monitoring agents, situations, and managed system lists) have been successfully deployed.

The name of each output file is the name of the endpoint, profile, or profile manager that was upgraded in the following format: resource_timestamp.xml. The output files are created in the following directories on the Tivoli server:

- *$DBDIR*/AMX/shared/analyze/endpoints/upgrade
- *$DBDIR*/AMX/shared/analyze/profiles/upgrade
- *$DBDIR*/AMX/shared/analyze/profilemanagers/upgrade

$DBDIR is the path name of the Tivoli object database directory.

Examples of using the **witmupgrade** command include:

- The following example upgrades all resources defined in the data files that reside in the default locations, using the default baseline file:

  ```
  witmupgrade -u
  ```

- The following example disables all monitors defined in the data files that reside in the default locations:

  ```
  witmupgrade -c
  ```

  Note: If you want to enable the monitors again, use the **wenblprb** command to enable the monitors and then redistribute the profiles that contain the monitors.

- The following example upgrades the monitors contained in the myProfile.xml data file, using the default baseline file. The myProfile.xml data file is the output file from using the **witmassess** command to assess the profile named myProfile:

  ```
  witmupgrade -x /tmp/myProfile.xml -u
  ```

- The following example rolls back the upgrade of all resources defined in the data files that reside in the /tmp/upgradefiles directory, using the baseline file contained in the /tmp/baseline directory:

  ```
  witmupgrade -d /tmp/upgradefiles -r -f /tmp/baseline/mybaseline.xml
  ```

5.1.4 The witmmtk command

IBM Tivoli Monitoring also provides the IBM Tivoli Monitoring Migration Toolkit: V5.1.2 to V6.2, to upgrade from IBM Tivoli Monitoring V5.1.2 to IBM Tivoli Monitoring V6.2.

You must install the toolkit on the Tivoli management region server and every managed node gateway with endpoints that you want to migrate. The installation can be performed using Tivoli commands, the Tivoli desktop, or remote installation software, such as the Software Distribution component of IBM Tivoli Configuration Manager. For more information you can refer to *IBM Tivoli Monitoring Version 6.2.0, Upgrading from IBM Tivoli Monitoring V5.1.2*, GC32-1976.

The **witmmtk** is the umbrella command for the toolkit. It is only used in association with one of the subcommands. Use the **witmmtk** command to run one of the migration toolkit subcommands. You issue each subcommand as:

```
witmmtk sub-command
```

Table 5-5 lists the **witmmtk** command and the subcommands. The subcommands are listed here in the order in which they are normally used during a migration. In the pages that follow, they are listed in alphabetical order.

Table 5-5 Migration commands

Command	Subcommand	Purpose
witmmtk	**javapath**	Specifies the location of the prerequisite Java software required by the migration tools.
	scantmr	Creates or updates the baseline data file that maps the infrastructure components of a Tivoli management region to a proposed equivalent Tivoli Monitoring Services infrastructure. When used with an existing baseline file, it validates the data that you have added and calculates the overall migration progress.
	lock	Locks the toolkit commands when you want to edit the infrastructure baseline file, or one of the assess files, with a text or XML editor.
	unlock	Unlocks the toolkit commands after a **lock** command was used.

Command	Subcommand	Purpose
witmmtk	**setpwd**	Stores the access credentials (user ID and password) of any object in the baseline file created by a previous **scantmr** command, or of any password required as a *UserSetting* in an endpoint assess file created by a previous **assess** command.
	encpwd	Encrypts any passwords that have been stored manually in the baseline infrastructure file or any endpoint assess file.
	assess	The **assess** command (also referred to as the *Assess tool*) collects V5.1.2 data from endpoints, profiles, or profile managers that you want to migrate. It uses this information to create an output data file or files that map the collected data to the monitoring elements used by V6.2. The output data files from the **assess** command are used as input to the **migrate** command (also referred to as the *Migrate tool*). The **migrate** command deploys the monitoring elements (monitoring agents, situations, or managed system lists) specified in the output files from the **assess** command. You can edit the output from an assessment before proceeding to migrate.

Command	Subcommand	Purpose
witmmtk	**migrate**	Deploys V6.2 resources based on specifications in the data output files from the **assess** command. It can also be used to roll back the migration of selected V6.2 resources and to clean up (remove) selected resources in the V5.1.2 environment when you no longer need them.
	trace	Sets the tracing on or off for the toolkit subcommands.

Examples of using the **witmmtk** command include:

- The following command runs the **encpwd** subcommand:

  ```
  witmmtk encpwd
  ```

- The following command displays the usage of the **javapath** subcommand:

  ```
  witmmtk javapath –?
  ```

5.2 Configuring IBM Tivoli Monitoring components

Although the majority of configuration is done during the product installation, you can use the Manage Tivoli Enterprise Monitoring Services utility to configure components at any time. You can also use the Manage Tivoli Enterprise Monitoring Services tool to start and stop components.

5.2.1 Starting Manage Tivoli Enterprise Monitoring Services: Windows

To start Manage Tivoli Enterprise Monitoring Services on a computer running Windows, click **Start** → **Programs** → **IBM Tivoli Monitoring** → **Manage Tivoli Monitoring Services**.

5.2.2 Starting Manage Tivoli Enterprise Monitoring Services for Linux and UNIX

Use the following steps to start Manage Tivoli Enterprise Monitoring Services on a computer running Linux or UNIX:

1. Change to the bin directory:

   ```
   cd install_dir/bin
   ```

2. Run the following command:

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

   where:

   -h (Optional) An option used to specify the installation directory.

   install_dir The installation directory for IBM Tivoli Monitoring.

   -s (Optional) An 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 previous commands with **-?** displays the syntax for using the **-s** option.

   The Manage Tivoli Enterprise Monitoring Services utility opens.

5.2.3 Changing the configuration of Tivoli Enterprise Monitoring Server

You can change the basic configuration of the monitoring server through Manage Tivoli Enterprise Monitoring Services. Use the following steps:

1. In the Manage Tivoli Enterprise 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, which enables you to set up backup communication methods. If the method that you identify as Protocol 1 fails, Protocol 2 is used. Click **OK**.
4. Complete the communications protocol fields for the monitoring server and click **OK**.
5. Restart the monitoring server.

Note: On Linux and UNIX, you can also use the **`itmcmd config -S`** command to change the configuration of a monitoring server.

5.2.4 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 will use when connecting to the monitoring server. Setting network interfaces affects all of the components that are installed on the local computer.

To specify the network interfaces to use 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:

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 that 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.

Note: This specifying network interfaces feature in the Linux or Unix environment is equivalent to “network name”.

5.2.5 User options

You can edit the font size and color user options through the Manage Tivoli Monitoring Services component on a Windows platform.

5.2.6 Starting and stopping components

You can start and stop the IBM Tivoli Monitoring components from Manage Tivoli Enterprise Monitoring Services. Use the following steps:

1. Right-click the component (such as a specific agent or Tivoli Enterprise Portal Server) that you want to start or stop.
2. Click **Start**, **Stop**, or **Recycle** (Windows only) from the menu.
3. Click **Actions** from the main menu, and click **Stop**, **Start**, or **Recycle**.

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.

5.2.7 Configuring user authentication on the hub monitoring server

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 must not contain spaces.
   e. Click **OK** and then click **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.
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, which 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 Lightweight Directory Access Protocol (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. Click **OK**.

      If you have selected the LDAP option, Figure 5-1 on page 159 is displayed.
4. Specify the following values, as required for your site, and then click **OK**:
   a. **LDAP user filter**
      The LDAP user filter maps Tivoli Enterprise Portal user IDs to LDAP login IDs.
   b. **LDAP base**
      The LDAP base is used in searches for your LDAP server. Your LDAP administrator provides this value.
   c. **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.
   d. **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.
   e. **LDAP port name**
      The LDAP server port number. This value can be omitted if your LDAP server is listening on port 389.
   f. **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.)

g. **LDAP SSL Communications: Use SSL?**
Specifies that Secure Sockets Layer (SSL) communications will be used to communicate with the LDAP server. If SSL is enabled, enter values for:

- **LDAP key store file**
The location of the IBM Global Security Tool Kit (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.

h. Click **OK** to accept the current settings.

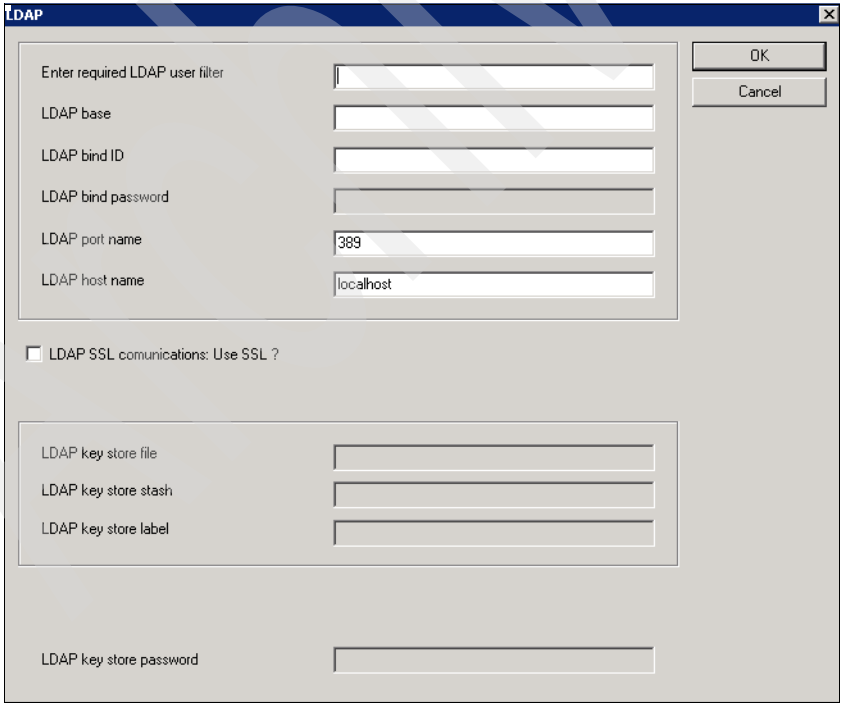


Figure 5-1 LDAP configuration window

5. In the Manage Tivoli Monitoring Services window, restart the hub monitoring server by right-clicking its name and selecting **Start**.

5.2.8 Creating a user on Tivoli Enterprise Portal

Use the following steps to create a user on Tivoli Enterprise Portal:

1. In Tivoli Enterprise Portal, click **Edit** → **Administer Users**.
2. Click **Create New User**.
3. Type a user ID, user name, and optional description for the user.
4. Click **OK**, and then, click **OK** again to close the window.

You can also enable user security in your monitoring environment by creating a matching user ID with password to the network domain user accounts or to the operating system where the hub monitoring server resides:

- User Accounts on Windows
- Password file on UNIX
- RACF® or ACF/2 host security system on OS/390® or z/OS

5.2.9 Configuring failover support

The optional Hot Standby feature enables you to maintain continuous 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.

There is no automatic switch that returns control to the hub monitoring server when it is available. If you want to switch back to the hub monitoring server, you must manually stop the backup monitoring server. Configuring the Hot Standby feature involves the following steps:

1. Install the hub and backup hub monitoring servers at the same time.
2. Add application support on the backup hub monitoring server.
3. Configure the Hot Standby feature on the monitoring server.
4. Configure the agents.
5. Verify that the failover support works.

5.2.10 Adding application support to backup hub monitoring server

If you are installing the hub and backup monitoring servers at the same time, you can add normal application support, either through the Windows installation program or by running the **itmcmd support** command on Linux or UNIX monitoring servers. If you add additional applications to your monitoring environment, add the support for these applications to both monitoring servers and restart the servers.

However, if you have previously installed your hub monitoring server and are now setting up failover support, the two monitoring servers might not be in sync if you add the default application support to the backup monitoring server during the installation. Any changes that you made to situations on the hub monitoring server are not replicated on the backup monitoring server. To address this issue, use the following steps to add applications support to your backup monitoring server.

For a Windows backup monitoring server, install the monitoring server using the installation program. When you come to the step to add application support, click **Cancel** instead of OK. When your installation is complete, start the backup monitoring server. The backup monitoring server connects to the hub monitoring server and automatically synchronizes with it.

For a Linux or UNIX backup monitoring server, install and configure the monitoring server using the **itmcmd support** command:

```
./itmcmd support -m -t tems_name pc pc pc
```

The **-m** parameter copies the support files to the monitoring server without adding it. When you are finished, start the backup monitoring server. The backup monitoring server connects to the hub monitoring server and automatically synchronizes with it.

After the initial configuration of your backup monitoring server, if you add an application to the hub monitoring server, you can add application support to both monitoring servers at the same time.

5.2.11 Configuring the Hot Standby feature on monitoring servers

Use the following steps to configure monitoring servers for the Hot Standby feature. You must configure the hub server, the standby hub server, and any remote servers that are associated with the hub server to make them aware of the backup topology.

Note: The hub and backup monitoring servers need to be configured as mirrors of each other.

The steps are:

1. In Manage Tivoli Enterprise Monitoring Services, right-click the name of the hub monitoring server and click **Reconfigure** (on Windows) or **Configure** (on UNIX).

   On Windows:

   a. Select **Configure Standby TEMS**.

   b. Enter the name of this monitoring server and specify the protocols that are used by the standby server. These protocols must be the same for both monitoring servers (the hub and the standby).

   c. Click **OK**.

   d. Enter the host name or IP address for the hub monitoring server and click **OK** in the window that displays the communication settings for this server.

   e. Enter the host name or IP address for the standby monitoring server in the Hostname or IP Address field and click **OK**.

   On UNIX:

   a. Select the **Advanced Settings** tab.

   b. Select **Specify Hot Standby**.

   c. Enter the host name for the backup monitoring server in the Standby TEMS Site field.

   d. Select the type of protocol to use for Hot Standby, which needs to be the same protocol on both the hub monitoring server and the monitoring server that you are going to use for failover support.

   e. If you specified any backup protocols for the hub monitoring server, identify identical protocols for the backup monitoring server.

   f. Click **Save**.

2. Stop and restart the monitoring server. (On Windows, the monitoring server stops automatically.)

3. Repeat these steps for the backup monitoring server and any remote monitoring servers.

5.2.12 Configuring agents

Agents use a feature called *secondary Tivoli Enterprise Monitoring Server* to ensure their availability. If the monitoring server to which the agent connects is unavailable, the agent switches to the defined secondary monitoring server. Use the following steps to configure a secondary Tivoli Enterprise Monitoring Server for any agents that connect to the hub monitoring server:

1. In Manage Tivoli Enterprise Monitoring Services, right-click an agent and click **Reconfigure** (on Windows) or **Configure** (on UNIX).
2. Select **Optional: Secondary TEMS Connection** and specify the protocol for the backup monitoring server. On UNIX agents, click **Protocols** to display the window where you configure secondary Tivoli Enterprise Monitoring Server.
3. Click **OK**.
4. Enter the host name or IP address for the hub monitoring server (if you have not already) and the port number, and click **OK**.
5. Enter the host name or IP address for the secondary monitoring server and click **OK**.
6. Restart your agent.

5.2.13 Verifying that failover support works

To verify that the failover support that is provided by the Hot Standby feature works, take your hub monitoring server off-line by stopping its servers in Manage Tivoli Enterprise Monitoring Services. When the hub monitoring server stops, reconfigure Tivoli Enterprise Portal Server to point to the backup monitoring server and restart the portal server. Open **Tivoli Enterprise Portal**. If everything is configured correctly, you can open the portal and view data.

5.2.14 Using Manage Tivoli Enterprise Monitoring Services to add application support to a monitoring server

Use the following steps to add application support to the monitoring server:

1. Right-click the monitoring server to which you want to add application support.
2. Click **Advanced** → **Add TEMS Application Support**.
3. Specify the location of the monitoring server and click **OK**:
   - On this computer
   - On another computer

4. If you selected a monitoring server on another computer, provide the Tivoli Enterprise Monitoring Server Node ID and communications protocol to use to communicate with the monitoring server. Click **OK**.

   Note: To view the Node ID, right-click the monitoring server name and click **Browse Settings**.

5. Select the products for which you want to add application support. Click **Select All** to choose all available products. Click **OK**.
6. When the process completes, a message is displayed containing information about the procedure. Click **Close**.
7. If the monitoring server is not already stopped, stop it.
8. Restart the monitoring server.

5.2.15 Using the itmcmd support command to add application support to a Linux or UNIX monitoring server

Use the following steps to add application support to a Linux or UNIX monitoring server from the command line:

1. If the monitoring server is not running, run the following command to start it:

   `./itmcmd server start` *`tems_name`*

   where *`tems_name`* is the name of the monitoring server.

2. Run the following command to add the application support:

   `./itmcmd support [-h` *`install_dir`*`] [-s] -t` *`tems_name pc pc pc pc ...`*

   where:

`-h`	(Optional) Parameter to specify the installation directory if it is not the directory in which this script is located. This parameter is usually unnecessary. Also, use this option to take action on an installation directory other than this one.
`install_dir`	The home directory that you created for IBM Tivoli Monitoring.
`-t`	Use this required option to specify the monitoring server name.
`tems_name`	Specifies the name of the monitoring server that you are configuring. This argument is required. Note that the monitoring server must be specified within the structure of ***`install_dir`***.

pc The product code of the product that will connect to this monitoring server. You can specify one or more products for which to add application support. If you are specifying multiple products, you must separate the product codes with either a space or comma as illustrated earlier.

3. Run the following command to stop the monitoring server:

   ```
   ./itmcmd server stop tems_name
   ```

4. Restart the monitoring server by running the following command:

   ```
   ./itmcmd server start tems_name
   ```

5.3 IBM Tivoli Data Warehouse

The new IBM Tivoli Data Warehouse V2.1 has two new processes that collect, summarize, and prune data that is gathered from IBM Tivoli Monitoring V6.2 agents. There is a new Warehouse Proxy agent that is the new data warehouse server. The Warehouse Proxy agent collects data from the IBM Tivoli Monitoring V6.2 agents and stores the data in a relational database (DB2, Oracle, or Microsoft SQL). You can optionally configure the Tivoli Data Warehouse V2.1 data to summarize and prune the historical data with another new process called the *Summarization and Pruning Agent*.

5.3.1 Configuring the Warehouse Proxy agent

The Warehouse Proxy agent is configured to connect to the database in order to insert and retrieve data from the database. The following steps show you how to perform the Warehouse Proxy agent configuration:

1. From the Manage Tivoli Enterprise Monitoring Services console, right-click the Warehouse Proxy and select **Reconfigure**.
2. Click **OK**.
3. Configure the protocol communication between Tivoli Enterprise Monitoring Server and the Warehouse Proxy and click **OK**.
4. Configure the hub Tivoli Enterprise Monitoring Server host name and the ports on which the Warehouse Proxy will connect and click **OK**.
5. Click **OK** when you receive the pop-up window shown in Figure 5-2 on page 166.

Figure 5-2 Warehouse Proxy ODBC configuration confirmation

6. Select the database type to be used for the Warehouse Proxy datasource, as shown in Figure 5-3.

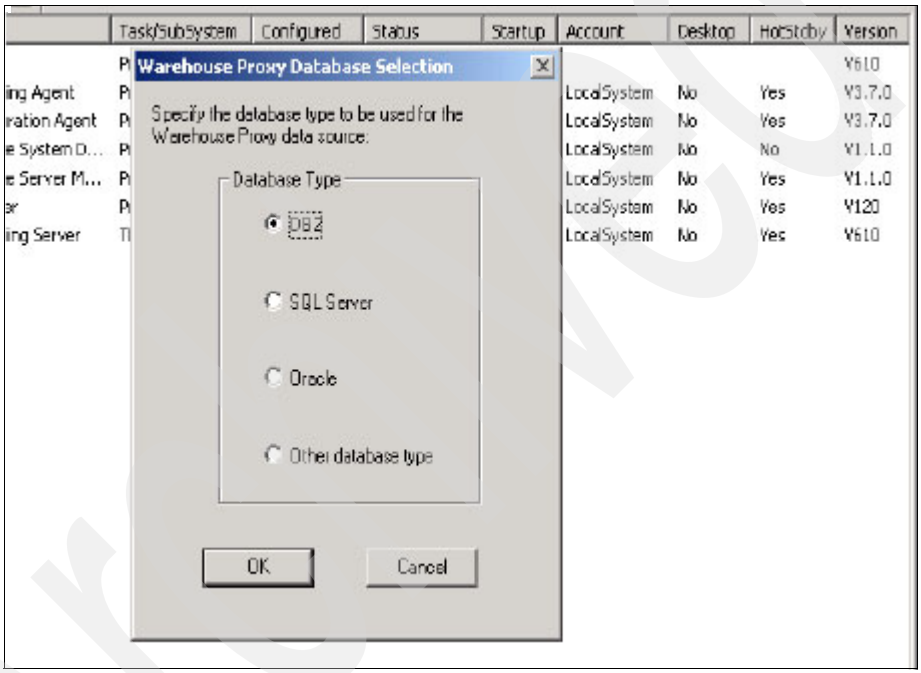


Figure 5-3 Database selection for Warehouse Proxy configuration

7. Fill in the following fields (see Figure 5-4 on page 167):
   - Data Source Name: Leave it as `ITM Warehouse`.
   - Database Name: Enter the name of the database that the Warehouse Proxy agent will use to store the data.
   - Admin User ID: Enter the database user administrator user ID, which was created during database installation (the default is `db2admin` for DB2).
   - Admin Password: Enter the user database administrator password.

– Database User ID: Enter the user ID that will own the table created to store warehouse data. This user must be created on the OS first; the default user is `ITMUser`.
– Database Password: Enter the password of the database user ID.
– Reenter Password: Enter the password again and click **OK**.

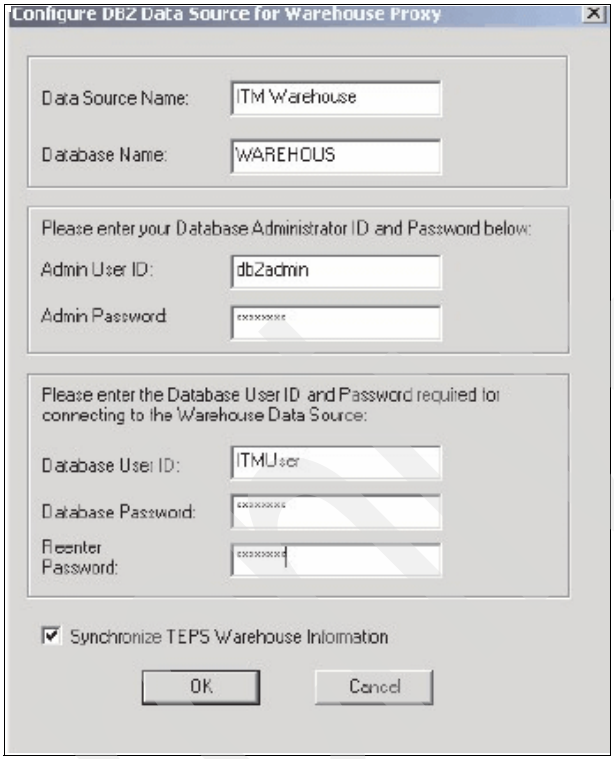


Figure 5-4 Data Source configuration window for Warehouse Proxy

Note: After completing this step, the database and the associated tables are created in your database.

8. Click **OK** in the next pop-up window stating that the Data Warehouse was successfully completed.
9. Click **Yes** in the next window to complete the configuration.
10. Restart the Warehouse Proxy agent by double-clicking it.

Important: You can change the default ODBC datasource name using the following procedure:

- Edit the windows registry regedit.

  Under the registry key:

  HKEY_LOCAL_MACHINE\SOFTWARE\CANDLE\KHD\Ver610\Primary\Environment

- Double-click the string **ODBCDATASOURCE** and enter the ODBC datasource name of your choice.
- The khdxprto.exe is the process name for the Warehouse Proxy agent running on Windows.

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 in the list. Use the environment variable KHD_WAREHOUSE_TEMS_LIST to specify a list of monitoring servers to associate to a Warehouse Proxy agent.

5.3.2 Configuring the Warehouse Summarization and Pruning Agent

When IBM Tivoli Monitoring V6.2 is installed, the Summarization and Pruning Agent can be configured with default values. The default values that are set during the installation of the Summarization and Pruning Agent can be used as the default values for all of the agent default attribute groups. If the Summarization and Pruning Agent scheduled summarization and pruning process (that is, the once per day process) has not run for the first time, the defaults for all agent default attribute groups can be reconfigured. We recommend that you do *not* start and schedule the Summarization and Pruning Agent before the first time that defaults are configured.

You can reconfigure the Summarization and Pruning Agent settings from the Management Tivoli Enterprise Monitoring Services console.

Figure 5-5 on page 169 is an example of the Summarization and Pruning Agent default settings panel.

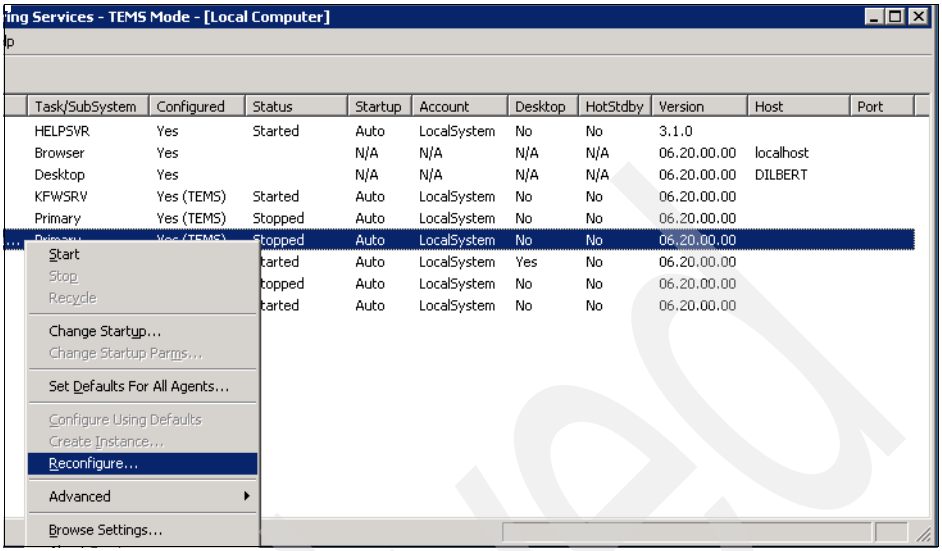


Figure 5-5 Summarization and Pruning Agent configuration

If the scheduled summarization and pruning process has never run, the values can be reconfigured and will be used by all of the agent default attribute groups, as shown in Figure 5-6 on page 170.

Note: If you want to reapply default settings for an agent that has already had summarization and pruning performed on it, delete the ksy.k<*pc*>.installed file where <*pc*> is the 2-letter product code for the agent:

- On a Windows system: install_dir\tmaIBM Tivoli Monitoring6\logs directory
- On a UNIX or Linux system: install_dir\logs directory

The panel in Figure 5-6 on page 170 contains the following fields:

- Apply settings to the default tables for all agents

  If this option is selected, all of the agent default attribute groups will inherit the defaults specified on this panel. After the summarization and pruning scheduled run has completed, changes to this panel will not affect the agent default attribute group settings.

- Collection Interval

  The *collection interval* sets the default time to collect data in the binary files. The location of the binary files depends on the collection location setting. The default 5 minute value might be a little low for all default attribute groups.

- Collection Location

  This is the default location for storing the binary files. We recommend that whenever possible that you select **TEMA** (that is, at the agent).

- Warehouse Interval

  This is the interval that the Tivoli Enterprise Monitoring agent or Tivoli Enterprise Monitoring Server binary data will be uploaded to the Warehouse Proxy agent. The options are 1 hour and daily. For environments with a lot of agents, we recommend that you select **1 hour** instead of daily.

- Summarization settings

  These options enable you to select the summarization tables that will be created in Tivoli Data Warehouse and used for aggregation.

- Pruning settings

  This field sets the length of time to keep data in the Tivoli Data Warehouse. Data older than the prune settings will be removed from Tivoli Data Warehouse.

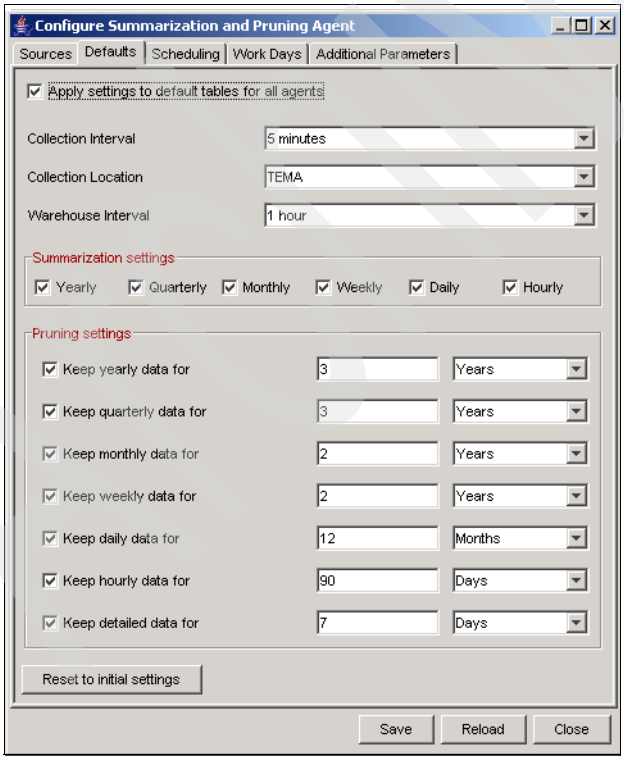


Figure 5-6 Summarization and Pruning Agent defaults configuration panel

Figure 5-7 shows the Summarization and Pruning Agent Scheduling tab configuration panel.

The panel in Figure 5-7 contains the following fields:

- Run every

  This option sets the daily cycle time. The default is 1 day. However, it can be set to run every 7 days. We recommend that you set the summarization and pruning run to happen every day.

- at

  This value is the time the summarization and pruning run is scheduled every day. The default is 02:00 am.

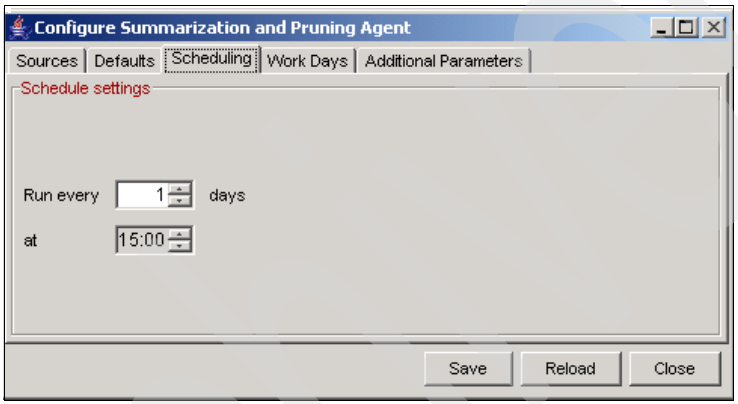


Figure 5-7 Summarization and Pruning Agent Scheduling tab configuration panel

Selecting the Work Days tab opens the panel that is shown in Figure 5-8 on page 172.

The panel in Figure 5-8 on page 172 contains the following fields:

- Week starts on

  If shift data is used, this sets the start day of the week.

- Specify shifts

  This option enables you to set peak and off-peak shifts. If you select this option, two additional records will be created for each attribute group in the summary tables. Because all data is aggregated (that is, rolled up) from the detail, there will be three summary records for each interval of an instance.

For example, the NT_Memory_D will have three records for each day for:

- One summarized record for all hours in the day
- One summarized record for off-peak hours per day
- One summarized record for peak hours per day

- Specify vacation days

  Additional historical data can be summarized based on vacation day settings.

Note: Changing the shift information after data has been summarized can create an inconsistency in the data. Previous data collected and summarized cannot be recalculated with the new shift values.

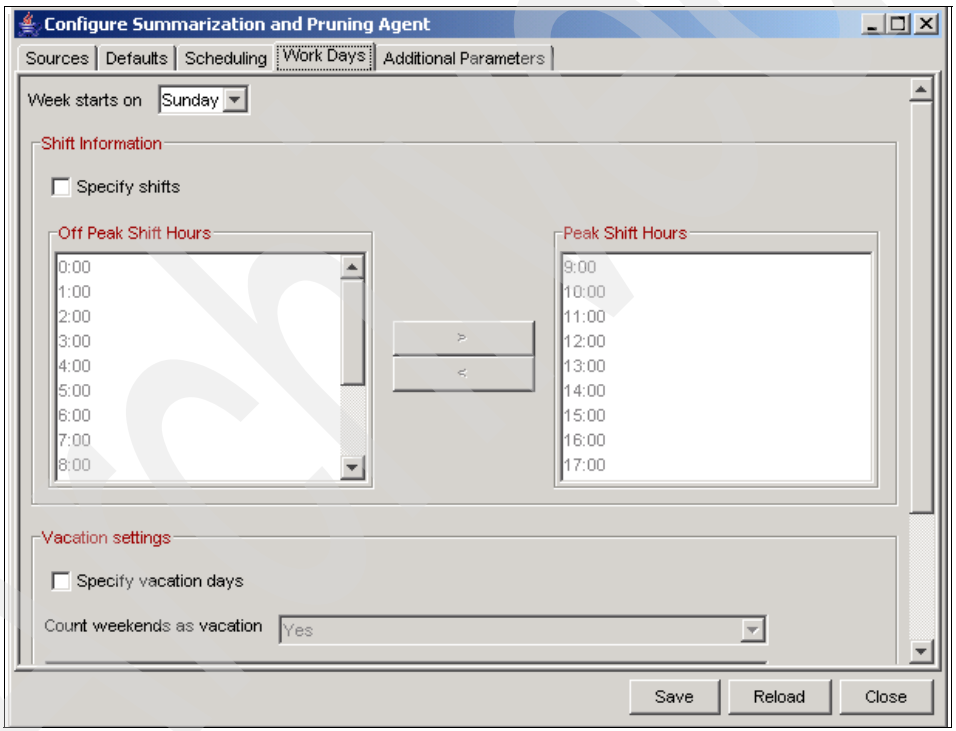


Figure 5-8 Summarization and Pruning Agent Work Days configuration panel

Selecting the Additional Parameters tab opens the panel shown in Figure 5-9 on page 173.

The panel in Figure 5-9 contains the following fields:

- Maximum row per database transaction

  Specify the maximum rows that can be deleted in a single transaction.

- Use timezone offset from

  This is a drop-down list that specifies which time zone to use. If the Tivoli Data Warehouse servers and agents are not all in the same time zone, and all the data is stored in the same database, use this option to identify the time zone that you want to use.

- Summarize hourly data older than and Summarize daily data older than fields

  Specify the age of the data that you want summarized in the Tivoli Data Warehouse. Values are 0 through *n*. The default is 1 for hourly data and 0 for daily data.

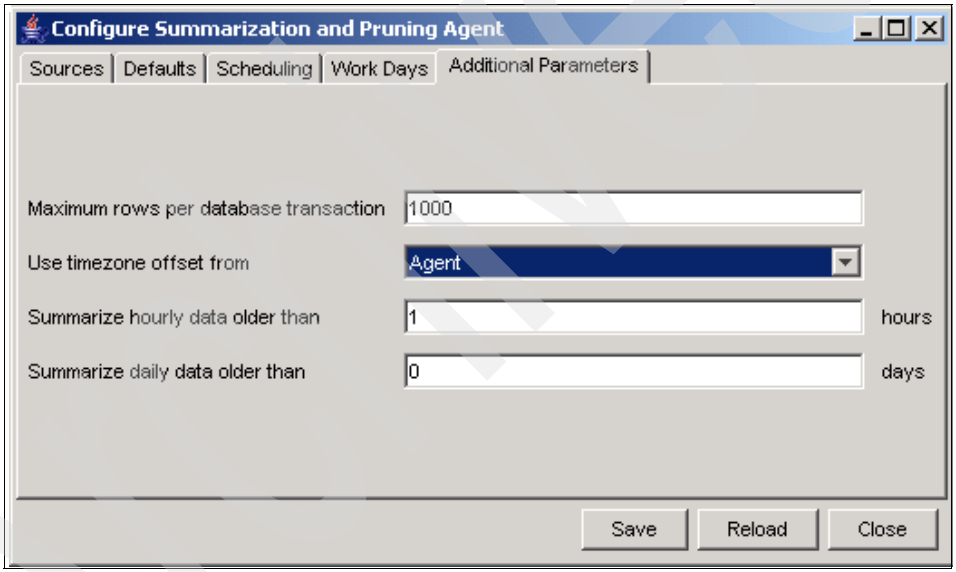


Figure 5-9 Summarization and Pruning Agent Additional Parameters tab

After the default Summarization and Pruning Agent configurations are complete, start the Summarization and Pruning Agent process. The Summarization and Pruning Agent process will wake up every 5 minutes to check to see if it needs to schedule the summarization and pruning run. After the summarization and pruning process is completed, the defaults are permanent and the ksy.k<*pc*>.installed files are completed in the logs directory.

Important: When configuring the Summarization and Pruning Agent, make sure that you set the time for the next execution to be at least 10 minutes into the future. The agent takes a couple of minutes to get started and rounds internally to the nearest 5 minutes. You might not have it run until the next cycle if you do not pay attention to this suggestion.

After the first summarization and pruning process has run, configure the individual agent attribute groups.

5.4 IBM Tivoli Universal Agent

IBM Tivoli Universal Agent is a generic agent that is used in conjunction with other Tivoli Enterprise Monitoring agents to collect data, monitoring systems, and applications in your network. You use and visualize this data in the Tivoli Enterprise Portal. You can use all standard Tivoli Enterprise Portal data viewing options with the Universal Agent.

It is extremely important to understand the difference between the standard Tivoli Enterprise Monitoring agents and the Tivoli Universal Agent, because these types of agents complement each other to provide a robust and completely flexible monitoring solution. Tivoli Enterprise Monitoring agents use a static set of hardcoded attributes or predefined data. Users cannot enhance the Tivoli Enterprise Monitoring agents in order to view more than these predefined attributes. The Universal Agent is, however, is a full-featured intelligent remote agent (IRA) with dynamic application capabilities. Using the Universal Agent, you can dynamically create custom attributes and catalogs. It adds to monitoring solutions to make them complete and flexible for all platforms.

Benefits of using the Universal Agent include:

- Monitors only the data attributes that interest you (configured through metafile applications).
- Enables you to respond quickly to changing monitoring and management scenarios. For example, you can easily change the metafile to support new features in an application.
- Monitors data that is not supported by other Tivoli Enterprise Monitoring agents.
- Integrates data from virtually any operating system and any source.
- Gives you control of attributes and the surfacing of data.
- Provides a means of agent-less monitoring.

Metafiles: Informing Universal Agent what data to collect and monitor

With applications called *metafiles*, we define the data structure to monitor. Metadata is a data map that specifies data characteristics based on application knowledge and monitoring requirements. It splits the input data into fields called *attributes* that can then be viewed or referenced in situations.

Note: You can have many metafiles, such as a metafile for each datasource and type.

Using metafiles, the Universal Agent knows what to monitor on the systems and hosts. After defining a metafile, you import it into the Universal Agent, and it is used by data providers that relay collected data to the Universal Agent. This data is finally used by Tivoli Enterprise Monitoring Server and is similar to data that is collected by specific IBM Tivoli Monitoring Agents. You can choose nine data provider categories depending on your monitoring requirements: API Server, API-Socket-File-Script (ASFS), File, HTTP, ODBC, Post, Script, Simple Network Management Protocol (SNMP), and Socket.

Metafile has both a version and modification number. When it is imported for the first time in the IBM Tivoli Universal Agent, it is assigned a version number of 0 and a modification number of 0. When changes are made in the metafile and it is refreshed on the Tivoli Universal Agent, the version or modification number is incremented by one, depending the type of the modification.

The following changes do not affect the version or modification number of the metafile:

- Time-to-live (TTL) value
- A change to the SOURCE statement
- Data type from P, S, or K to any of P, S, or K
- Delimiter specified in the ATTRIBUTE statement
- A change to the RECORDSET statement
- A change to the CONFIRM statement
- A change to attribute FILTER parameters
- A change to the SQL statement

The following changes affect the modification number (minor changes):

- Adding a new attribute to the end of the attribute list for an attribute group
- Adding a new attribute group at the end of the metafile

- Adding, removing, or changing help text
- Atomizing an existing attribute
- Adding, removing, or changing Scale or Precision values
- Adding, removing, or changing Caption values
- Adding, removing, or changing Warehouse or Aggregation parameters
- Adding, removing, or changing HistoricalTimestamp or PrimaryKey options

The following changes increment the version number (major changes):

- Renaming or deleting an existing attribute
- Changing the type of an attribute
- Changing the length of an attribute
- Changing the name of an attribute group
- Adding a new attribute anywhere other than at the end of a list of existing attributes
- Changing the order of attributes
- Changing a data type from E to P, S, or K
- Changing a data type from P, S, or K to E
- Adding a new attribute group anywhere other than at the end of a metafile

Commands to create, validate, refresh, and import the metafile include:

- To generate a metafile for an ODBC data provider, use the following command:

  ```
  kumpcon generate <datasource> user=<userid> paswd=<password>
  ```

- To validate a metafile, use the following command:

  ```
  kumpcon validate <metafile>.mdl
  ```

- After changing the statement and saving the metafile, you *must* refresh it in the Universal Agent. Enter the following command to refresh the metafile:

  ```
  kumpcon refresh <metafile>.mdl
  ```

- To import a new metafile:

  ```
  kumpcon import <metafile>.mdl
  ```

5.5 The tacmd command

A new set of commands (**tacmd** option) has been added so that you can administer your environment from the command line (both Windows and UNIX).

5.5.1 The tacmd login command

Use the **tacmd login** command to log in to a monitoring server and create a security token for use by subsequent **tacmd** commands:

```
tacmd login {-s|--server} {[PROTOCOL://]HOST[:PORT]} [{-u|--username}
USERNAME] [{-p|--password} PASSWORD] [{-t|--timeout} TIMEOUT]
```

Where:

-s|--*server* Specifies the host name of the Tivoli Enterprise Monitoring Server in to which to log.

-u|--*username* Specifies the user to authenticate.

-p|--*password* Specifies the password of the user to authenticate.

-t|--*timeout* Specifies the maximum number of minutes that can elapse between invocations of **tacmd** before the user is denied access. The default timeout is 15 minutes. The maximum timeout is 1440 minutes (24 hours). If a user name and password are not specified, you are prompted for them.

Note: The **tacmd login** command is required prior to being able to issue any other commands.

5.5.2 The tacmd addBundles command

Use the **tacmd addBundles** command to add one or more deployment bundles to the local agent deployment depot. By default, this command also adds all deployment bundles that are prerequisites of the deployment bundle being added if the prerequisite bundles do not already exist in the depot.

If you do not already have an agent depot, the bundles are added to the location defined by the DEPOTHOME environment variable in the KBBENV environment file.

You must run this command locally on a monitoring server containing a depot:

```
tacmd addBundles {-i|--imagePath} IMAGEPATH [{-t|--product|--products}
PRODUCT ...] [{-p|--platform|--platforms} PLATFORM ...]
[{-v|--version|--versions} VERSION ...]
[{-n|--noPrereq|--noPrerequisites }] [{-f|--force }]
```

where:

-i|--*imagePath* The directory that contains the deployment bundles to be added to the depot.

-t|--*product*|--*products*	The product code or codes of the agents to add. This value corresponds to the value that is displayed in the Product Code field that is displayed by the **viewDepot** or **listBundles** command.
-p|--*platform*|--*platforms*	The platform code or codes of the agents to add. This value corresponds to the value that is displayed in the Host Type field that is displayed by the **viewDepot** or **listBundles** command.
-v|--*version*|--*versions*	The version or versions of the agents to add. This value corresponds to the value that is displayed in the Version field that is displayed by the **viewDepot** command.
-n|--noPrereq|--	**noPrereq** indicates that prerequisite bundles are not automatically added.
-f|--force	This option installs any matching deployment bundles to the depot without prompting for confirmation first.

5.5.3 The tacmd viewDepot command

Use the **tacmd viewDepot** command to display the types of agents that you can install from the deployment depot on the server in to which you are logged or the specified remote server:

```
tacmd viewDepot [{{-j|--depot} DEPOT}]
```

where:

-j|--*depot*	Specifies the name of the remote server that hosts the depot when you are logged in to the hub monitoring server.

Example 5-1 on page 179 lists additional **tacmd** commands.

Example 5-1 Additional important tacmd commands

```
“tacmd addSystem” which deploys an agent and required components to a
managed system
“tacmd createMode” which deploys the OS agent to a new system
“tacmd listSystems” which lists the agents running on a particular
system and their status

“tacmd logout” logs out the user prior to the default logout of 15
minutes
“tacmd restartAgent” cycles the agent on a managed system
“tacmd startAgent” starts the agent on a managed system
“tacmd stopAgent” stops the agent on a managed system
“tacmd updateAgent” used when upgrading agent components
“tacmd viewAgent” provides detailed information about an agent on a
system
```

5.5.4 Return codes

Table 5-6 on page 180 lists the return codes for the **tacmd** commands.

Table 5-6 Return codes for the tacmd command-line interface commands

Code	Category	Description
0	Success	Indicates that the command was successful.
1	Syntax Error or Help	Indicates either that the help command was given or that the syntax used was incorrect.
2	No Permission	Indicates that the user does not have permission to issue the command.
3	Version Mismatch	Indicates that the version of the server is not what was expected.
4	Communication Error	Indicates that an error occurred in the communications with the server.
5	Timeout	Indicates that an operation waiting for data did not receive it within the time it was expected.
6	Input Error	Indicates that the input to the command was not what was expected.
7	Server Exception	Indicates that an error occurred on the server that caused the command to fail.
8	Command Error	Indicates that an internal error occurred while executing the command.
9	Invalid Object	Indicates that a specified object does not exist.

5.5.5 The tacmd editSit command

Use the **tacmd editSit** command to edit a situation:

```
tacmd editsit {-s|--situation} sitname {-p|--property|--properties}
name="value" [ name="value"]...[-f|--force]

tacmd editSit {-l|--local} filename {-p|--property|--properties}
name=value ...
```

where:

- **-s|--situation *sitname*** Specifies the name of the situation to edit.
- **-p|--property |--properties name=*value* ...**

  Specifies one or more name=value pairs that identify the properties of the new situation and their values. Valid property names are:

  – **Desc or Description** - Description of the situation. Input is given as text enclosed between double quotation marks.

- **Sampling Interval** - Input is given in this format, ***ddd/hhmmss***, within double quotation marks.
- **Formula - Situation Formula** - Input is given within double quotation marks. Keywords are prefixed with an asterisk (*).
- **Distribution - Situation Distribution** - Input must be a valid managed system name or names.
- **Advice - Expert Advice for situation** - Input is given as text enclosed between double quotation marks.
- **Action** - The action to be performed when the situation becomes true. Program name or command to be executed.
- **RunOnStart** - Specifies whether the situation has to be executed on start. Valid input is either Yes or No.
- **SitInfo** - Holds the Tivoli Enterprise Console EIF data; a combination of SEV, TFWD, TDST separated between ";" The SitInfo parameters must be enclosed in double quotation marks. SEV can take values Critical, Warning, Minor, Harmless, or Unknown. TFWD=Y or N. TDST can take up to five valid Tivoli Enterprise Console destination server IDs separated by a single double quotation mark (",",)

► **-l|--local** ***filename***

Indicates the file name of the local situation definition to edit, so that no changes are made to the situation definition on the monitoring server.

► **-f|--force**

Disables the message that asks if you are sure that you want to edit the situation.

The following command edits the No_Transactions definition to not run at startup, which requires that you start the situation manually:

```
tacmd editSit -s No_Transactions -p RunOnStart=NO
```

The following command edits the SaveWork definition to run at startup:

```
tacmd editsit -s SaveWork -p Desc="Alerts User to save.."
Formula="*IF *VALUE Local_Time.Minutes *GT 31" Advice="Please save your
work..."
Interval="000/001500" Distribution="Primary:HDCHASDSTC0219:NT"
Action="net send HDCHASDSTC0219 Please Save your Work.." RunOnStart=Yes
SitInfo="SEV=Critical;TFWD=Y;TDST=100"
```

5.5.6 Commands for UNIX only

The following commands are available only on UNIX monitoring servers.

The cinfo command

Use the **cinfo** command to view the following information for your monitoring server:

- An inventory of installed IBM Tivoli products
- The configuration settings for products
- The installed CD versions in the current install_dir directory
- The configuration settings for products in the context of the actual variables that are used by the installation program
- A list of running IBM Tivoli processes (such as agents or monitoring server)
- An validated list of running IBM Tivoli processes, after first performing an update on the tracking database to remove stale PIDs (processes that are logged as “running”, but the processes are not found when the system attempts to verify that they are running by using the **ps** command)

The command can be run in several ways.

Typing **cinfo** opens the menu that is shown in Example 5-2.

Example 5-2 CINFO menu

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

The command can also be run without a menu. You can invoke the four numbered menu options in Example 5-2 as:

- **cinfo -i**
- **cinfo -r**
- **cinfo -c <*pc*>**
- **cinfo -v**

Typing **cinfo -?** displays this help:

```
cinfo [-h candle_directory] [-c product] [-i] [-r] [-s product] [-R]
[-v]
```

where:

-c *product*	Displays configuration prompts and values.
-i	Displays an inventory of installed products.
-r	Shows running processes.

-s *product*	Displays configuration parameters and settings.
-R	Shows running processes after updating a tracking database.
-v	Shows the installed CD versions in this CandleHome.

Note: An exit status of 0 indicates that the command ran successfully. An exit status greater than 0 indicates that there was a failure in the process.

5.5.7 The itmcmd config command

Use the **itmcmd config** command to configure or reconfigure the following items for IBM Tivoli Monitoring on UNIX:

- The IP port that the hub monitoring server uses to listen for requests
- The hosts that can run a product
- The location of the hub monitoring server in the network
- The monitoring server to which an agent connects
- Whether a monitoring server is a hub or a remote server

You can only configure one product at a time. If you reconfigure a monitoring server, you must stop and restart that monitoring server before the changes take effect. The **itmcmd config** command prompts for input for the required parameters. Scripts are in the *install_dir*/bin directory, where *install_dir* is the directory where you installed IBM Tivoli Monitoring.

Use the following syntax to configure a monitoring server:

```
itmcmd config -S [ -h install_dir ] [ -a arch ] -t tems_name
itmcmd config -S [ -h install_dir ] -u -t tems_name pc
itmcmd config -S [ -h install_dir ] [-g] [-t tems_name]
```

Use the following syntax to configure a monitoring agent:

```
itmcmd config -A [ -h install_dir ] [ -a arch ] [ -t agent_host_name ]
pc
itmcmd config -A [ -h install_dir ] [ -a arch ] [ -o domain_name ] pc
itmcmd config -A [ -h install_dir ] [-g] pc
```

where:

-S	Indicates that you are configuring a monitoring server.
-A *pc*	Indicates that you are configuring a monitoring agent.
pc	Specifies the product code for the agent that you want to configure.

-h *install_dir* (Optional) Identifies the installation directory if it is not the one in which the script is located. Also, use this option to take action on an IBM Tivoli Monitoring installation directory other than the one in the current system.

-s (Optional) Option to specify *safe mode* operation. Safe mode invokes the Java Runtime Environment (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.

-a *arch* Optional parameter to specify the architecture where **arch** is one of the abbreviations used to indicate architecture. This parameter enables you to configure an agent and a monitoring server for an architecture other than the architecture that you are using. For example, if you are on AIX 5L and want to configure a Solaris computer, this option is required. Otherwise, the default is the computer that you are using.

-u Adds application support (catalog and attribute files) to a monitoring server for agents that were not installed or for non-UNIX-based agents. If you specify the **-u** parameter, you must also specify the product code (***pc***) for the agent or agents. This parameter is only used with the **-S** parameter.

-t *tems_name* Required parameter that identifies the name of the monitoring server.

-o *instance_name* The instance name for the agent that you want to start.

The itmcmd dbagent command

Use the **itmcmd dbagent** command to start the IBM Tivoli Monitoring for Sybase and IBM Tivoli Monitoring for Oracle monitoring agents:

```
./itmcmd dbagent [-d trace_option] [-h install_dir] [-s server,...]
start | stop [pc]
```

where:

-d *trace_option* Enables diagnostic reporting for one or all monitored database tables. This option enables debug tracing for the following items:

Table Turns on KBB_RAS1 tracing for table (kor*xxxx*, kra*xxxx*). Table names are case-insensitive. You can use ksh wildcards (but not regexp).

debug	Turns on collector and agent internal tracing through **-dddd**.
d	Fine-tunes the internal tracing level: **-d**, **-dd**, **-ddd**, **-dddd**, **-ddddd** (debug or ddds also change col.out to wrap after 100000 lines, and keep col.ou[1-9]), for example, col.ou1, col.ou2, and so forth
all	*,debug.
ALL	**ddddd** + all possible agent KBB_RAS1: (UNIT:K ALL). Note that any form of tracing also turns on KBB_RAS1 (UNIT:KDD ALL).
-h ***install_dir***	(Optional) Identifies the installation directory if it is not the one in which the script is located. Also, use this option to take action on an IBM Tivoli Monitoring installation directory other than the one in the current system.
-s ***server***	Starts monitoring only for the specified servers.
start | **stop**	Starts or stops the specified agent.
pc	Specifies the agent on which you want to take action. If you have installed agents for more than one kind of database, Oracle and Sybase, for example, you can specify the product code for the database type on whose agent you want action taken. The default is that **itmcmd dbagent** applies to all agents.

5.6 Agent Builder

IBM Tivoli Monitoring Agent Builder is a set of tools that is used for creating agents, installation packages for the created agents, and value-add solutions for existing agents. To install the Agent Builder, you must first install and have running one of the following operating systems:

- Windows 2003 Server SE (32-bit) with Service Pack 1
- Windows 2003 Server EE (32-bit) with Service Pack 1
- Windows 2003 Data Center
- Windows XP Professional
- Windows 2000 Server
- Windows 2000 Advanced Server
- Red Hat Enterprise Linux 4.0 + U2
- Red Hat Desktop Linux 4.0 + U2
- SUSE Linux Enterprise Server 9 Sp1
- AIX 5.2 ML10 or higher
- AIX 5.3 ML5 or higher

To run your agent, install IBM Tivoli Monitoring, which must be running on your system as well as an OS agent. The supported operating systems for running an agent created by the Agent Builder are:

- AIX
- Hewlett-Packard UNIX (HP-UX)
- Linux
- Solaris
- Windows

5.6.1 Product code for new agent

Type the registered product code for your new agent. A range of product codes is reserved for use with the Agent Builder. The allowed values are K00-K99. These values are for internal use only and are not intended for agents that will be shared or sold.

5.6.2 Starting the Agent Builder

Start (launch) the Agent Builder by typing the following information on the command line:

- Windows: Install_Location\agentbuilder.exe. Or, go to either **Start** → **All Programs** → **IBM Tivoli Monitoring** → **Agent Builder** or click the Agent Builder desktop icon.
- All other supported operating systems: Install_Location/agentbuilder

5.6.3 Generating the Install Package

You can use the Generate Agent Wizard to generate a Solution Installer Package for a new agent.

To generate a Solution Installer package for the new agent, launch the Generate Agent Wizard using one of the following methods:

- Right-click the **itm_toolkit_agent.xml** file and select **IBM Tivoli** → **Generate Agent**.
- Select the **itm_toolkit_agent.xml** file and select **Generate Agent** on the toolbar.
- Double-click the **itm_toolkit_agent.xml** file to open the multi-paged editor and select **IBM Tivoli Monitoring Agent Editor** → **Generate Agent**.

5.7 IBM Tivoli Monitoring V5.X Endpoint features

IBM Tivoli Monitoring V6.2 is the base software for the Monitoring Agent for IBM Tivoli Monitoring V5.X Endpoint. IBM Tivoli Monitoring provides a way to monitor the availability and performance of all of the systems in your enterprise from one workstation or several designated workstations. IBM Tivoli Monitoring also provides useful historical data that you can use to track trends and to troubleshoot system problems.

5.7.1 Configuring and distributing Monitoring Agent for IBM Tivoli Monitoring V5.X Endpoint

Use this procedure to enable data collection from the managed systems that you want to monitor. You can perform this procedure in two ways:

- Distribution
- Manual distribution

If you have sufficient bandwidth to transfer all of the files, use the distribution procedure. If your bandwidth is insufficient to transfer all of the files, manually distribute the files and push only the configuration.

The Monitoring Agent for IBM Tivoli Monitoring V5.X Endpoint is started and stopped by the IBM Tivoli Monitoring V5.1.2 engine and installed in the IBM Tivoli Monitoring V5.1.2 environment. To facilitate the installation, configuration, and operation, you install it by using traditional Tivoli endpoint distribution mechanisms through the new **`witm61agt`** command line interface.

You can also use this command to modify the configuration of an endpoint where the agent is already running. The changes specified by using this procedure take effect the next time that you restart the engine.

After successfully configuring the seeding of data for a Windows endpoint, look for the string DataSeeding=<ITM5|ITM6|BOTH> in the file $LCF_DATDIR/LCFNEW/Tmw2k/Tmw2k.log to help verify that the IBM Tivoli Monitoring V5.X engine is correctly configured.

Distribution

Perform the following steps:

1. Use the following command on each targeted system that you have listed:

   ```
   witm61agt -c CMSAddress[:BackupCMSAddress] [-f] [-n] [-i seeding]
   [-o outfile] [[-D Variable=Value] ... ] [ -P protocol ] [-p port]
   {-a |endpoint [endpoint ...] | @filename}
   ```

   Where:

-f	Forces the distribution to proceed even if the operating system version check fails.
-n	No distribution of binaries, just performs configuration.
-i	The IBM Tivoli Monitoring **wdmepconfig** command will also be invoked on each endpoint. ***seeding*** specifies where data will go. Valid values are **ITM5**, **ITM6**, or **BOTH**.
-o	Does not distribute binaries or configure, just dumps endpoint list to ***outfile***.
-D	Adds the setting **Variable=Value** to the environment file for the agent.
-P	Specifies the network protocol to use: **TCP** or User Datagram Protocol (**UDP**). The default is **TCP**.
-c	Specifies the network name of the monitoring server. Optionally, you can specify a backup server, separated by a colon (**:**).
-p	Specifies the TCP/IP port number on which the monitoring server listens.
-a	All endpoints that have IBM Tivoli Monitoring profiles distributed to them will receive the distribution.
endpoint	Distributes to the named endpoints.
@filename	Distributes to all endpoints named in the specified file.

2. If you have not set the logging behavior of the IBM Tivoli Monitoring engine using the **-i** option in the previous step, you can use the following command, which only sets that logging behavior:

   ```
   wdmepconfig {-e endpoint | @endpoint_file} {-D DataSeeding=ITM5 |
   ITM6 | BOTH}
   ```

   where:

   -e *endpoint* For IBM Tivoli Monitoring 5.1.2, a list of one or more names of the endpoints.

   -e @*endpoint_file* For IBM Tivoli Monitoring V5.1.2, the file that contains the list of endpoints.

   -D DataSeeding Application to which to log data with the following possible values:

   - **ITM5** IBM Tivoli Monitoring V5.1.2. This is the default value. The data is logged in Tivoli Data Warehouse and Web Health Console, but not Tivoli Enterprise Portal.
   - **ITM6** IBM Tivoli Monitoring V6.2. The data is logged in Tivoli Enterprise Portal, but not in Tivoli Data Warehouse and Web Health Console.
   - **BOTH** IBM Tivoli Monitoring V5.1.2 and IBM Tivoli Monitoring V6.2. This is the preferred setting. You can start with this option, decide which one is preferred, and then reconfigure accordingly.

After you have successfully installed and configured the Monitoring Agent for IBM Tivoli Monitoring 5.x Endpoint to the same environment which IBM Tivoli Monitoring V5.1.x was running, you can remove IBM Tivoli Monitoring V5.1.x Data Warehousing capability in favor of IBM Tivoli Monitoring V6.2 Data Warehousing capability. Wait until after collecting data for warehousing from both IBM Tivoli Monitoring V5.1.x and IBM Tivoli Monitoring V6.2 for a period of time and when data integrity between the two products satisfies the business need.

5.7.2 The wep command

The **wep** command performs actions on the endpoint information contained in the endpoint list maintained by the endpoint manager. Using this command, you can list the endpoints in a Tivoli management region (Tivoli region) and their assigned gateway, retrieve and set endpoint information, migrate an endpoint from one gateway to another gateway, or update other endpoint data within a Tivoli region.

The following command example lists the endpoints assigned to the jadams-gateway:

```
wep ls -g jadams-gateway
```

Example 5-3 shows the output.

Example 5-3 Endpoints assigned to the jadams-gateway wep ls output

```
1122334455.1.512  jadams-gateway
1122334455.10.500+ cookU
1122334455.11.500+ cookA
1122334455.12.500+ jadams
```

The following command example lists the endpoint platforms assigned to the jadams-gateway:

```
wep ls -g jadams-gateway -i interp
```

Example 5-4 shows the output.

Example 5-4 Endpoint platforms assigned to the jadams-gateway

```
aix4-r1
linux-ix86
aix4-r1
w32-ix86
linux-ppc
```

5.8 Upgrading from IBM Tivoli Monitoring V6.1

Use the tasks listed in Table 5-7 to upgrade from IBM Tivoli Monitoring V6.1 to IBM Tivoli Monitoring V6.2.

Table 5-7 Upgrading from Tivoli Monitoring V6.1 to Tivoli Monitoring V6.2

Task	Action
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. Stop all components that you are upgrading and change their startup from **Automatic** to **Manual**. Restart the computer on which you are installing IBM Tivoli Monitoring.

Task	Action
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.
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. Support for base agents is upgraded automatically, but you must add application support for any other monitoring agents you are upgrading.

The typical upgrade scenarios when upgrading to IBM Tivoli Monitoring V6.2 are upgrading from IBM Tivoli Monitoring V5.1.2, upgrading from Omegamon Platform V350, or upgrading from Omegamon Platform V360.

6

Troubleshooting and performance tuning

This chapter focuses on the troubleshooting and performance tuning of an IBM Tivoli Monitoring V6.2 installation and its various components. In the IBM Tivoli Monitoring V6.2 Certification Exam, troubleshooting and performance tuning-related questions are grouped in one section; therefore, we discuss them together.

This chapter discusses the following topics:

- Troubleshooting and tuning the historical database
- IBM Tivoli Monitoring V6.2 trace and log facilities
- Tivoli Enterprise Portal Server troubleshooting
- Heartbeat
- Situations
- SOAP interface
- Workspaces

For more in-depth troubleshooting information that we do not describe here, refer to *IBM Tivoli Monitoring Problem Determination Guide, Version 6.2*, GC32-9407.

6.1 Troubleshooting and tuning the historical database

It is important to understand how the IBM Tivoli Monitoring V6.2 historical database works in order to be able to first understand how to tune and troubleshoot.

6.1.1 Tivoli Data Warehouse V2.1 overview and architecture

Tivoli Data Warehouse V2.1 has two processes that collect, summarize, and prune data gathered from IBM Tivoli Monitoring V6.2 agents. The *Warehouse Proxy agent* is the data warehouse server. The Warehouse Proxy agent collects data from the IBM Tivoli Monitoring V6.2 agents and stores the data in a relational database (DB2, Oracle, or Microsoft SQL). Tivoli Data Warehouse V2.1 can optionally be configured to summarize and prune the historical data with another process called the *Warehouse Summarization and Pruning Agent*. If you choose not to run the Summarization and Pruning Agent, you still get historical, detailed data in the database tables. However, you do not get summarized data if you do not run the Summarization and Pruning Agent. Therefore, if you are trying to determine if any data is being collected from the Tivoli Enterprise Monitoring agents, you need to make sure that the Warehouse Proxy agent is running.

Figure 6-1 shows an overview of historical data collection.

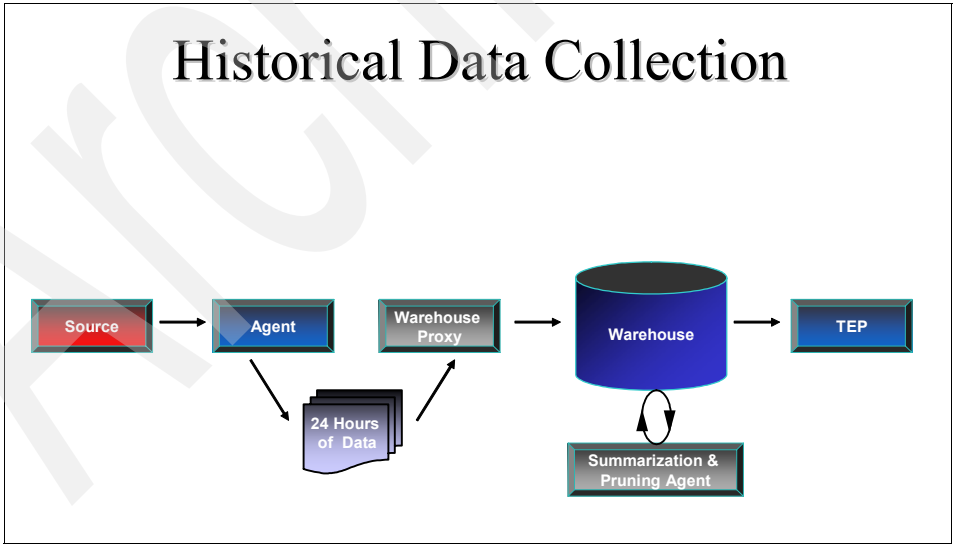


Figure 6-1 Historical data collection overview

6.1.2 Historical data architecture overview

The IBM Tivoli Monitoring V6.2 historical data collection architecture consists of three primary components. The following components are used to collect data in the IBM Tivoli Monitoring V6.2 architecture:

- Warehouse Proxy agent
- Warehouse Summarization and Pruning Agent
- Tivoli Data Warehouse V2.1

Warehouse Proxy agent

The Warehouse Proxy agent is the bridge between the active monitoring system and the historical data repository. It handles warehousing requests from all managed systems in the enterprise. It uses Open Database Connectivity (ODBC) to write the historical data to a supported relational database. Only one warehouse proxy agent can be configured and running in an IBM Tivoli Monitoring instance (that is, the hub Tivoli Enterprise Monitoring Server) at one time. The Warehouse Proxy can only successfully connect to a hub monitoring server.

Summarization and Pruning Agent

The Summarization and Pruning Agent maintains the data within the data warehouse by aggregation and pruning data that is based on client specifications. The IBM Tivoli Monitoring administrator sets up how often to collect the detailed data, at what intervals to aggregate and prune, and how often to run the aggregation and pruning engine. Typically, the summarization and pruning process is scheduled to run only once a day.

Tivoli Data Warehouse V2.1

The Tivoli Data Warehouse database is an integral part of the solution. It stores a large amount of attribute data, and clients will want to host this data on existing database farms. The database is used by Tivoli Enterprise Portal if historical data is represented. External reporting tools and other applications can access the data and use this database to operate.

6.1.3 Configuring the historical database

There are two parts to configuring the Tivoli Data Warehouse V2.1 in IBM Tivoli Monitoring V6.2. The first part is configuring the Summarization and Pruning Agent default parameters, which we cover in 6.1.3, “Configuring the historical database” on page 195. This part is usually done during the installation and basic configuration.

The second part is configuring the specific agent attribute groups from the Tivoli Enterprise Portal History configuration icon, which we describe next.

History configuration

After the first summarization and pruning process has run, configure the individual agent attribute groups. The agent attribute groups can be configured from the Tivoli Enterprise Portal Server History configuration icon as shown in the steps in Figure 6-2 on page 197. You must configure the specific agents to start collecting data in order to get data in Tivoli Data Warehouse V2.1.

The following steps refer to the numbered steps in Figure 6-2 on page 197:

1. Select the History configuration icon from the Tivoli Enterprise Portal Server GUI.
2. Highlight the specific attribute groups for which you want to collect historical data and add the configuration settings. If you click **Show Default Groups**, the panel highlights all of the preconfigured attribute groups for the current agent. This function is useful if this is the first time that you are setting up an agent for historical collection.
3. Click **Configure Groups** for the highlighted groups. If it is the first time that you are configuring an attribute group and you have clicked **Show Default Groups**, all of the default settings that were defined in the Summarization and Pruning Agent configuration will be loaded.
4. Highlight the specific groups again and click **Start Collection**.

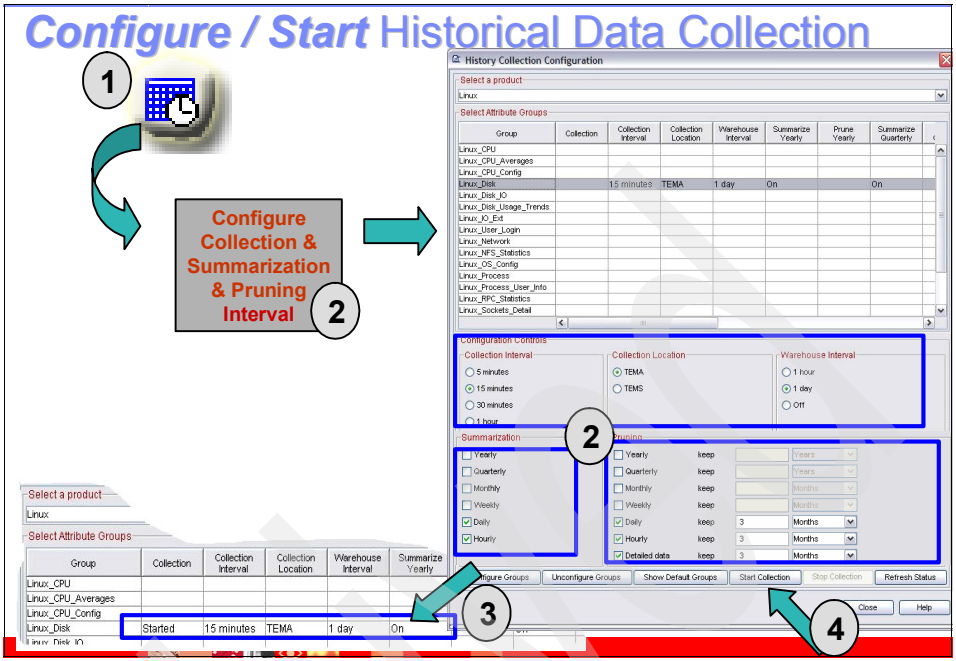


Figure 6-2 History collection configuration

Figure 6-3 on page 199 is an example of configuring the default attribute groups for the Linux OS agent.

The following list describes the fields and buttons in Figure 6-3 on page 199:

- Collection Interval (check boxes)

  The collection interval sets the default time to collect data on the Tivoli Enterprise Monitoring agent or Tivoli Enterprise Monitoring Server to the binary files. The default 5 minute value might be a little low for all default attribute groups. You can configure the collection interval for one group or a list of highlighted groups.

- Collection Location (check boxes)

  The collection location is the default location for storing the binary files. We recommend that, whenever possible, you select **TEMA** (that is, at the agent).

- Warehouse Interval (check boxes)

  The warehouse interval is the interval at which the Tivoli Enterprise Monitoring agent or Tivoli Enterprise Monitoring Server binary data will be uploaded to the Warehouse Proxy agent. The options are 1 hour, 1 day (daily), and Off. For environments with many agents, we recommend selecting **1 hour** instead of 1 day. If you select Off, no data will be collected in Tivoli Data Warehouse for the selected attribute groups. However, if the attribute group is started with the interval off, the binary data will be collected on the agent, although it will never be pruned.

- Summarization

  This area enables you to select what summarization tables will be created in the Tivoli Data Warehouse for the specific attribute groups.

- Pruning

  This area sets the time to keep data in the Tivoli Data Warehouse. Data older than the prune settings will be removed from the Tivoli Data Warehouse.

- Configure Groups (button)

  Click this button to configure the highlighted attribute groups' historical configuration settings. You can highlight a single group or multiple groups.

- Unconfigure Groups (button)

  Click this button to unconfigure the highlighted attribute groups' historical configuration settings. You can highlight a single group or multiple groups.

- Show Default Groups (button)

  This button highlights all of the predefined (by the agent) attribute groups. Click this button to configure the highlighted attribute groups' historical configuration settings. You can highlight a single group or multiple groups.

- Start Collection (button)

  This button starts all of the highlighted attribute groups. You can highlight a single group or multiple groups.

- Stop Collection (button)

  This button stops all of the highlighted attribute groups. You can highlight a single group or multiple groups. If one of the highlighted attribute groups is already stopped, this button is unavailable.

- Refresh Status (button)

  This button refreshes the status (Started or Stopped) of all of the agents.

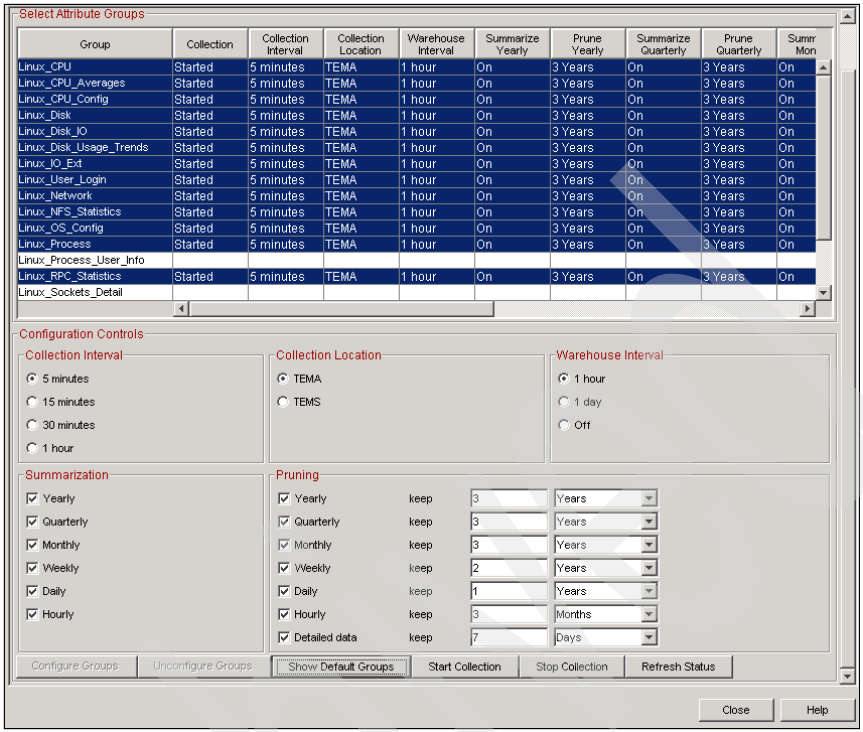


Figure 6-3 History configuration panel

6.2 IBM Tivoli Monitoring V6.2 trace and log facilities

IBM Tivoli Monitoring V6.2 contains an extensive trace facility that can provide helpful information about the state of the components. There are several types of logs created by IBM Tivoli Monitoring V6.2, and the most important log type is reliability, availability, and serviceability (RAS). RAS logs are in the English language and are available on the Tivoli Enterprise Monitoring Server, Tivoli Enterprise Portal Server, and monitoring agents. Other logs include installation, seed, LG0, ODBC, and other configuration files. In this section, we discuss several of the trace settings and readings that are generated by the trace logs.

Table 6-1 on page 200 summarizes the IBM Tivoli Monitoring V6.2 log names and locations.

Table 6-1 Log names and locations

Windows		**UNIX**	
Tivoli Enterprise Portal Server	*install_dir*\logs*hostname_cq_timestamp-xx.log*	Tivoli Enterprise Portal Server - Linux	*install_dir*/logs/hostname_cq_timestamp-*xx*.log
Tivoli Enterprise Monitoring Server	*install_dir*\logs*hostname_*ms_*timestamp-xx*.log	Tivoli Enterprise Monitoring Server	install_dir/logs/hostname_ms_timestamp-*xx*.log
Agents	*install_dir*\tmaitm6\logs log names vary by agent: ► RAS1 logs generally have the syntax of *hostname_PC_timestamp-xx*.log. ► The *.LG0 log file shows the connectivity with Tivoli Enterprise Monitoring Server, the situations that are running, and the status of Take Actions.	Agents	install_dir/logs log names vary by agent: ► RAS1 logs generally have the syntax of *hostname_PC_timestamp-xx*.log. ► The *.LG0 log file shows the connectivity with Tivoli Enterprise Monitoring Server, the situations that are running, and the status of Take Actions.
Warehouse Proxy	install_dir/logs/*hostname*_hd_*timestamp-xx*.log	Warehouse Proxy	Currently not available on UNIX
tacmd	install_dir\bin\kuiras1.log	tacmd	install_dir/logs/kuiras1.log
IBM Tivoli Monitoring V5.x Monitoring Agent	Endpoint logs: %LCF_DATDIR%/LCFNEW/KTM/logs/ktmras1.log Tivoli region logs: %DBDIR%/KTM/logs ► trace_witm61agt___#_pid.log ► trace_ITM61Integration_Install____#_pid.log	IBM Tivoli Monitoring V5.x Monitoring Agent	Endpoint logs: $LCF_DATDIR/LCFNEW/KTM/logs/ktmras1.log Tivoli region logs: *$DBDIR*/KTM/logs ► trace_witm61agt___#_pid.log ► trace_ITM61Integration_Install____#_pid.log
Seeding process	*install_dir*\CNPS\logs\seedPPC.log *install_dir* InstallITM\logs\CMSSeed log for Tivoli Enterprise Monitoring Server	Seeding process	*install_dir*/logs/*hostname*_ci_<*tems pid*>.log

Windows		UNIX	
Summarization and Pruning Agent	*install_dir*\logs*hostname*_sy_*timestamp-xx*.log	Summarization and Pruning Agent	*install_dir*/logs/*hostname*_sy_*timestamp-xx*.log
Installation logs	*install_dir*\InstallITM ► IBM Tivoli Monitoring *date PID*.log - Main installation log. ► TEPS_ODBC.log - Configuration of the Tivoli Enterprise Portal Server ODBC connection. ► Warehouse_Configuration .log - Configuration of the Warehouse proxy.	Installation logs	*install_dir*/logs ► candle_installation.log - Main installation log. ► InstallPresentation.log - Tivoli Enterprise Portal Server seeding log. ► db2prep.log - Tivoli Enterprise Portal Server configuration log, assuming DB2 is the database.
Tivoli Enterprise Portal desktop client	*install_dir*\CNP\kcjerror.log *install_dir*\CNP\kcjras1.log This log file contains all of the RAS1 tracing for the Tivoli Enterprise Portal client When launched via Java Web Start: %USERPROFILE%\Application Data\IBM\Java\Deployment\log\javaws*nnnnn*.trace where "*nnnnn*" is a unique, randomly generated numeric suffix to support generational logs (that is, the last generated log will not be overlaid by the most current execution of Tivoli Enterprise Portal using Java Web Start. This is in contrast to the Tivoli Enterprise Portal Browser client, which has a fixed name and is overlaid with each execution cycle.	Tivoli Enterprise Portal desktop client	*install_dir*/logs/*hostname_PC_timestamp*.log When launched via Java Web Start: ${user.home}/.java/deployment/log/javaws*nnnnn*.trace where "*nnnnn*" is a unique, randomly generated numeric suffix to support generational logs (that is, the last generated log will not be overlaid by the most current execution of Tivoli Enterprise Portal using Java Web Start. This is in contrast to the Tivoli Enterprise Portal Browser client, which has a fixed name and is overlaid with each execution cycle.

Note: Table 6-1 uses the following variables:

- *xx*: The rotating log number
- *PC*: The 2-letter product code, for example, UX for the UNIX Agent
- *PPC*: The 3-letter product code, for example, KUX for the UNIX Agent

6.2.1 Trace settings

Several environment variables control tracing the components. There several methods by which these variables can be modified. Table 6-2 on page 203 defines many of the environment variables. Note that this is not an exhaustive list.

Table 6-2 Trace environment variables

Variable	Description
KBB_RAS1	Controls the trace level in the RAS logs.
KDC_DEBUG	Diagnosing communications or connectivity problems, or both.
KBB_RAS1_LOG	Log file location of the RAS1 log.
INVENTORY	File containing the inventory of RAS1 logs for the component.
MAXFILES	Total number of log files to maintain. The default is 32 MB.
LIMIT	Maximum log file size per file in MB. The default is 5.
COUNT	Maximum number of log files per session. The default is 5.
Universal Agent: Specific settings	
KUMP_ODBC_DEBUG=Y	ODBC Data Provider tracing.
KUMP_HTTP_DEBUG=Y	HTTP Data Provider tracing.
KUMP_SCRIPT_DEBUG=Y	Script Data Provider tracing.
KUMP_SNMP_DEBUG_TRAP=Y KUMP_SNMP_DEBUG_DISCOVERY_ROUTE=Y KUMP_SNMP_DEBUG_DISCOVERY_NETWOR K=Y KUMP_SNMP_DEBUG_MIB_MANAGER=Y KUMP_SNMP_DEBUG_MIB_IO=Y	Simple Network Management Protocol (SNMP) Data Provider tracing. All of the debug environment variables listed previously default to No. As an example, if you use the SNMP Data Provider and have problems collecting Management Information Base (MIB) data, you set two environment variables: KUMP_SNMP_DEBUG_MIB_MANAGER=Y KUMP_SNMP_DEBUG_MIB_IO=Y
ERROR (UNIT:kumpfile Error State Detail Flow Metrics) (UNIT:kumpdcmf ALL)	Detailed File Data Provider tracing.
ERROR (UNIT:kumpsosr ALL) (UNIT:kumpspst ALL) (UNIT:kumpscku ALL) (UNIT:kumpstcp ALL) (UNIT:kumplpba ALL)	Detailed API or Socket Data Provider tracing.
ERROR (UNIT:kumamain ALL)	Problems involving managed system online/offline processing.
ERROR (UNIT:kumpdpda Error Output) (UNIT:kumpmd2a Error Detail)	Incorrect report data.

Variable	Description
ERROR METRICS	Problems involving Universal Agent memory usage.

To manage the tracing of the IBM Tivoli Monitoring components:

- Modify the appropriate environment file:
  - Tivoli Enterprise Monitoring Server:
    - Windows: *install_dir*\CMS\KBBENV
    - UNIX: *install_dir*/config/*hostname_ms_hostname*.config
  - Tivoli Enterprise Portal Server:
    - Windows: *install_dir*\CNPS\KFWENV
    - Linux: *install_dir*/config/cq.config
  - Tivoli Enterprise Portal Client:
    - From the Tivoli Enterprise Portal menu, select **File** → **Trace Options**.
    - Select a trace class from the list or as instructed by IBM Software Support (such as UNIT:Workspace ALL): ALL provides data for all classes. Use the setting temporarily, because it generates large amounts of data. ERROR logs internal error conditions. This setting provides the minimum level of tracing with little resource overhead and ensures that program failures will be caught and detailed. NONE turns off the error log so that no data is collected.
  - Agents:
    - Windows: *install_dir*\TMAITM6*PPC*ENV (where *PPC* is the 3-letter product code for the agent)

      For example, Windows Agent: C:\IBM\ITM\TMAITM6\KNTENV
    - UNIX: *install_dir*/config/*pc*.config (where *pc* is the 2-letter product code for the agent)

      For example, Linux Agent: /opt/IBM/ITM/config/lz.config
  - Command line **`tacmd`**:
    - Windows: *install_dir*\bin\KUIENV
    - UNIX: *install_dir*\bin\tacmd
  - IBM Tivoli Monitoring V5.x Monitoring Agent:
    - Windows: %LCF_DATDIR%\LCFNEW\KTM\KTMENV
    - UNIX: $LCF_DATDIR/LCFNEW/KTM/KTMENV

- Modify the trace settings using the Manage Tivoli Enterprise Monitoring Services GUI:
  a. Right-click the desired component, and select **Advanced** → **Edit Trace Parms**.
  b. This opens a menu that enables you to modify the trace settings (see Figure 6-4).

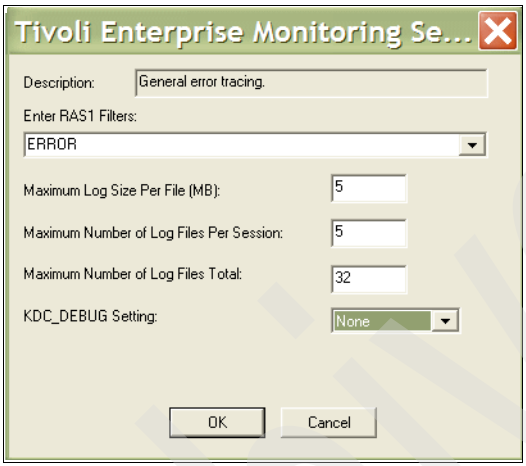


Figure 6-4 Trace parameter menu for Tivoli Enterprise Monitoring Server

- Connect to the IBM Tivoli Monitoring Service Index using a browser:
  a. In the browser, enter:

     `http://systemname:1920`

  b. If multiple components are installed, select the appropriate one and enter a valid user and password for authentication.

     This action opens the IBM Tivoli Monitoring Service Console for the selected component. At the bottom of the page, you can change the settings. Refer to the *IBM Tivoli Monitoring Problem Determination Guide, Version 6.2.0*, GC32-9458-01, for more details about using and blocking this tool.

After you modify the trace settings, you need to recycle the corresponding component in order for the change to take effect. The log file for the component will show the current trace level in the header of the log, as shown in Example 6-1 on page 206.

Example 6-1 Header from Tivoli Enterprise Monitoring Server log file

```
!435BFB0A.0000!=====================>  IBM Tivoli RAS1 Service Log
<========================
+435BFB0A.0000      System Name: aixurania                   Process ID: 8344
+435BFB0A.0000     Program Name: kdsmain                      User Name: root
+435BFB0A.0000        Task Name: cms                       System Type: AIX;5.2
+435BFB0A.0000   MAC1_ENV Macro: 0xA326                     Start Date: 2005/10/23
+435BFB0A.0000       Start Time: 17:05:14                      AS Limit: None
+435BFB0A.0000       Core Limit: 1024M                       CPU Limit: None
+435BFB0A.0000       Data Limit: 2048M                     Fsize Limit: 1024M
+435BFB0A.0000     Nofile Limit: 2000                      Stack Limit: 32M
+435BFB0A.0000    Service Point: root.aixurania_ms       UTC Start Time: 435bfb0a
+435BFB0A.0000  Executable Name: kdsmain                     ITM Home: /opt/IBM/ITM
+435BFB0A.0000      ITM Process: aixurania_ms
+435BFB0A.0000         KBB_RAS1: ERROR (UNIT:kglcry all)
+435BFB0A.0000      KBB_ENVPATH: KBBENV
+435BFB0A.0000
================================================================================
```

6.2.2 Integration Agent

Beginning with the IBM Tivoli Monitoring V5.x Agent component, these agents keep their log files in the following locations:

- On Windows endpoints:
  %LCF_DATDIR%/LCFNEW/KTM/LOGS/KTMRAS1.LOG
- On UNIX or Linux endpoints:
  $LCF_DATDIR/LCFNEW/KTM/LOGS/KTMRAS1.LOG

The data in these log files is specific to only the IBM Tivoli Monitoring V5.x Agent component. Notice that the locations are in the traditional Tivoli installation locations.

Sometimes, after we install a new Integration Agent, it does not show up immediately in Tivoli Enterprise Portal Server. While this is frustrating, there are several places that we can look for help:

- Verify that you restarted IBM Tivoli Monitoring Engine.
- Ensure that IBM Tivoli Monitoring resource models are running.

If an Integration Agent is not showing up in Tivoli Enterprise Portal Server, check the logs and look for `ST` or `DC_SERVER_UNAVAILABLE`. If you see this message, Tivoli Enterprise Monitoring Server probably cannot be resolved.

If when looking at IBM Tivoli Monitoring V5.X endpoints, you do not see any IBM Tivoli Monitoring V6.x Integration Agent code, the distribution probably failed. Check the MDist 2 log and see if the distribution ID failed to register.

When an Integration Agent appears unavailable in the Tivoli Enterprise Portal console, most likely the IBM Tivoli Monitoring V5.x engine on that agent, server, or endpoint had a problem. Make sure that the XML files are still being created by the IBM Tivoli Monitoring V5.x Agent, and also verify that the profiles are still set up for data logging.

In addition to these methods, the following additional log files are critical to troubleshooting:

- IBM Tivoli Monitoring V5.x Engine logs
- IBM Tivoli Monitoring V5.x PAC Provider logs

Occasionally, data might not be presented in the Tivoli Enterprise Portal Server even though the IBM Tivoli Monitoring Engine is running. If this is the case, make certain that the IBM Tivoli Monitoring V5.x Integration Agent is running and that the Resource Models are defined in the Integration Agent XML file.

If an IBM Tivoli Monitoring V6.2 Agent shows a status of OFFLINE, first ensure that the agent is running. If not, simply start the agent. If the agent still shows an OFFLINE status, verify the configuration of the agent to the Tivoli Enterprise Monitoring Server.

6.2.3 Universal Agent

When troubleshooting IBM Tivoli Universal Agent, you have additional methods to trace problems. Set the KDC_DEBUG variable to Y for yes. The KDC_DEBUG variable diagnoses communication problems between the Universal Agent and the Tivoli Enterprise Portal Server.

6.3 Tivoli Enterprise Portal Server troubleshooting

When determining errors about loading data from the Tivoli Enterprise Monitoring agent to the Tivoli Data Warehouse through the Warehouse Proxy agent, look in the relational database management system (RDBMS) database at a table called WAREHOUSELOG. However, this table will not be useful in determining Tivoli Enterprise Portal GUI display problems related to viewing historical data. Sometimes, timing parameters defined (*TACMD_TIMEOUT* variable) in the Tivoli Enterprise Monitoring Server can affect a user's ability to display historical data.

When logging on to the Tivoli Enterprise Portal Server through a browser, you might see HeapDumps and JAVACore entries. Make sure that the user's Java environment has the following parameters defined: **-Xms128m** and **-Xmx256m**.

The minimum level of Java Runtime Environment (JRE) in order for the Tivoli Enterprise Portal Server to run is Java 1.5.2.

If you are getting an out-of-memory condition, java.lang.OutOfMemoryError, when you are logged on to Tivoli Enterprise Portal, it manifests itself in various ways. For example, in browser mode, the window might be disabled after an hour or two. If you are connecting to multiple portal servers from the same computer, increase the memory by 125 MB for each portal server.

Review the Java log plugin150.trace file on your system to confirm the cause. On a Windows system, this file is in C:\Documents and Settings\Administrator\Application Data\IBM\Java\Deployment\log.

In the Tivoli Enterprise Portal Server logs, the KFW_DSN entry tells you the datasource name.

6.3.1 Creating users

You create users through the Administer Users panel (Ctrl+u). There is a default user. Changes to this default user changes the defaults when you use the default user as a template to create other users. However, the default user is just a template, and subsequent changes to the template do not impact existing users that were created from the template.

The default template can be copied using the option to create another user while the default user is selected.

When creating a new user or creating another user, you are prompted to supply three pieces of information for the user. The first, user ID, is the only mandatory field that you must supply. Note that this user ID is limited to 10 characters with no spaces. The next field is user name. Note that this field is not the same thing as the user ID. This field can have spaces and needs to be used to categorize users. An example is "ITSO operators." The user name is visible in the users' list and can be helpful to organize your users. The final field is a user description. This field can contain spaces and punctuation. You can use this field to store information about the user, such as corporate ID number, e-mail address, and phone number.

Previously, we stated that there is no concept of groups. There is, however, a concept of templates (such as the default user) that can aid in the creation of user accounts. When you create a "template" account, name it in such a way that it is visible to you as a template. See Example 6-2 on page 209.

Example 6-2 Template accounts

```
userid: template1 (or tmpltoprns --> remember! limited to 10
characters)
user name: template for creation of operator accounts
user description: this template needs to be used to create all
operators.
```

Consider the following important points:

- You do not want the template user IDs to correlate to actual users. It is a security violation to allow this correlation. Make sure that your system administrators do not create a user account with these names, because you do not want anyone to gain access to the environment and start using template administrators to perform functions.
- Remember to create another user after selecting your template, not create new user.
- Create all users based on copies of the templates (and thus not the default user) or new users. This action enables you to keep to your policies for security and job separation.

6.3.2 Authentication

We strongly recommend authentication to meet most corporate security requirements. The authorization of users is activated by using Manage Tivoli Enterprise Monitoring Services on Windows or the **`itmcmd manage`** command on Linux or UNIX.

When using authentication for users, this account will be associated with a user name on Tivoli Enterprise Portal Server. This account can be a Windows domain account, a system account, or a Lightweight Directory Access Protocol (LDAP) domain account. However, the following restrictions apply:

- The account must exist on the Tivoli Enterprise Portal Server and Tivoli Enterprise Monitoring Server servers.
- The account can be a domain account on Windows if the Tivoli Enterprise Portal Server and Tivoli Enterprise Monitoring Server are both Windows machines.
- The account must use 10 or fewer characters for the user name.

The authentication is performed against the Windows accounts or domain accounts, RACF or ACF/2 on z/OS, and /etc/passwd on Linux or UNIX or in the LDAP domain.

The three major areas of definition for a user are permissions, applications, and workspaces.

The Permissions tab lets you assign granularity to the capabilities of your users. The philosophy when giving permissions to users is to keep them to the minimal permissions for their job.

In the Applications tab, you control to which agents and applications the user has access and the type of access.

The Workspaces tab defines the views that the user can access. Granularity here only comes from creating custom Navigator views and removing access to the Physical and Logical views. You can also set the default view for the Navigator view for this user.

You cannot restrict a user to a set of machines, for example, when using the Physical Navigator view for this user. However, the default view restricts the user to the view that you select here or later.

As an example, you can select UNIX Systems in the Physical Navigator and restrict the administrator to only UNIX systems (any and all systems in that view are then available). You *cannot* choose to restrict the administrator to a single system under UNIX or to give the administrator multiple choices, such as UNIX and Windows.

To provide a more granular set of limited views for systems or applications requires multiple accounts or a custom workspace with a limited number of systems and using that workspace instead of the Physical or Logical Navigators for those users.

If a user is experiencing login problems and receives a message similar to the message shown at the bottom of the window in Figure 6-5 on page 211, check the following items:

- Is your security authenticator running?
- Is the Tivoli Enterprise Portal Server database running?
- Is the user ID defined in the Tivoli Enterprise Portal Server database?

Figure 6-5 Authentication error

6.3.3 Verifying that the user is defined in Tivoli Enterprise Portal Server database

You might be asked to verify that a user is set up in IBM Tivoli Monitoring V6.2. The simplest way to verify if a user is set up in IBM Tivoli Monitoring V6.2 is by clicking the User Administrator icon in Tivoli Enterprise Portal and looking for the user, but doing this does not ensure that the user is set up in the OS.

User names can only be 10 characters in length. Keep this in mind, because the user IDs must match the OS.

If security is enabled and a user is defined in the User Administrator, but the user still cannot log in, you must first verify that the user is defined on the Tivoli Enterprise Monitoring Server.

To determine if security is enabled, try these options:

- On UNIX:

  ```
  opt/IBM/ITM/bin/itmcmd config -S -g -t fins | grep SECURITY
  ```

- On Windows

  Right-click **TEMS** from Manage Tivoli Enterprise Monitoring Services, select **Reconfigure**, and check whether the Security option is selected.

6.3.4 Tivoli Enterprise Portal Server logs

When troubleshooting the Tivoli Enterprise Portal Server, be sure to check the following location for logs:

```
INSTALL_DIR/CNPS/LOGS
```

When troubleshooting connectivity messages in the Tivoli Enterprise Portal Server log, you might see entries similar to the one shown in Example 6-3.

Example 6-3 Tivoli Enterprise Portal Server log

```
43611641.007D-A08:ctsqlconnectionsql1.cpp,632,"CTSQLEvaluatorSQL1_i::Co
nnection::_init") SQL1: Looking for hub at 'IP.SPIPE:TEMSSERVER1'...
.....
(43611657.0000-1F8:kdebscn.c,133,"KDEB_SocketConnect") connection
procedure failed, socket error 1
```

These errors suggest there is a firewall port or Tivoli Enterprise Portal Server configuration problem.

If a user can connect to the Tivoli Enterprise Portal Server through the browser interface, but the user *cannot* connect to the desktop client, ensure that the desktop client is configured to the appropriate Tivoli Enterprise Portal Server and that it is available.

If application seeding failed during the installation, you might see a display similar to the one shown in Figure 6-6.

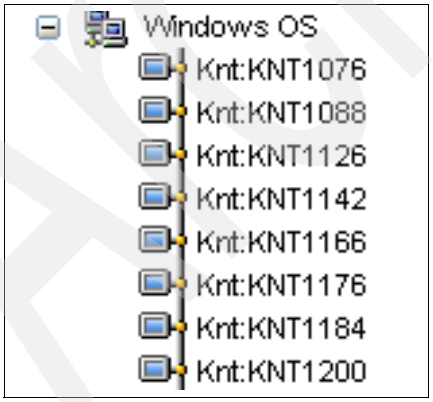


Figure 6-6 The agent names do not show up correctly

The agent names do not show up correctly. In this situation, reload the application support.

Use the ODBC datasource to test the connection of the portal server to the database on Windows as shown in Figure 6-7 and Figure 6-8.

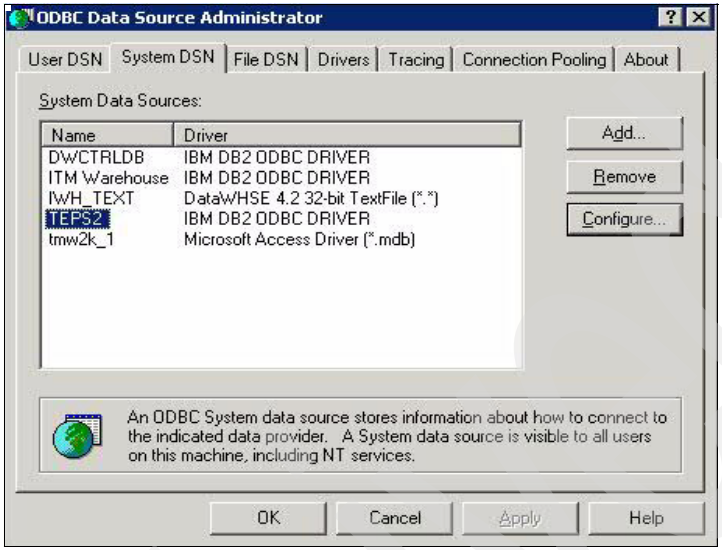


Figure 6-7 Select the ODBC Datasource Name

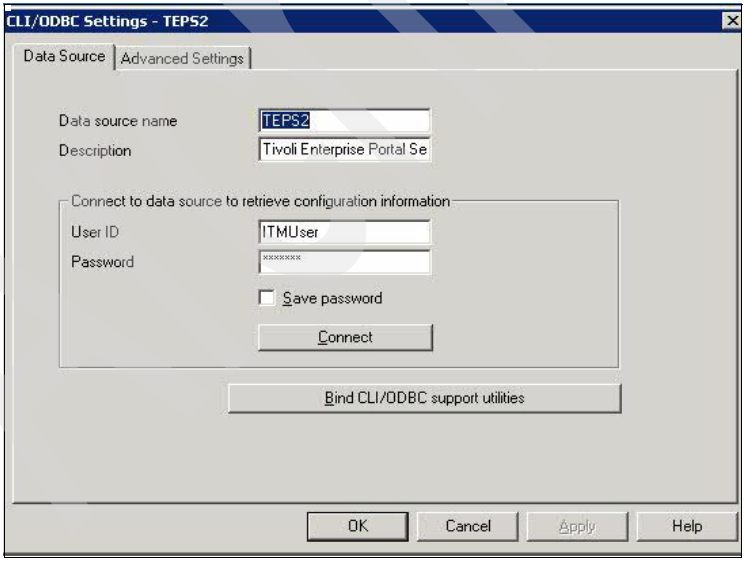


Figure 6-8 Enter the database user ID and password

6.4 Heartbeat

The *CTIRA_HEARTBEAT* variable is set at the Tivoli Enterprise Monitoring agents and remote Tivoli Enterprise Monitoring Servers. It defines the interval at which the Tivoli Enterprise Monitoring agent or remote Tivoli Enterprise Monitoring Server will send its heartbeat to the hub. The default is 10 minutes for the Tivoli Enterprise Monitoring agent (value set to 600). The Tivoli Enterprise Monitoring agent will only detect a “hub down” condition if the heartbeat is not accepted at the hub. By setting the *HEARTBEAT* to a shorter interval, the Tivoli Enterprise Monitoring agent switches more quickly to the new hub after the primary hub fails. Use this parameter with care, because it will increase network traffic and also usage of the Tivoli Enterprise Monitoring Server that will need to handle more heartbeat calls. We recommend that you do not set this value lower than 2 or 3 minutes. In addition, if you have Tivoli Enterprise Monitoring agents or remote Tivoli Enterprise Monitoring Servers that have a higher priority than other agents or servers, you can set the heartbeat interval shorter for these higher priority agents and servers, but leave it at 10 minutes for the other lower priority agents and servers.

Note: Changing this parameter does not influence the interval at which the Tivoli Enterprise Monitoring Server will report a Tivoli Enterprise Monitoring agent as offline. The interval changes the time at which the Tivoli Enterprise Monitoring agent sends the heartbeat, but the Tivoli Enterprise Monitoring Server still only checks every 10 minutes if any Tivoli Enterprise Monitoring agent or remote Tivoli Enterprise Monitoring Server has not updated its heartbeat row and needs to be reported as offline.

If an agent is unavailable in the physical navigation tree, it is offline.

Refer to 5.1 “Setting the heartbeat frequency” of *IBM Tivoli Monitoring: Implementation and Performance Optimization for Large Scale Environments*, SG24-7443, for a detailed discussion of this topic.

6.5 Situations

A *situation* is a defined set of conditions and actions that the Tivoli Monitoring V6.2 agent has been configured to recognize and respond to (“take action”). A situation can be a simple monitor threshold with the associated threshold values, or it can be a more complex Boolean formula. The major component of the situation is the “formula.”

Determine the time frames within which the situation will run. In addition, try for the longest sampling intervals possible, because sampling can increase

processor usage. Reserve short situation sampling intervals (1 minute or less) for highly critical applications and their most critical alerts. Prioritize situations by the user department. Short situation sampling intervals might be used, for example, to reduce the number of situations if increased processor usage is unworkably high, or possibly to add situations or shorten their intervals if there are sufficient resources to do so.

Best practices creating situations

Data for situations and events is collected at regular intervals. However, situations often do not need to be active on a 24x7 basis; many alerts might only be required during normal business hours, for example. The first way to control resource usage by situations is to stop and start them at the times that they are required. This control can be accomplished by creating policies (that start and stop situations at the right time) or externally by using an automation or scheduling software, for example, that starts and stops situations using Web services.

One of the most critical success factors of the project is discussing with user departments which and how to build situations. If you do not monitor critical components by using a situation or if you do not use the right thresholds, there is a risk of problems arising without being noticed.

If you set the situation intervals to be too short, the increased processor usage will be too high and the overall implementation might even become unreliable when the components cannot handle the workload any more. For example, if Tivoli Enterprise Monitoring Server is evaluating more situations than it can handle, or receiving more alerts, it starts to queue them, generating even more increased processor usage, which delays raising critical alerts. So, enable only the situations that are required. Use the same situations across similar systems without creating multiple situations for similar systems.

If the situation interval is too long, problems might be detected too late, thus the importance of in-depth planning and review with the user department and the need for the department to delegate a senior member to assist with this project. If the user representative is a junior member, this representative might not be sufficiently aware of critical performance factors and might even lack sufficient authority to defend the outcome of the discussions with this department.

Discuss the following items:

- Critical performance factors for the application or system. These performance factors need to be translated into data attributes to be monitored by using them in situations.
- What are the best values to check these attributes against? Do you need to create multiple situations to watch several levels of severity?

- If you do need several levels of severity for the same data, keep the sampling interval the same; the levels will be grouped together and the data will only be collected one time (see “Grouping situations” on page 216).
- Select realistic alert values. If a situation triggers and resets frequently, the Tivoli Enterprise Portal user is queried too many times and might lose reactivity over time. In addition, a situation that triggers and resets frequently can cause unnecessary increased processor and network usage to the Tivoli Enterprise Monitoring Server; processing is required to handle the alerts and also to store the data that led to the alert.
- At which intervals do these factors need to be checked? In addition, check whether the data that is required for the situation is collected in the background; certain Tivoli Enterprise Monitoring agent data (mainly Plex mainframe data) is not collected in an on demand manner, but rather at a fixed interval. These data collectors are running as UADVISOR probes in the Tivoli Enterprise Monitoring agent and Tivoli Enterprise Monitoring Server. The situation that uses this data needs to have an interval that is at least the same as the UADVISOR interval. Otherwise, the same UADVISOR collected data will be used twice or more for the situation evaluation.
- Which systems do we monitor? Group systems into user-managed system lists. Situations will then be distributed to these managed system lists. When a system needs to be added for the same kind of alerting later, the only change required will be to the managed system list.
- When the situation triggers, what advice can be given to the operator? This information will be put into the situation advice and will be presented to the operator when the alert is raised and advice is selected. This way, the operator is assisted in taking the correct actions that are consistent with the company’s policies.
- Is any automated action required? And if so, what? This discussion results in either a simple command to be executed on the system (reflex automation in the situation) or in a more complex set of automation scripts (that will be added into a policy).

Grouping situations

Grouping situations can potentially save many resources, but unfortunately, grouping situations cannot be set manually. The Tivoli Enterprise Monitoring Server decides whether or not to group situations. The following conditions must be met before a situation can be part of a group:

- All situations in the group use elements from the same attribute group.
- All situations must use the same interval setting.
- All situations must have autostart YES.
- A situation cannot contain an UNTIL clause.

- Distribution lists might be different.
- A situation cannot contain a display item.
- A situation cannot contain a take action item.
- The MISSING function is not supported.
- The SCAN and STR functions are not supported.
- Group functions on the attribute criteria (such as average and total) are not supported.
- Event persistence is not supported.

If the situation is grouped with other situations, the data collection required to get the attributes that are referenced in the situation is performed only once for the group. All situations in the group make use of the same data.

Tivoli Enterprise Monitoring Server performs situation grouping during startup. If the Tivoli Enterprise Monitoring Server finds a number of situations that are eligible for grouping, it creates a new internal situation that performs the data collection at the specified interval.

All grouped situations then compare their criteria to the data that is returned by the internal situation. These internal situations only exist for the duration of the Tivoli Enterprise Monitoring Server run. They get an internal name that starts with _Z_. The full name is built from the following parts: _Z_, *table name*, *sequence number*.

For example, on Windows, when grouping situations on table WTPROCESS, the grouped situation will be called _Z_WTPROCESS0. These situations are not added to the permanent situation tables in Tivoli Enterprise Monitoring Server (such as TSITDESC); however, because they are only temporary, they can only be seen in situation temporary tables, such as TSITSTSC.

To verify if any grouped situations are created, you can run the SQL statement that is shown in Example 6-4 on page 218 from a Tivoli Enterprise Portal view using custom SQL.

Example 6-4 SQL statement from a Tivoli Enterprise Portal view

```
SELECT SITNAME,
       ATOMIZE,
       DELTASTAT,
       LCLTMSTMP,
       NODE,
       ORIGINNODE,
       RESULTS,
       SITCOUNT,
       TYPE
FROM
O4SRV.TSITSTSC;
```

Because the grouping only occurs at Tivoli Enterprise Monitoring Server startup, any new situations or modifications will not benefit from grouping until the Tivoli Enterprise Monitoring Server is restarted.

Where is the situation evaluated

Situations can be evaluated at either the Tivoli Enterprise Monitoring agent or Tivoli Enterprise Monitoring Server. Ideally, all situations are evaluated at the Tivoli Enterprise Monitoring agent and as close to the datasource as possible. Unfortunately, the Tivoli Enterprise Monitoring agent is limited in its capacity to evaluate the situation. The evaluation is moved to the Tivoli Enterprise Monitoring Server in the following conditions:

- If the situation has attributes that cross Tivoli Enterprise Monitoring agents
- If advanced checking is used (string scan)

If situations cannot be evaluated at the Tivoli Enterprise Monitoring agent, the Tivoli Enterprise Monitoring Server takes over. You need to try to avoid evaluating situations at the hub Tivoli Enterprise Monitoring Server. All Tivoli Enterprise Monitoring agents need to report into a remote Tivoli Enterprise Monitoring Server.

Building a situation in the correct order

When starting to build a new situation, first create an overview of the attributes to test. Attributes will be tested from first to last, or from left to right on the Tivoli Enterprise Portal panel, in the order that they are entered in the situation.

We recommend knowing the data behind the attributes. The first test needs to return as few rows as possible. The next step can then further filter a limited set of rows.

For example, on Windows, to check if process XYZ uses more than *n* amount of real storage, test two attributes (process name and real storage usage). If we first test real storage use, the result set from this might contain multiple rows. Secondly, we need to check if our process name is among the returned rows. It is more efficient to first test on the process name. This way, the result will be one row. Then, follow this first test with the test on the storage usage just on this single row.

In addition, using complex conditions, such as string scan, sum, and average, is best performed on a limited result set; therefore, first evaluate the attributes against simple conditions to reduce the result set.

6.6 SOAP interface

Simple Object Access Protocol (SOAP) is a communications protocol, which is based on Extensible Markup Language (XML), that lets applications exchange information through the Internet. SOAP is platform-independent and language-independent. SOAP uses XML to specify a request and reply structure. It uses HTTP as the transport mechanism to drive the request and to receive a reply.

The IBM Tivoli Monitoring V6.2 Web Services solution provides you with an industry-standard open interface into IBM Tivoli Monitoring V6.2 solutions. This open interface provides easy access to performance and availability data, enabling you to use this information for advanced automation and integration capabilities.

IBM Tivoli Monitoring V6.2 Web Services implements a client/server architecture. The client sends SOAP requests to the IBM Tivoli Monitoring V6.2 SOAP server. The server receives and processes the SOAP requests from the client. Predefined SOAP methods let you perform many functions within the platform environment. You can begin to use SOAP methods immediately. You can also use IBM Tivoli Monitoring V6.2 SOAP methods as templates to create your own advanced methods.

SOAP works with any programming or scripting language, any object model , and any Internet wire protocol. The SOAP methods can be invoked through Perl, JavaScript™, VBSCRIPT, JSCRIPT, C++, and through a browser.

Important: Prior to using the IBM Tivoli Monitoring V6.2 solution, you must have a basic understanding of SOAP, XML, XML namespaces, and the Web Services Description Language (WSDL).

IBM Tivoli Monitoring V6.2 provides numerous SOAP methods for use with the Web Services integration. These methods enable you to dynamically query and control installations.

The SOAP methods can perform the following actions:

- Stop or start policies and situations.
- Retrieve attribute data that you can display in charts or reports.
- Open and close events.
- Make real-time requests for data.
- Issue SOAP requests as system commands in Tivoli Enterprise Portal Server.
- Generate daily operation summaries.
- Retrieve data in the Tivoli Date Warehouse.

Note: User access controls for SOAP are through the user IDs created within Tivoli Enterprise Portal Server. Define the access privileges for querying and modifying data through the SOAP interface.

Two methods for using the SOAP interface:

- Microsoft Internet Explorer
- The SOAP client command line utility

When you use the SOAP client in conjunction with Internet Explorer to issue SOAP requests, you can modify, if needed, the tags or the text. In contrast, the command line utility simply displays the output of the request at the command prompt.

SOAP methods

Table 6-3 on page 221 lists the SOAP methods in IBM Tivoli Monitoring V6.2.

Table 6-3 SOAP methods

SOAP method	Supported tags	SOAP tag usage examples
CT_Acknowledge Send an event acknowledgement into the IBM Tivoli Monitoring platform.	<name>The name of the situation. This is required. <source> The source of the event (agent name or monitoring server name). The acknowledge applies to all the active sources of the named alert if the source is not supplied. <data> "No data was provided" is inserted if not provided. <item>Display item. Optional: <userid> The user ID to access the hub monitoring server. "nnn.nnn.nnn.nnn" is inserted if not provided. <password> The password to access the hub monitoring server. Required for monitoring server/hub logon validation. <type> specifies the event type (sampled by default). The value can be "sampled" or "0", "pure" or "1", and "meta" or "2". <hub> Specifies the alias name of a remote hub that has been configured in the hub's list. The SOAP request is routed to this hub. <expire> Expires the acknowledgement after the number of minutes entered here.	<CT_Acknowledge> <hub>z/OSPROD</hub> <name>situation_from_CT </name> <source>CT_supported_system </source> <data>Jack is taking care of this failure</data> <item>subsystem</item> <userid>sysadmin</userid> <password>xxxxxxxx</password> <type>pure</type> </CT_Acknowledge><expire>60 </expire>

SOAP method	Supported tags	SOAP tag usage examples
CT_Activate Start a situation or a policy running on the IBM Tivoli Monitoring platform. Note that situations for agents connecting to a remote Tivoli Enterprise Monitoring Server cannot be started using this method.	<name> The name of the situation or policy. This is a required tag. <type> The type of object being activated. This tag is required. <userid> The user ID to access the hub monitoring server. "nnn.nnn.nnn.nnn" is inserted if not provided. <password> The password to access the hub monitoring server. Required for monitoring server/hub logon validation. Optional: <hub> Specifies the alias name of a remote hub that has been configured in the hub's list. The SOAP request is routed to this hub.	<CT_Activate> <hub>z/OSPROD</hub> <name>name_of_situation_or_policy </name> <type> situation</type> <userid>sysadmin</userid> <password>xxxxxxxx</password> </CT_Activate>

SOAP method	Supported tags	SOAP tag usage examples
CT_Alert Send an event into the IBM Tivoli Monitoring platform.	<name> The name of the situation. This is required. <source> The source of the event (agent name or monitoring server name). This is a required tag. <data> “No data was provided” is inserted if not provided or if no optional object.attribute tag provided. <item>Display item. Optional: <userid> The user ID to access the hub monitoring server. "nnn.nnn.nnn.nnn" is inserted if not provided. <password> The password to access the hub monitoring server. Required for monitoring server/hub logon validation. <hub> Specifies the alias name of a remote hub that has been configured in the hub’s list. The SOAP request is routed to this hub. <data><object.attribute> Returns the value of the attribute (or attributes) specified to the Initial Attributes view of the Event results workspace. <type> specifies the event type (default is sampled). The value can be "sampled" or "0", "pure" or "1", and "meta" or "2".	<CT_Alert> <hub>z/OSPROD</hub> <name>situation_from_XXX </name> <source>XXX_supported_system </source> <data> <NT_Logical_Disk.Disk_Name> C:</NT_Logical_Disk.Disk_Name> </data> <item>subsystem</item> <userid>sysadmin</userid> <password>xxxxxxxx</password> </CT_Alert> Note: When you specify object.attribute in the data tag, leave out any non-alphanumeric characters other than the underscore (_). For example, NT_System.%_Total_Processor_Time is entered as NT_System.Total_Processor_Time.

SOAP method	Supported tags	SOAP tag usage examples
CT_Deactivate Stop a situation or policy on the IBM Tivoli Monitoring platform. Note: Situations for agents connecting to a remote Tivoli Enterprise Monitoring Server cannot be stopped with this method.	<name> The name of the situation or policy. This is required. <type> The type of object (situation or policy). This is required. <userid>The user ID to access the hub monitoring server. "nnn.nnn.nnn.nnn" is inserted if not provided. <password> The password to access the hub monitoring server. Required for monitoring server/hub logon validation. Optional: <hub> Specifies the alias name of a remote hub that has been configured in the hub's list. The SOAP request is routed to this hub.	<CT_Deactivate> <hub>z/OSPROD</hub> <name>name_of_situation_or_policy</name> <type>situation</type> <userid>sysadmin</userid> <password>xxxxxxxx</password> </CT_Deactivate>
CT_Deactivate Stop a situation or policy on the IBM Tivoli Monitoring platform. Note: Situations for agents connecting to a remote Tivoli Enterprise Monitoring Server cannot be stopped with this method.	<name> The name of the situation or policy. This is required. <type> The type of object (situation or policy). This is required. <userid>The user ID to access the hub monitoring server. "nnn.nnn.nnn.nnn" is inserted if not provided. <password> The password to access the hub monitoring server. Required for monitoring server/hub logon validation. Optional: <hub> Specifies the alias name of a remote hub that has been configured in the hub's list. The SOAP request is routed to this hub.	<CT_Deactivate> <hub>z/OSPROD</hub> <name>name_of_situation_or_policy</name> <type>situation</type> <userid>sysadmin</userid> <password>xxxxxxxx</password> </CT_Deactivate>

SOAP method	Supported tags	SOAP tag usage examples
CT_EMail Send the output from another CT SOAP method, such as CT_Get, using e-mail through a Simple Mail Transfer Protocol (SMTP) server to a defined e-mail address. (not available on z/OS)	<server> smtp server name/network address is required. <sender> Sender's e-mail address is required. <receiver> Receiver's e-mail address is required. <subject> E-mail subject is optional. <message> E-mail message is optional. <attachmenttitle> Attachment title is optional. <request> When specifying a second-level request, such as CT_Get, each sub-request must be included within a <request> </request> tag. Optional: An id=" " element added to the <request> tag generates a <request id="XMLID"> element enclosing the corresponding response for that sub-request.	<CT_EMail> <server>smtp.server</server> <sender>myemail@something.com </sender> <receiver>youremail@whatever.com </receiver> <subject>Here's your data.</subject> <message>Table data supplied as attachment below. It is presented in comma-separated value (csv) format to be used by Microsoft Excel.</message> <attachmenttitle>tabledata.csv </attachmenttitle> <request id="XMLID"> <CT_Get> <object>NT_Process </object> <target>TIPrimary: DCSQLSERVER:NT</target> <userid>sysadmin</userid> <password>xxxxxxxx</password> </CT_Get> </request> </CT_EMail>
CT_Execute Runs the SOAP request that is stored in a file.	<filename> is required and specifies the file name that contains the SOAP request to be run. The file must reside in the \html directory. On z/OS, it must reside in RKANDATV.	<CT_Execute> <filename>execute1.xml</filename> </CT_Execute>

SOAP method	Supported tags	SOAP tag usage examples
CT_Export Send the output from another CT SOAP method, such as CT_Get, to a defined file. (not available on z/OS)	<filename> The name of the file to contain the exported data. This is a required tag. Note: When inserting the file name tag into a quoted string literal of certain programming languages, such as C++, back slashes need to be doubled.<warehouse/> Specifies that data is to be exported to the Tivoli Enterprise Portal data warehouse through ODBC. <filename> and <warehouse/> are mutually exclusive, but one must be supplied. <request> When specifying a second-level request, such as CT_Get, each sub-request must be included within a <request> </request> tag. Optional: An id=" " element added to the <request> tag generates a <request id="XMLID"> element enclosing the corresponding response for that sub-request. To the <filename> tag, you can add an optional date and time stamp variable. The variable is enclosed in dollar signs ($) and can contain a combination of *yy/mm/dd/hh/mm/ss* (for year/month/day/hours /minutes/seconds). The date and time stamp attributes can be specified in any order, except *mm* must be preceded by *yy* or *hh* to identify it as either month (after year) or minutes (after hours).	<CT_Export> <filename>g:\exchange\excel \ntprocess$*yymmddhhmmss*$.htm </filename> <request> <attach>prefix.xsl</attach> </request> <request id="XMLID"> <CT_Get> <object>NT_Process</object> <target>Primary:DCSQLSE RVER:NT</target> <userid>sysadmin</userid> <password>xxxxxxxx</password> </CT_Get></request> <request> <attach>suffix.xsl</attach> </request> </CT_Export> <filename>g:\exchange\excel \ntprocess$yymmdd$.htm</filename>

SOAP method	Supported tags	SOAP tag usage examples
CT_Get Receive a group of XML objects or individual XML objects from any IBM Tivoli Monitoring platform agent. You can use this to obtain real-time data. Important: When issuing a CT_Get request against a particular agent type, the monitoring server where the SOAP server is running must be configured and seeded for that agent type.	<object> The name of the object to be retrieved. Required (by default, retrieves all the public elements of an object). <userid>The user ID to access the hub monitoring server. "nnn.nnn.nnn.nnn" is inserted if not provided. <password>The password to access the hub monitoring server. Required for monitoring server/hub logon validation. Optional: <target> Name of the agent. Caution: Defaults to "*ALL". Retrieves all available targets. <history>Y retrieves historical data if available. <results>PARSE retrieves status history event attributes. Only valid for Status_History object. Multiple: more than one can be specified. <attribute>Attribute name of object. This tag can be specified multiple times. <hub> Specifies the alias name of a remote hub that has been configured in the hub's list. The SOAP request is routed to this hub. <afilter> Returns rows meeting filter criteria, such as attribute; operator; value operators: EQ, NE, GE, GT, LE, LT, or LIKE. Like pattern characters: '%' matches any single character. ' * ' matches one to many characters. Only supported for character attributes. Multiple afilters are only supported as conjuncts, for example, using AND to join together.	<CT_Get> <hub>z/OSPROD</hub> <object> NT_System</object> <target> Primary:DCSQLSERVER:NT</target> <userid>sysadmin</userid> <password></password> <history>Y<history> <attribute>Server_Name</attribute> <attribute>Processor_Queue_Length</attribute> Note: When you specify an attribute in the attribute tags, leave out any non-alphanumeric characters other than the underscore (_). For example, %_Total_User_Time is entered as Total_User_Time. <afilter>Write_Time;GT;1020804</afilter> <afilter>Write_Time;LT;1020805</afilter> </CT_Get>

SOAP method	Supported tags	SOAP tag usage examples
CT_Redirect Reroute a SOAP request to another registered SOAP method outside of the domain of the IBM Tivoli Monitoring platform.	<request endpoint=" "> This is a required tag. The <request endpoint= " "> value must specify the target of the redirected SOAP request. The entire XML supplied as the value of the request element is sent to that endpoint. When CT_Redirect is specified within a second-level request, such as CT_Export, the <endpoint=" "> attribute is specified *only* within the CT_Redirect method.	<CT_Redirect> <request endpoint= \"http://services.xmethods.net: 80/soap/servlet/rpcrouter\"> <SOAP-ENV:Envelope xmlns:SOAP-ENV= \"http://schemas.xmlsoap.org /soap/envelope/\"> <SOAP-ENV:Body><ns1:getTemp xmlns:ns1=\"urn:xmethods-Temperature \"SOAP-ENV:encodingStyle= \"http://schemas.xmlsoap.org/ soap/encoding/\"> <zipcode>93117</zipcode> </ns1:getTemp> </SOAP-ENV:Body> </SOAP-ENV:Envelope> </request> </CT_Redirect>"
CT_Reset Send an event reset (close event) to the IBM Tivoli Monitoring platform.	<name> The name of the situation. This is a required tag. <source> The source of the event (agent name or monitoring server name). The reset applies to all of the active sources of the named alert if the source is not supplied. <item>Display item. Optional: <userid> The user ID used to access the hub monitoring server. "nnn.nnn.nnn.nnn" is inserted if not provided. <password> The password used to access the hub monitoring server. Required for monitoring server/hub validation. <hub> Specifies the alias name of a remote hub that has been configured in the hub's list. The SOAP request is routed to this hub. <type> Specifies the event type (default is sampled). The value can be "sampled" or "0", "pure" or "1", and "meta" or "2".	<CT_Reset> <hub>z/OSPROD</hub> <name>situation_from_CT </name> <source> CT_supported_system </source> <item>subsystem</item> <userid>sysadmin</userid> <password>xxxxxxxx</password> </CT_Reset> Note: Sampled events can be closed only if the situation has been stopped or deleted. Use the <type> tag if CT_Reset will be closing a pure event.

SOAP method	Supported tags	SOAP tag usage examples
CT_Resurface Resurface an acknowledged event in the IBM Tivoli Monitoring platform.	<name> The name of the situation. This is required. <source> The source of the event (agent name or monitoring server name). The resurface applies to all the active sources of the named alert if the source is not supplied. <item>Display item. Optional: <userid> The user ID used to access the hub monitoring server. "nnn.nnn.nnn.nnn" is inserted if not provided. <password>The password used to access the hub monitoring server. Required for monitoring server/hub validation. <hub> Specifies the alias name of a remote hub that has been configured in the hub's list. The SOAP request is routed to this hub. <type> Specifies the event type (default is sampled). The value can be "sampled" or "0", "pure" or "1", and "meta" or "2".	<CT_Resurface> <hub>z/OSPROD</hub> <name>situation_from_CT </name> <source> CT_supported_system </source> <item>subsystem</item> <userid>sysadmin</userid> <password>xxxxxxxx</password> </CT_Resurface>
CT_WTO Send a Universal Message into the IBM Tivoli Monitoring Platform.	<data> The message to be sent. This is required. <category> This tag is optional/blank is the default. <severity>This is optional, blank is the default. <userid> The user ID used to access the hub monitoring server. "nnn.nnn.nnn.nnn" is inserted if not provided. <password> The password used to access the hub monitoring server. Required for monitoring server/hub validation. <hub> Specifies the alias name of a remote hub that has been configured in the hub's list. The SOAP request is routed to this hub.	<CT_WTO> <hub>z/OSPROD</hub> <data> This is Universal Message </data> <category>Critical Messages </category> <severity> High Severity </severity <userid>sysadmin</userid> <password>xxxxxxxx</password> </CT_WTO>

6.7 Workspaces

When creating views, avoid using the thresholds selection in the view. Instead, a better practice is to create a query that focuses on the data to be displayed. Build the query so that the necessary selections are made at the query level and only the required attributes are returned. When making the selection at the query level, rather than by setting these thresholds on the Thresholds tab, you are asking the Tivoli Enterprise Monitoring agent to return only a limited result set (using less CPU and storage at the Tivoli Enterprise Monitoring agent, Tivoli Enterprise Monitoring Server, and Tivoli Enterprise Portal Server and reducing increased network traffic). However, if the selection is made on the Thresholds tab, the Tivoli Enterprise Monitoring agent is asked to return a (possibly much) larger result set and the selection of the data for visualization will only occur at the Tivoli Enterprise Portal Server level.

The only exception to this rule is when you are building a workspace that contains several views that use extremely similar data; if a single query can be used for all views on the same workspace, that query will only be executed once. The individual views can then further select a subset of the query's result set and cater to additional visualization "make up." Using multiple queries on the same workspace slows down the response time for the user, because the queries will be executed one by one. In addition, network traffic can increase.

Limit the distribution of Navigator items on the Logical view to the systems for which the reports are required. Running the queries and collecting the data for systems that are not of interest for the user is a waste of resources. To ease distribution, we recommend that you create user-managed systems lists that group systems in the way that users look at them. For example, a user-managed system list can be created for all Windows database servers or for all servers that run a specific application.

Tivoli Enterprise Portal paging is an important consideration. By default, Tivoli Enterprise Portal displays reports in pages of 100 rows. We recommend that you keep this setting; if more rows are allowed per page, or if no paging is selected, Tivoli Enterprise Portal needs more storage on the client side to handle all of the data. This situation causes OS paging if sufficient real storage is unavailable and greatly slows down the performance of Tivoli Enterprise Portal. Ideally, reports must not exceed 100 rows.

Be aware that all pages are stored at Tivoli Enterprise Portal Server. If your query returns a large result set, it disrupts memory at Tivoli Enterprise Portal Server. Because Tivoli Enterprise Portal Server has to service multiple users, it can quickly run out of storage and start OS paging. This situation is detrimental to response times.

Refrain from using autorefresh on report panels to enhance the performance. If you want to regularly check if a specific attribute is within an acceptable range, do not use reports to check this condition, but rather create a situation to watch over the resource. The situation is executed at the lowest level component, at Tivoli Enterprise Monitoring agent if possible, and does not require increased processor and network usage at the Tivoli Enterprise Monitoring Server and Tivoli Enterprise Portal Server at every interval, as a report update does.

Specifically, if multiple users monitor the same resources or workload, create situations to watch the performance. That way, the detailed data from monitoring this resource will only be created once (by the situation) and not multiple times (for every user).

7

Administration

The Administration section of any certification exam is typically extremely straightforward. Between real-world experience and understanding the product guides and this book (including the information in the screen captures), all of the questions can be answered easily. In addition, because administration is such a large part of any product, it can be an extremely large section of an exam.

We divide administration into sections to help you focus on the areas covered by the certification exam and, more importantly, to assist you in the day-to-day usage of IBM Tivoli Monitoring V6.2.

This chapter discusses the administration of IBM Tivoli Monitoring V6.2 through the following topics:

- Situation editor
- Workspace
- Manage Tivoli Enterprise Monitoring Services
- Historical data collection
- Integration with other Tivoli event systems
- IBM Tivoli Monitoring V6.2 command line

7.1 Situation editor

The Situation editor brings intelligence to the IBM Tivoli Monitoring V6.2 suite by allowing for more complex correlation to occur at the agent level. It also removes the complexity of introducing correlations found in versions of IBM Tivoli Monitoring prior to Version 6.1.

A *situation* is a defined set of conditions and actions that the Tivoli Monitoring V6.2 agent has been configured to recognize and respond to ("take action"). A situation can be a simple monitor threshold with the associated threshold values, or it can be a more complex Boolean formula. The main component of the situation is the "formula."

A basic threshold formula is usually a threshold value or range. For example, a basic threshold formula can signal a warning if the CPU utilization goes higher than 50% but stays lower than 75%. You can also set a situation formula for a time period, for example, a formula for checking that a condition exists on, or between, Monday and Saturday.

7.1.1 Understanding the terms

For this discussion, you need to understand the following terms, as defined in *IBM Tivoli Monitoring User's Guide, Version 6.2.0*, SC32-9409:

- Event: An action or an occurrence, such as running out of memory or completing a transaction, that can be detected by a situation. The event causes the situation to become true and an alert to be issued.
- Event indicator: The colored icon that displays over a Navigator item when an event opens for a situation.
- Monitor interval: A specified time, scalable to seconds, minutes, hours, or days, for how often the monitoring server checks to see if a situation has become true. The minimum monitor interval is 30 seconds; the default is 15 minutes.
- Persistence: Indicates that a situation must remain true for a specified number of consecutive samples before an event is reported to the Tivoli Enterprise Portal.
- Pure event: A *pure event* is an event that occurs automatically, such as when an out of paper condition occurs on the printer or when a new log entry is written. Situations written to notify you of pure events remain true until they are manually closed or automatically closed by an UNTIL clause.
- Sample: The data that the monitoring agent collects for the server instance. The *interval* is the time between data samplings.

- Sampled event: *Sampled events* happen when a situation becomes true. Situations sample data at regular intervals. When the situation is true, it opens an event, which gets closed automatically when the situation goes back to false (or you can close it manually). Sampled events drive the historical data collection.
- Situation: A *situation* is a set of conditions that are measured according to criteria and evaluated to be true or false. A condition consists of an attribute, an operator (such as greater than or equal to), and a value. It can be read as, "If system condition compared to value is true." An example of a situation is "IF - CPU usage > - 90% - TRUE." The expression "CPU usage > 90%" is the situation condition.
- State: The severity of the situation event: critical, warning, or informational. Indicated by a colored event indicator, the state is set in the Situation editor and can vary for different Navigator items.
- Status: The true or false condition of a situation.
- View: A window panel, or frame, in a workspace. It might contain data from an agent in a chart or table, or it might contain a terminal session or browser, for example. A view can be split into two separate, autonomous views.

7.1.2 Creating a situation

In order to create a situation, you must have Modify authority. Modify authority allows the user to create new situations and to edit and to delete situations in the Situation editor. View authority allows the user to see situations in the Situation editor and to see acknowledgements in the Event Acknowledgement window.

Note: *IBM Tivoli Monitoring Administrator's Guide, Version 6.2.0*, SC32-9408, describes all of the permissions that are required for various IBM Tivoli Monitoring V6.2 operations.

Starting the Situation editor

The Situation editor can be launched by either right-clicking a navigator item and selecting **Situations**, by right-clicking a situation in the event flyover list or the situation event console and selecting **Edit Situation**, by clicking the Situation Editor icon in the toolbar, or by pressing Ctrl+E in the default workspace of the Physical Navigator view.

Use the first method when creating a new situation to automatically associate it with a navigator item. The last three methods do not allow you to associate (or disassociate) a situation with a navigator item or change its state or sound. Figure 7-1 on page 236 shows the open Situation editor.

Note: Situations are only in the pop-up menu of Navigator items that have managed systems assigned. In the Navigator Physical view, managed systems are preassigned to every item except those items at the operating platform level (such as Linux systems) and cannot be changed. In the Navigator Logical and custom views, managed systems are assigned when you create a Navigator item or edit its properties.

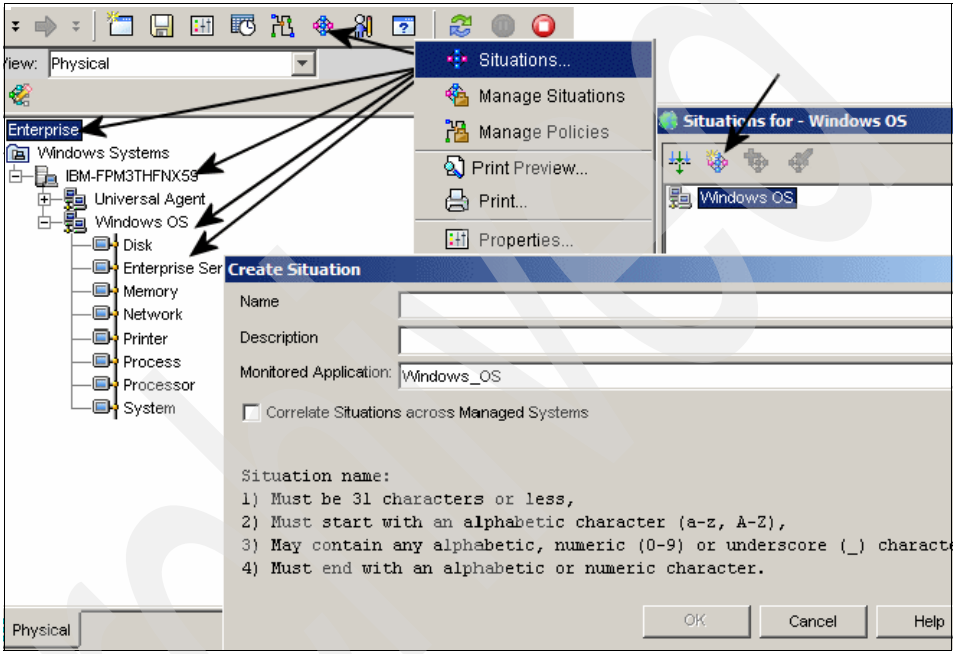


Figure 7-1 Open Situation editor

Naming the situation

The name must begin with a letter and have fewer than 32 letters and numbers and can include underscores (_). The description must be fewer than 64 characters. The description is displayed in the Situation editor, in the Manage Situations window, and when you select the situation for embedding in or correlating with another situation.

Creating the formula

After filling in the name of the situation, the Select condition dialog box is displayed. Select the type of condition that you want, either Attribute Comparison or Situation Comparison, and the associated Attribute Group, Attribute Item, or Situation Name entries.

The Situation editor window is now displayed. Here, you can modify the description, formula, sampling interval, sound, and state. The tabs provided at the top enable you to choose to which systems to distribute, enter expert advice, define actions to take, and set an UNTIL event for pure events (Figure 7-2).

Note: If you open the Situation editor from the toolbar, the situation that you just created will not be associated with any Navigator items and no event indicator is displayed when the situation becomes true. You must associate a situation with a Navigator item or change its state and click **Apply**.

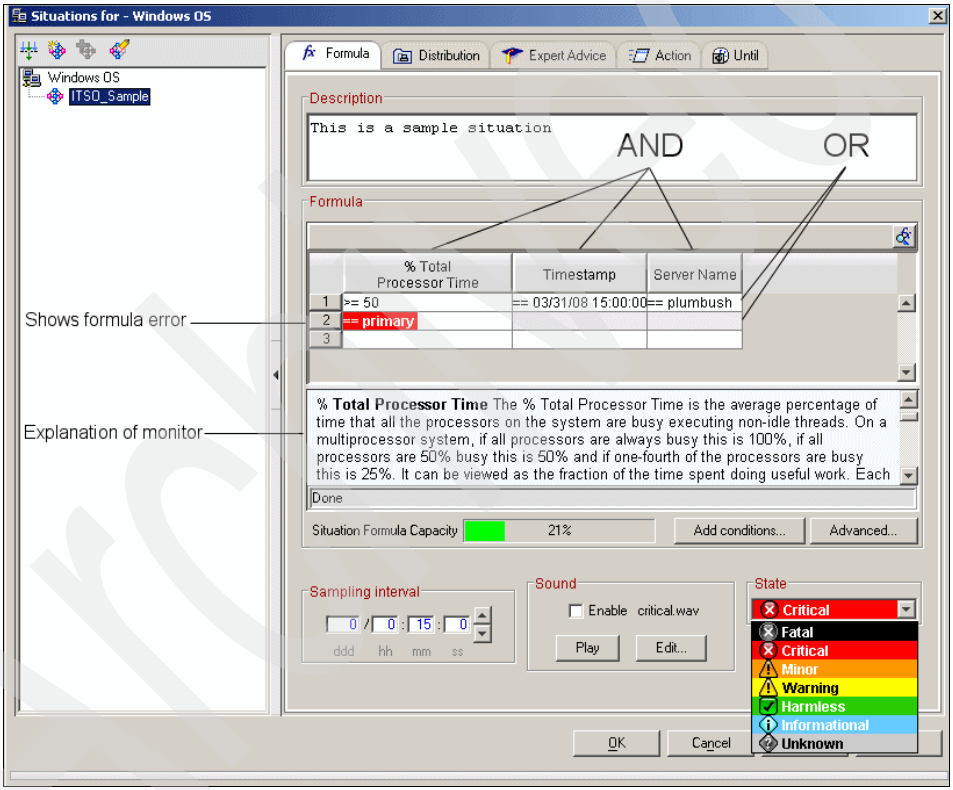


Figure 7-2 Situation editor for a sampled event

Description

The description field is limited to 64 characters and can be used to enter a brief, plain text definition of your situation.

Formula

When creating the situation formula, click inside the cell under the column heading and compose an expression consisting of a function, a relational operator, and a test value. Next, we briefly describe the various elements that make up the formula expression:

- Formula functions:

  Formula functions are broken up into two categories. The functions available for a particular attribute depend on its characteristics. Access these functions by clicking on the 'V' icon under the attribute column heading:

  - Cell Functions

    VALUE (default), CHANGE, DATE, MISSING, PCTCHANGE, SCAN, STR, and TIME

  - Group Functions

    AVG, COUNT, MAX, MIN, and SUM

- Relational operators:

  To change a relational operator, click the '==' icon under the attribute column heading. Valid operators are:

  - == Equal
  - != Not equal
  - > Greater than
  - >= Greater than or equal
  - < Less than
  - <= Less than or equal

- Attribute characteristics:

  The three major types of attributes are:

  - Numeric

    Numeric attributes represent a count, percentage, seconds, bytes, or another unit of measurement.

  - Text

    Names, such as the host name or a process name, are text attributes. Usually, the time stamp and enumerated attributes are treated as text attributes. Single quotes are required around multiple-word text values.

– Time stamp

  Most attribute groups have a time stamp attribute. Certain attribute groups have different names, such as Start Date and Time. You can tell which attributes are time stamp attributes by their format in a table view, which is *mm/dd/yy hh:mm:ss*.

Another type of attribute is treated as a numeric or text attribute:

– Enumerated

  Enumerated attributes have a predefined set of values and the tabular editor supplies a list from which to choose. For example, the WebSphere MQ attribute, Action to Take has values of n/a, delete, create, and discover.

When building a formula, the rows indicate “OR” statements, and the columns indicate “AND”. Therefore, if you want to build a situation that can turn true for any number of met conditions, put them in rows. When building formulas for which all conditions must be true, use columns.

The section immediately under the formula window is context sensitive and will display information regarding the attribute that you are editing in the formula window.

Add conditions, Advanced, Sampling interval, Sound, and State

To add another condition to the situation, click **Add conditions** and select the condition type, attribute group, and attributes, or situations that you want to add to the situation.

To add situation persistence or a display item to the situation, click **Advanced**.

- Situation Persistence: Specify how long a situation must remain true before an event is reported to the Tivoli Enterprise Portal by indicating the number of consecutive samples that must test true.
- Display Item: If you set a display item that is set for a multiple-row attribute group, the situation continues to look at the other rows in the sampling and opens more events if other rows qualify.

The **Sampling interval** is not used for pure events, such as the Universal Agent. This interval is the amount of time between the monitor collecting information to satisfy your formula’s attributes.

The **Sound** gives you the ability to set up an audible alert for a situation that equals true. This alert will *only* be heard on the portal console; it will *not* be heard on an IBM Tivoli Enterprise Console or a managed system.

The **State** indicates the severity of the message. The possible values are:

- Critical
- Warning
- Informational

Selecting systems for distribution

The Distribution tab is straightforward and enables the user to choose which managed systems will receive this situation (Figure 7-3). It does contain managed lists, so you can push a situation to a group of systems.

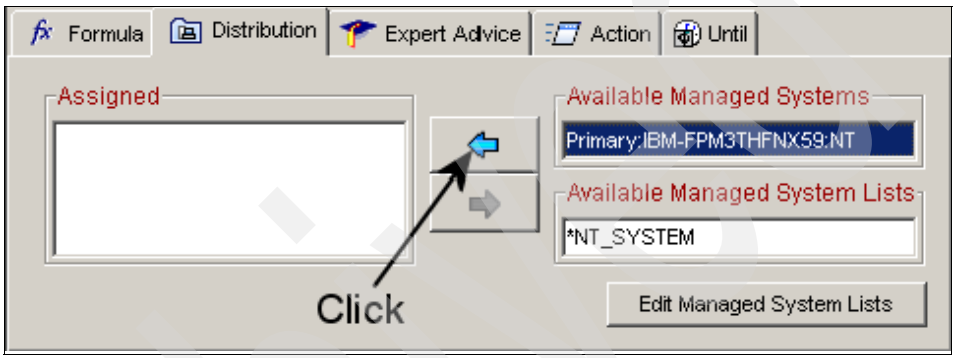


Figure 7-3 Distributing a situation

Consider the following items:

- If you change an embedded situation, you must restart each situation that embeds it.
- The properties of the embedding situation, such as the monitoring interval, override the properties of the embedded situation.
- You must distribute each embedded situation to the same managed systems as the embedding situation. Otherwise, the embedding situation does not run.
- When you stop a situation that embeds other situations, only the embedding situation is stopped; the embedded situations continue to run.
- Situations are stored at the hub monitoring server. It is possible that while you were building the situation that any of the embedded situations might have been deleted. If this deletion happens, a message will tell you that the embedded situation is missing when you attempt to save your changes. You need to remove the embedded situation from this situation before you can save your changes. You can always create a new situation to be embedded or find another one that is the equivalent and embed that one.

- In the unlikely event that two users attempt to save a situation with the same name simultaneously, an error occurs, ensuring that one situation does not overwrite another situation.
- If you are running multiple versions of a monitoring agent, you will be able to distribute a situation only to the managed systems that the version supports.

Expert advice

The Expert Advice tab provides information to someone watching the console for alerts. It contains information related to the alert and can be provided in the following formats (refer to *IBM Tivoli Monitoring User's Guide, Version 6.2.0*, SC32-9409, for more details):

- HTML
- URL
- JavaScript (limited support)
- Text scripting language

Action

The Action feature in a situation is similar to "Run Program" in past versions of Tivoli Monitoring.

Leave **System Command** selected or select **Universal Message**.

For a system command, write the command exactly as you enter it manually for the application and operating platform on which it is running.

For a Universal Message, write the category, severity, and the text to display in the Universal message console view:

- Category of messages to see (for example, critical, warning, information), up to 16 characters
- Severity of the message, one word of up to 8 characters, such as 1 or high
- Message text when the situation occurs, up to 256 characters

If the condition is true for more than one monitored item:

- Only take action on the first item to issue the command on only the first row that meets the condition.
- Take action on each item to issue the command once for each row of data returned that meets the condition.

For example, if the situation fires when any process uses more than 80% of the CPU, you can issue a command to terminate just the first process that meets this criteria, or you can issue a command to terminate all processes that meet the criteria.

The “Where should the Action be executed (performed)” option determines where to perform the action, on the system where the agent resides or the monitoring server to which it is connected, and provides the following choices:

- Execute the Action at the Managed System (Agent)
- Execute the Action at the Managing System (TEMS)

If you are sending a Universal Message, the action takes place at the monitoring server.

For the “If the condition stays true over multiple intervals” field, you have the following choices:

- Do not take action twice in a row to execute the command or universal message once and not every time that incoming data matches the condition.
- Take action in each interval to invoke the command or issue the universal message when the situation is true in an interval, irrespective of its state in the previous interval.

Figure 7-4 shows the Action tab.

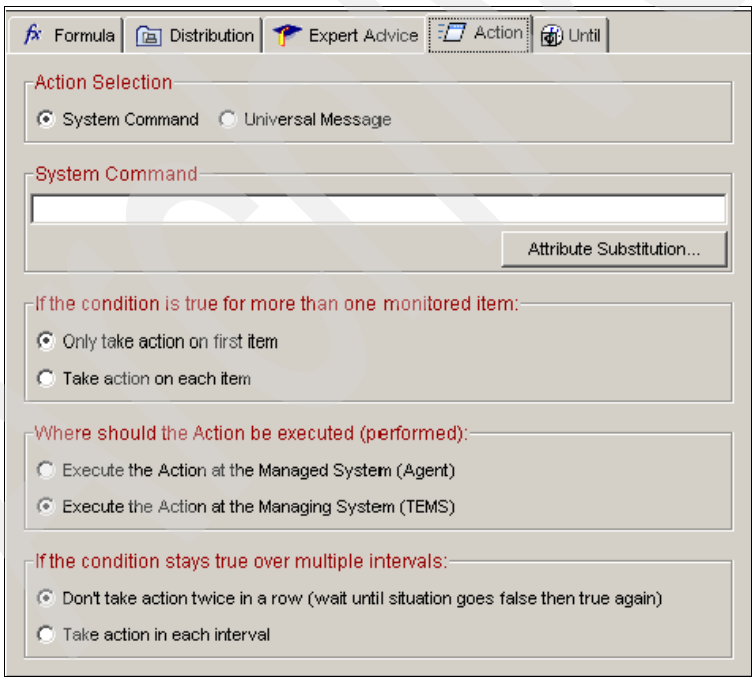


Figure 7-4 Take Action tab

The Until tab

The Until tab (Figure 7-5) enables you to close an open event for this situation based on two criteria:

- Another Situation is TRUE

  Choose another situation from which a TRUE event will close your current situation.

- Interval Expires

  Specify a time that the event will automatically expire.

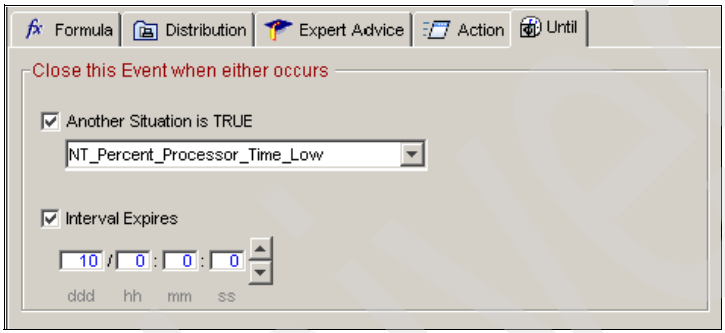


Figure 7-5 Until tab

7.1.3 Association

When you create a situation, it must be associated with a Navigator item before an event indicator can display there. Association is done manually for situations created in the Situation editor when it was opened from the toolbar. When you associate a situation with a Navigator item, the situation state (Critical, Warning, or Informational) and sound are also associated with the item. You can have different states and sounds for the same situation.

Note: Your user ID must have View Situation and Workspace Author Mode permissions to use this function.

7.1.4 Predefined situations

Several predefined situations are available under the Tivoli Enterprise Monitoring Server branch of the Situation editor. The Tivoli Enterprise Monitoring Server situations are not distributed initially:

- **NonPrimeShift** checks for times after 5 PM and before 8 AM from Mondays to Fridays.

- **PrimeShift** checks for the prime shift time of 8 AM to 5 PM from Mondays to Fridays.
- **QOMEGAMON_ONLINE** checks that the monitoring server has taken a data sample at the managed system. The sampling occurs every 10 minutes by default and at zero seconds, such as 09:00. If the seconds are greater than zero, it indicates the managed system is not online.
- **Weekday** becomes true any day from Monday through Friday. This situation is useful for inclusion in policies that are used to start a situation running on weekdays or to stop a situation from running on weekdays. It is used in conjunction with the Weekend policy, described next.
- **Weekend** becomes true on Saturdays and Sundays. This situation is useful for embedding in situations to run on weekends or to stop a situation from running on weekends. It is used in conjunction with the Weekday policy, described earlier.

7.2 Workspace

In this section, we discuss workspace administration and creating views in a workspace.

7.2.1 Workspace administration

☑ The Workspace Author Mode enables the user to create and edit workspaces, links, and terminal emulator scripts. If you disable Workspace Author Mode, the user cannot make any of these changes but can continue monitoring and responding to alerts; the tools can still be seen, but they are disabled. The Workspace Author Mode does not allow users to stop agents that are actively displaying data on the workspace and differs from the Workspace Administration Mode (described next) because changes affect only the user who performed the action.

☐ The Workspace Administration Mode is available only for the SYSADMIN user ID and new IDs made from it from the Create Another User window. When Administration Mode is enabled, changes that you make to workspaces affect all of the users that are connected to the same portal server. When it is disabled, workspace changes that you make are not shared with other users.

Note: Select **Do not allow modifications** in the Workspace Properties whenever you create or edit a workspace in Administration Mode. Otherwise, if a user edits that workspace, you no longer own the workspace and cannot override that user's changes.

7.2.2 Views

The predefined workspaces for your IBM Tivoli Monitoring product consist primarily of chart and table views. You can save them as new workspaces and customize them with more than a dozen types of views.

Data views

The table and chart views are the first step to getting something meaningful from the data that is being collected. When you understand what values and states are causing problems, you can refine your views to show what is important.

The table view and the chart view provide current and historical information about monitoring data from Tivoli Enterprise Monitoring agents, such as system performance and configuration:

- *Pie charts* show portions of a whole (such as a percentage).
- *Bar* and *plot charts*, as well as *gauges*, show the values of each attribute.

Table views

Table views show current data that is retrieved from a monitoring agent and show one column for every attribute. The table reports a single row of data or multiple rows, depending on the nature of the attribute group.

The table view also has features for refining the display to suit your needs. These features include adjusting column width, locking columns, and using drag and drop to change the order of columns. You can also re-sort column data in ascending or descending sequence by clicking on the column heading.

Note: You can also build a query that specifies a sort order, which is necessary for multiple-page tables if you want all of the rows sorted and not just those rows in the current page.

Chart views

Your predefined workspaces can have any of five chart views (see Table 7-1 on page 246:

- *Pie Chart* has a slice for every data point in a single data series (row). Pie charts are well suited for showing the proportional value of related attributes to a whole, such as the percentage attributes that show how memory is being used.
- *Bar Chart* displays a bar for each data point. Bar charts are best suited for comparing values among related attributes. The stacking bar chart is well suited for showing multiple values for the same attribute.

- *Plot Chart* shows changes over a period of time by drawing a continuous line from one data point to the next data point with one data point for each data sampling and one line for each selected attribute. The plot chart can be used for plotting multiple-row attribute groups (or historical data from a single-row attribute group) and multiple managed systems. You can also control the refresh rate of the plot chart so that it is independent of the refresh rate of the workspace as a whole. The plot chart is well suited for showing trends over time and among related attributes.
- *Circular Gauge* shows the proportional amount of a data series with one gauge for each chosen attribute. This type of chart is well suited for showing individual elements that change frequently, such as percentage user time.
- *Linear Gauge* shows the collective value of every item in a single data series with one gauge for each chosen attribute. This type of chart is well suited for showing cumulative values.

Table 7-1 Chart types: Each type of chart is best suited for displaying a certain type of data

Chart type	Best for	Multiple attributes	Multiple rows	Multiple managed systems	Time span
Pie Chart	Showing proportional value to the whole	One slice per attribute	One pie for each row	One pie for each managed system	Yes
Bar Chart	Comparing values among related attributes	One bar per attribute. Stacking bars show one segment per attribute	One set of bars for each row. Stacking bars show one bar per row	One set of bars for each managed system	Yes
Plot Chart	Showing trends over time and among related attributes	One line per attribute; one data point for each data sampling	Yes	Yes	Yes
Circular Gauge	Showing individual elements that change frequently	One gauge per attribute	No	No	No
Linear Gauge	Showing cumulative values	One gauge per attribute	No	No	No

Creating views with the Query editor

The following permissions are applicable for creating views with the Query editor:

- View: Enables the user to access the Query editor through the Properties editor and to select a query for the selected table or chart.
- Modify: Enables the user to create, edit, and delete queries in the Query editor.

Note: If you do not see the Queries tool, your user ID does not have View or Modify Query permissions; if you can open the Query editor but the tools are disabled, your user ID does not have Modify Query permission.

Note: Anyone with permission to create custom queries obtains access to all of the Open Database Connectivity (ODBC) datasource names (DSNs) created at the Tivoli Enterprise Portal Server. Add database user IDs (to be used in the DSN) to your database software, making sure to restrict user access to only those tables, columns, and so on allowed by your organization's security policies.

In the following section, we describe how to create views with the Query editor, illustrating this process with screen captures. For this example, we have the "Enterprise" highlighted in the physical view. Our first graph shows the system's physical memory usage in a bar graph.

We follow these steps:

1. Because this example compares data from multiple systems, we chose a bar graph. Start by clicking the bar graph icon (highlighted in Figure 7-6). Your cursor switches to a hand. Move the hand over the window panel where you want to have the bar graph.

Figure 7-6 Table, pie chart, bar chart, plot chart, circular gauge, and linear gauge toolbar

2. The following window (Figure 7-7 on page 248) opens after you choose the window panel in which you want to place the graph. From here, you can start by assigning a query that will provide the data for the bar graph.

   Click **Click here to assign a query**.

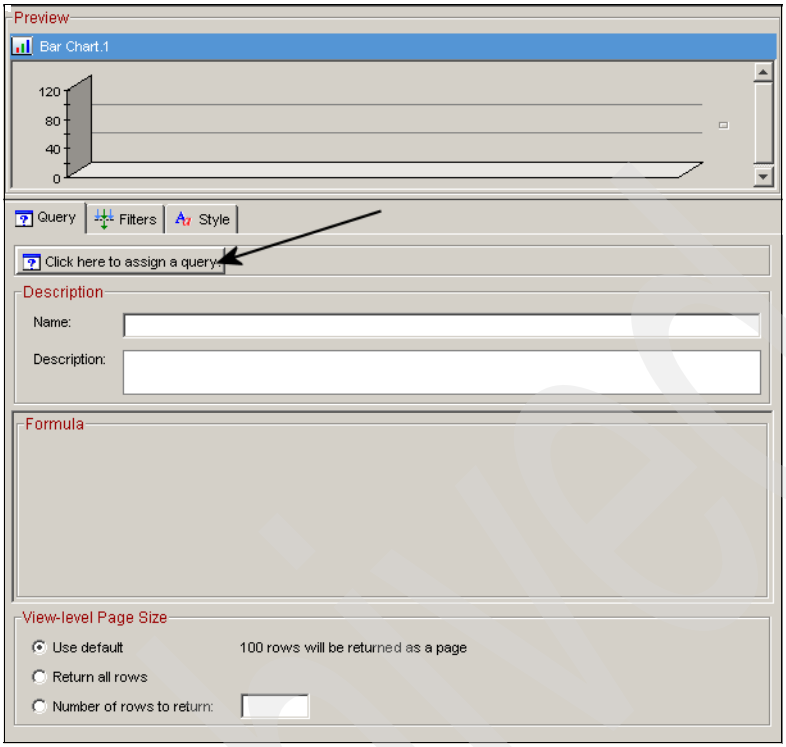


Figure 7-7 Situation editor

3. In the window that opens, you can either create a new query or, as in Figure 7-8, you can copy another query. If you choose to copy another query, you can pre-filter the columns from which you will have to choose. The use of custom queries that pre-filter the data used in a table or chart causes faster data retrieval by requiring less agent collection overhead and ensures that no extraneous data is displayed.

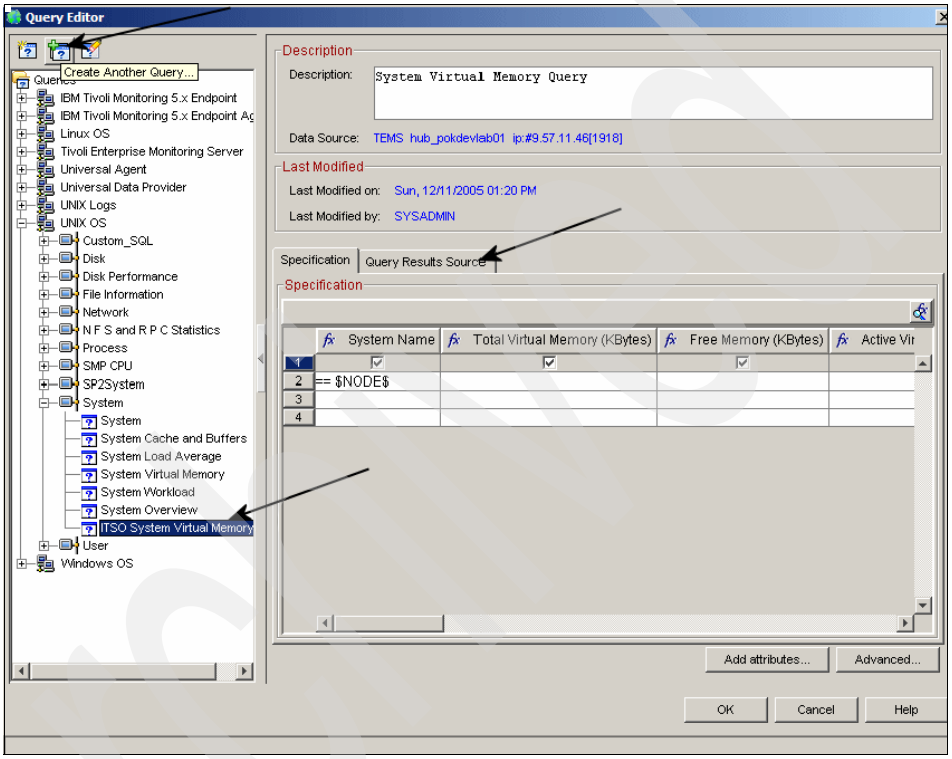


Figure 7-8 Building the query

Note: The attributes in a query can be from one group only; you cannot mix attributes from multiple groups in the same query.

4. In the Query Results Source table, select the systems that will be part of this query. In order to be able to change this value, select **Let user assign explicitly**. Figure 7-9 shows an example of the Query Results Source table.

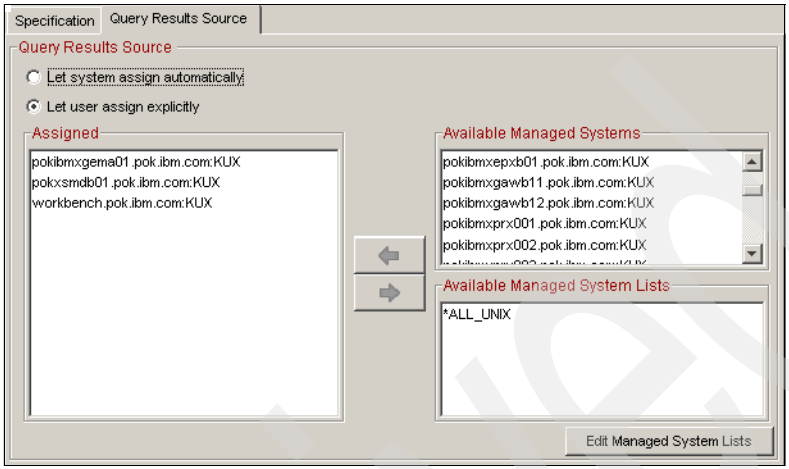


Figure 7-9 Assign systems to be included in the query

5. When you copy a query, two buttons become active on the Correlation tab. On the Advanced Options panel, you can sort or group the data (sort and group are mutually exclusive). Refer to Figure 7-10.

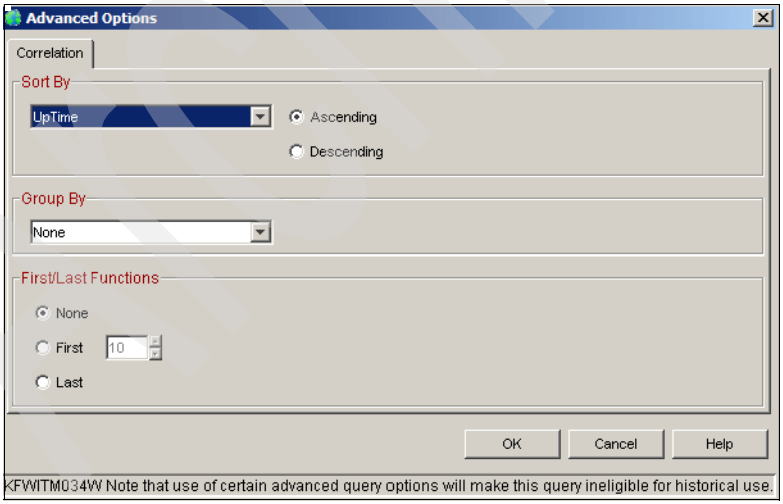


Figure 7-10 Advanced Options

6. Click **OK** to leave the Assign Query menus and return to the graph properties. Here, you can apply filters for what data will be seen. This action is frequently referred to as *post-filtering*. You can also sort the data, which will affect your graph, by clicking the label in the Data Snapshot™ section.

   Figure 7-11 shows the Filters tab.

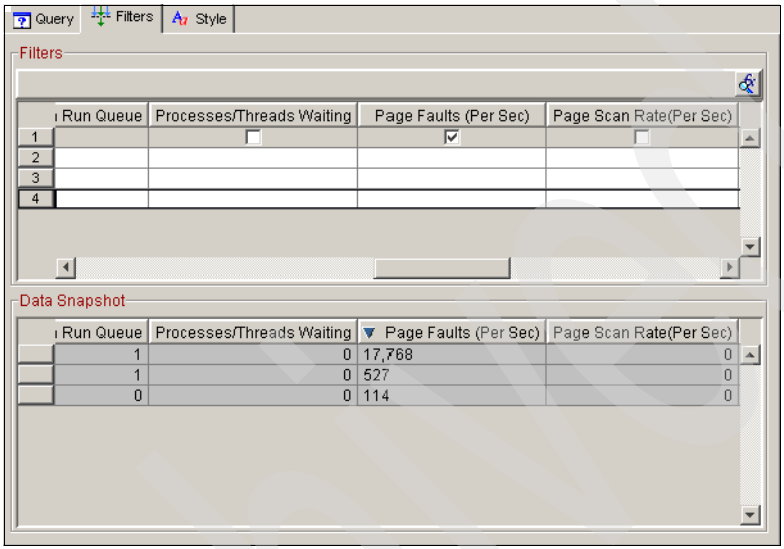


Figure 7-11 Adding filters

7. The Style tab enables you to customize your chart, including (but not limited to):

   – Vertical as opposed to horizontal (swap the axes)
   – Change colors
   – Move or add the legend
   – Add axis labels
   – Add a title
   – Two-dimensional (2-D) as opposed to three-dimensional (3-D) objects

   Figure 7-12 on page 252 shows how to change the style of the chart, and Figure 7-13 on page 252 shows the resulting graph.

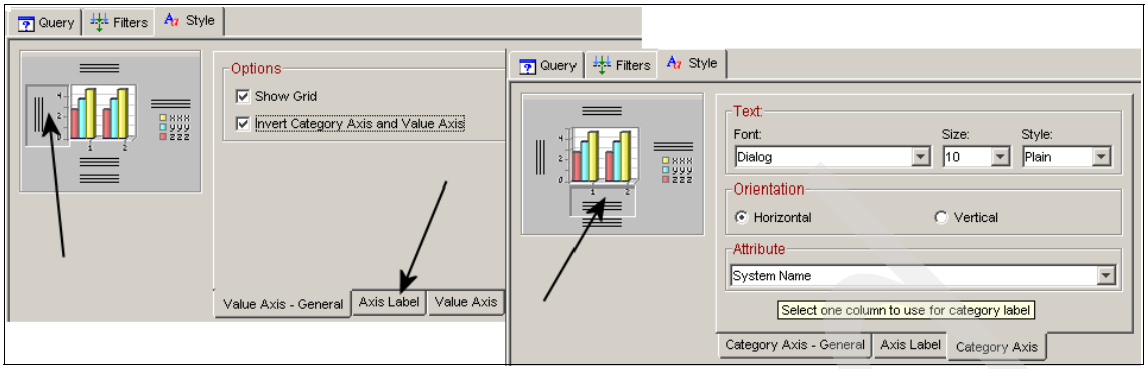


Figure 7-12 Change the style of the chart

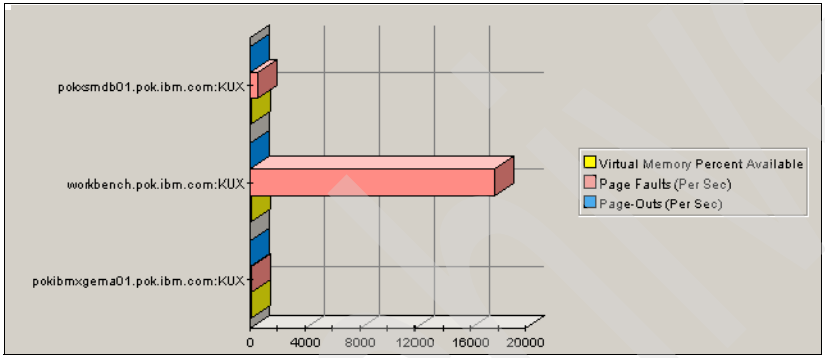


Figure 7-13 Final graph

7.2.3 Graphic views

To add a graphic view to the workspace, perform the following steps:

1. Open the workspace where you want the view.
2. If you want the view to occupy a new pane, click **Split Vertically** or **Split Horizontally** in one of the views.
3. Click **Graphic View**.
4. Click inside the view where you want the graphic. The cursor changes to a hand as you move inside the workspace. After you click, the old view is replaced by the default graphic, and the child Navigator items of the current item appear as icons on the graphic.
5. If you want to change the background image or the style of the icons or their labels, edit the graphic view Properties.

6. Click **Select** and then drag icons into position. Use this tool and other graphic view tools to manipulate the view.
7. If you want to add other Navigator items to the view, drag them from the Navigator view. You can drag items one at a time or use Ctrl+click to select multiple items and drag them as a group. Be careful to drag and not click, which selects and opens the workspace for that Navigator item.
8. To keep the graphic view in this workspace for future work sessions, do one of the following actions:
   - Click **Save** to update the workspace properties with the new view.
   - Select **Save Workspace As** from the File menu to save this view as a new workspace and leave the original workspace as it was.

Customize graphics in the graphic view

If you are using any custom graphics or a background in Tivoli Enterprise Portal, you must open them in a graphic editor that supports bean-managed persistence (BMP) files and save them in PNG, GIF, or JPG format. We explain how to customize the graphic view, because the product documentation does not provide updated details about this procedure. Perform the following steps:

1. Create the image that you want to use as a background in a graphical editor and save it as a PNG, JPG, or GIF file using a one-word name (underscores are acceptable).
2. Copy the image to:

   /opt/IBM/ITM/<*product code*>/cw/classes/candle/fw/resources/backgrounds/user

   Example 7-1 shows the pokmap.jpg file copied into this directory.

Example 7-1 pokmap.jpg copied

```
/opt/IBM/ITM/li6243/cw/classes/candle/fw/resources/backgrounds/user/pok
map.jpg
```

3. After adding the graphic view to a workspace, right-click anywhere inside the view and click **Properties**, as shown in Figure 7-14 on page 254.

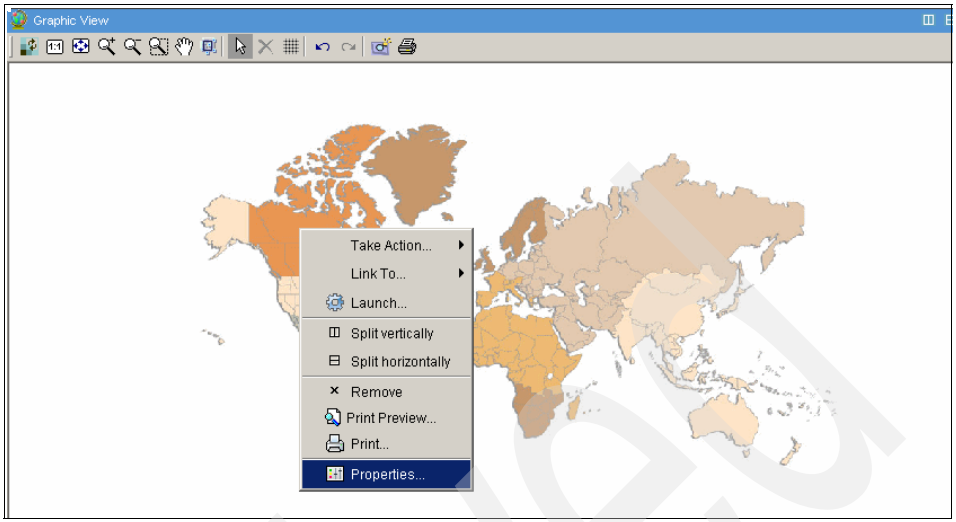


Figure 7-14 Right-click to display Properties

4. Click the middle (plot area) of the thumbnail graphic (Figure 7-15).

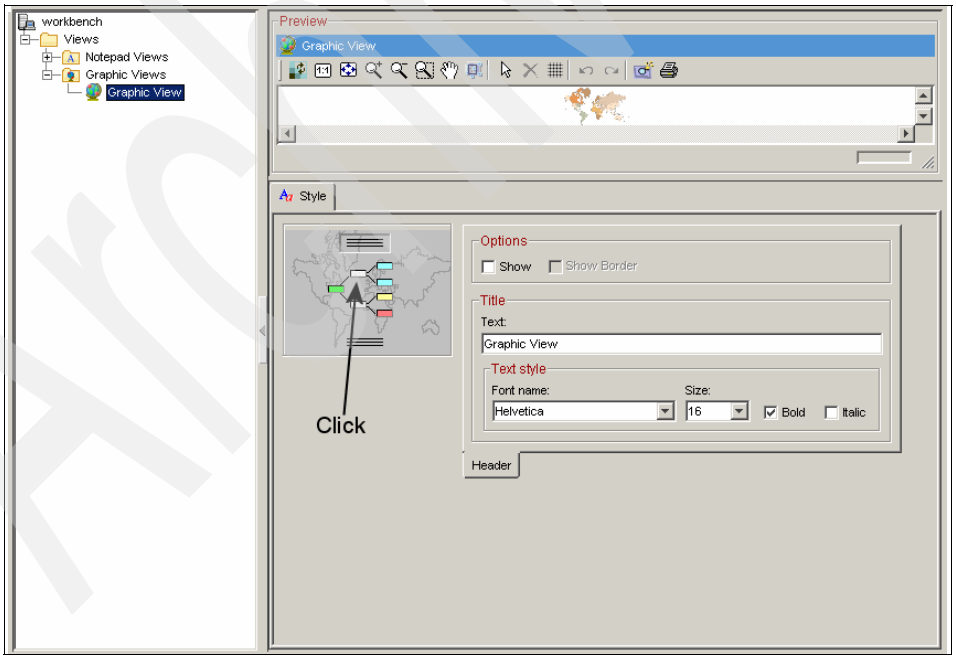


Figure 7-15 Click in the middle of the thumbnail graphic

5. In the Background area, click **Image**.

6. If you want the image to shrink or expand to fit the full view space, select **Fit to view**. If you leave this option cleared, the image retains its original size. If it is larger than the view space, scroll bars are displayed; if it is smaller than the view space, it will be placed at the top left corner with white space filled in the rest of the view space.
7. Click **Browse**, and select the image that you added in step 1 from the list of images that opens (Figure 7-16).

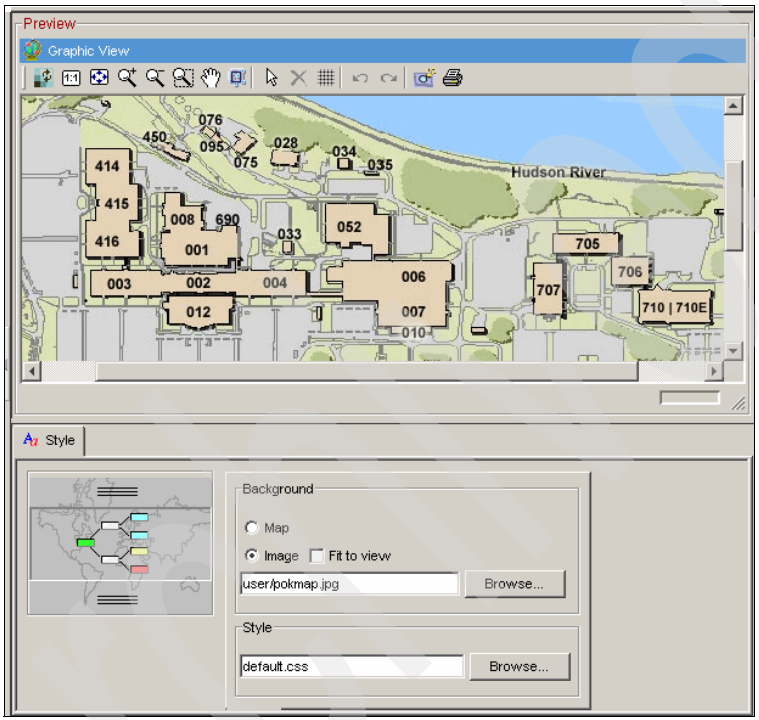


Figure 7-16 Click Browse and find your saved graphic

8. Click **Apply** if the graphic view is showing behind the window and you want to see how your image will look in the view space (Figure 7-17 on page 256).

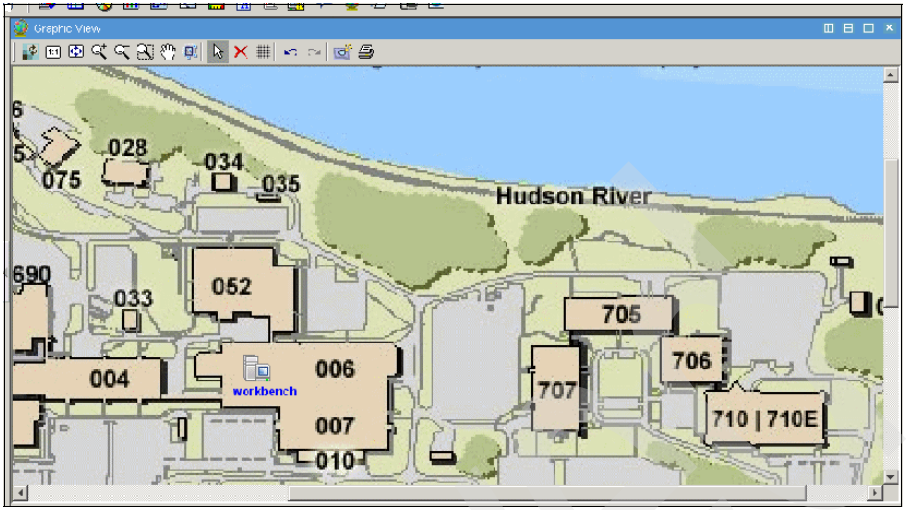


Figure 7-17 Final view (zoomed in)

7.3 Manage Tivoli Enterprise Monitoring Services

The Manage Tivoli Enterprise Monitoring Services is an often overlooked component of the IBM Tivoli Monitoring V6.2 product suite despite its incredible importance. Manage Tivoli Enterprise Monitoring Services runs on any machine with IBM Tivoli Monitoring V6.2 installed on it, including agents. The functionality includes:

- Configure Tivoli Enterprise Monitoring Server
- Configure OS agents, Universal Agents, and Application agents
- Configure the Warehouse Summarization and Pruning Agent
- Stop and start agents, Tivoli Enterprise Monitoring Server, and Tivoli Enterprise Portal Server
- Manage log files (Linux only)

Depending on what components are installed on the machine, you have different services and applications to configure. The Linux and Windows Manage Tivoli Enterprise Monitoring Services have differences between the two operating systems, which will affect your workflow in certain cases.

The major functions found in the Windows Manage Tivoli Enterprise Monitoring Services include (see Figure 7-18):

- Add TEMS application support
- Edit EIF Configuration
- Edit TEC Mapping File
- Edit Variables
- Edit ENV File
- Edit Trace Parms
- View Trace Log
- Start, Stop, and Recycle
- Change Startup
- Configure and Reconfigure

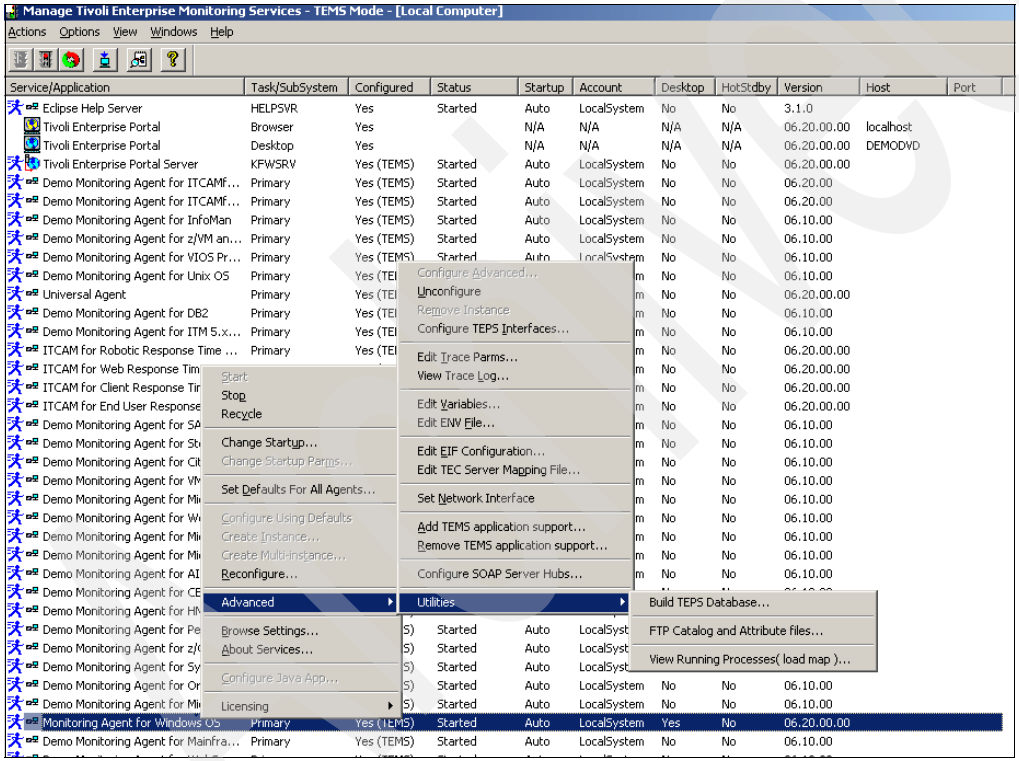


Figure 7-18 Windows Manage Tivoli Enterprise Monitoring Services

The major functions found in the Linux Manage Tivoli Enterprise Monitoring Services include (see Figure 7-19 on page 258):

- Add TEMS application support
- Set Agent Permissions
- Manage Log Files

- Install Product Support (TEMS)
- Start, Stop, and Recycle
- Configure

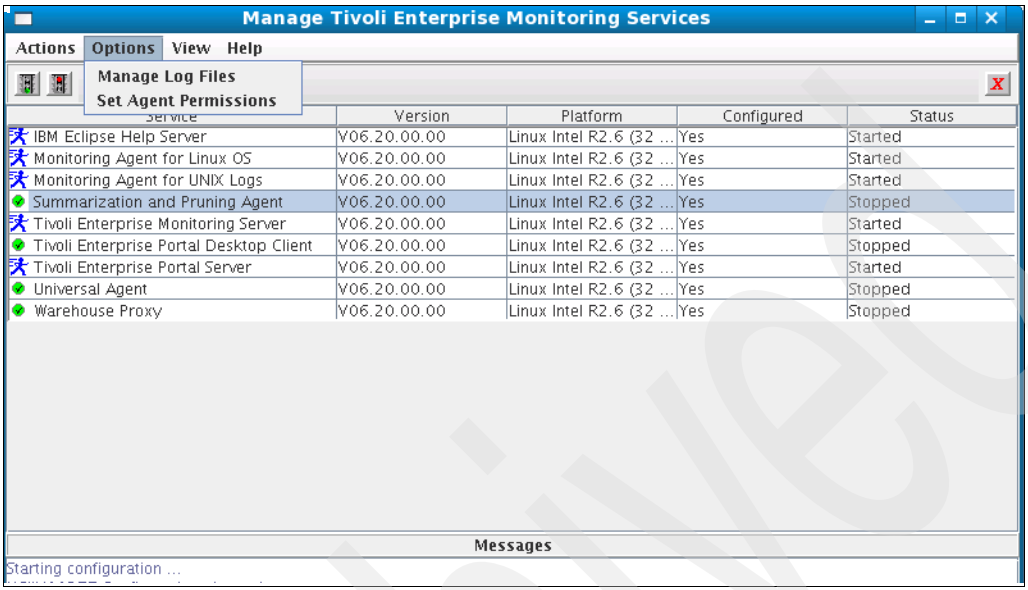


Figure 7-19 Linux Manage Tivoli Enterprise Monitoring Services

7.4 Historical data collection

IBM Tivoli Monitoring provides an optional component known as the *Tivoli Data Warehouse*. Tivoli Data Warehouse includes extremely powerful tools for collecting data, displaying short-term history reports, and also uploading data to a relational database for long-term storage, summarization, and report generation.

Note: In order to create a situation, you need Configure authority. Configure authority allows the user to open the History Collection Configuration window, configure history files and data roll off, and start and stop data collection, summarization, and pruning for various attribute groups.

The components of the Tivoli Data Warehouse are:

- Historical data collection
- Warehouse proxy
- Warehouse schema
- Warehouse summarization and pruning agent

Historical data collection

Configuration programs allow you to specify the collection of historical data. The historical data is stored in short-term history files either at the Tivoli Enterprise Monitoring Server or at the monitoring agent. You can choose to specify that historical data is sent to the Tivoli Data Warehouse database for long-term storage. The data model is the same data model across the long-term and short-term historical data.

Warehouse Proxy agent

The Warehouse Proxy agent is the bridge between the active monitoring system and the historical data repository. It handles warehousing requests from all managed systems in the enterprise. It uses ODBC to write the historical data to a supported relational database. Only one warehouse proxy agent can be configured and running in an IBM Tivoli Monitoring instance (hub Tivoli Enterprise Monitoring Server) at one time. The Warehouse Proxy can only successfully connect to a hub monitoring server.

Warehouse schema

The Tivoli Data Warehouse has one or more tables for each product, with column names that relate to the data contents. This platform follows a simple data model that is based on the concept of attributes. An *attribute* is a characteristic of a managed object (node).

Summarization and Pruning Agent

The Summarization and Pruning Agent maintains the data within the data warehouse by aggregation and pruning data based on client specifications.The IBM Tivoli Monitoring administrator sets up how often to collect the detailed data, what intervals at which to aggregate and prune, and how often to run the aggregation and pruning engine. Typically, the summarization and pruning process is scheduled to run once a day.

7.4.1 Historical data types

As mentioned previously, there are two types of data stores for the IBM Tivoli Monitoring V6.2 historical data component:

- Short-term data
- Long-term data

Short-term data

Short-term data is typically referred to in IBM Tivoli Monitoring V6.2 as data that is stored in binary files less for than 24 hours. In the IBM Tivoli Monitoring V6.2 architecture, historical data collection can be configured to store the binary files locally on the Tivoli Enterprise Monitoring agent, or it can be configured to store

the binary files on the Tivoli Enterprise Monitoring Server, which can be configured by agent type.

In both cases (Tivoli Enterprise Monitoring agent and Tivoli Enterprise Monitoring Server), the binary data is considered short-term, because it is only designed for 24-hour access. When the Summarization and Pruning Agent is configured, it can be set up to prune this short-term data. After the short-term data is successfully loaded into the Tivoli Data Warehouse by the Warehouse Proxy agent, it is pruned on the Tivoli Enterprise Monitoring agent or Tivoli Enterprise Monitoring Server if it is more than 24 hours old. If the Warehouse Proxy agent is not configured to collect the short-term data, a user-defined pruning job will have to be implemented.

Long-term data

Long-term data in IBM Tivoli Monitoring V6.2 is typically referred to as data that is more than 24 hours old and has been collected into the Tivoli Data Warehouse relational database management system (RDBMS) by the Warehouse Proxy agent. The long-term data resides in tables in the Tivoli Data Warehouse database. The long-term RDBMS tables contain detailed data and summarized data in Tivoli Data Warehouse. The Summarization and Pruning Agent can be configured to run every day to roll up data from the detailed level to hourly, weekly, monthly, quarterly, and yearly intervals. The Summarization and Pruning Agent also prunes the summarized tables.

7.4.2 Data collection options

To provide flexibility in using historical data collection, Tivoli Enterprise Portal permits you to:

- Turn history collection on or turn off all history collection for multiple selected Tivoli Enterprise Monitoring Servers and multiple selected attribute groups for a product.
- Save the history file at the Tivoli Enterprise Monitoring Server or at the remote agent.
- Define the collection interval to use to save data into the Tivoli Data Warehouse. The collection interval can be every hour, once a day, or off.
- Define how you want to summarize your historical data.
- Define how and when you want to prune your historical and detailed data.

Historical data collection can be specified for individual monitoring servers, products, and tables. However, all agents of the same type that report directly to the same Tivoli Enterprise Monitoring Server must have the same history collection options. In addition, for a given history table, the same history

collection options are applied to all monitoring servers for which that history table's collection is currently enabled.

History collection at the agent

We normally recommend collecting history data at the agents, which provides the following benefits:

- Reduces agent to Tivoli Enterprise Monitoring Server network traffic, because history data is not sent to Tivoli Enterprise Monitoring Server.
- Decreases Tivoli Enterprise Monitoring Server workload, especially when doing warehousing.
- Reduces history data file size, because data for only that agent or node exists in the file, which is critical when warehousing is enabled.

For scalability reasons, collect and store your historical data at the Tivoli Enterprise Monitoring agent rather than the Tivoli Enterprise Monitoring Server. However, there are certain product and attribute group combinations that are only collected at a specific place, either the monitoring server or the monitoring agent. The configuration files that are installed by the agent control where the collection of these product and attribute group combinations occurs.

History collection at Tivoli Enterprise Monitoring Server

History collection at the Tivoli Enterprise Monitoring Server provides the following benefits:

- Central control of history data files.
- Single point of file management when roll-off scripts or programs are used instead of warehousing.
- Necessary when sites require unobtrusive or restricted resource usage on the agent machines.
- Sites using history warehousing with agents outside of firewalls do not require that an additional network port is opened to firewall traffic for the Warehouse Proxy agent.

7.4.3 Starting the Summarization and Pruning Agent

Perform the following steps:

1. Right-click **Summarization and Pruning Agent** in your Manage Tivoli Enterprise Monitoring Services.
2. Select **Configure Advanced**, which opens the window in Figure 7-20 on page 262.

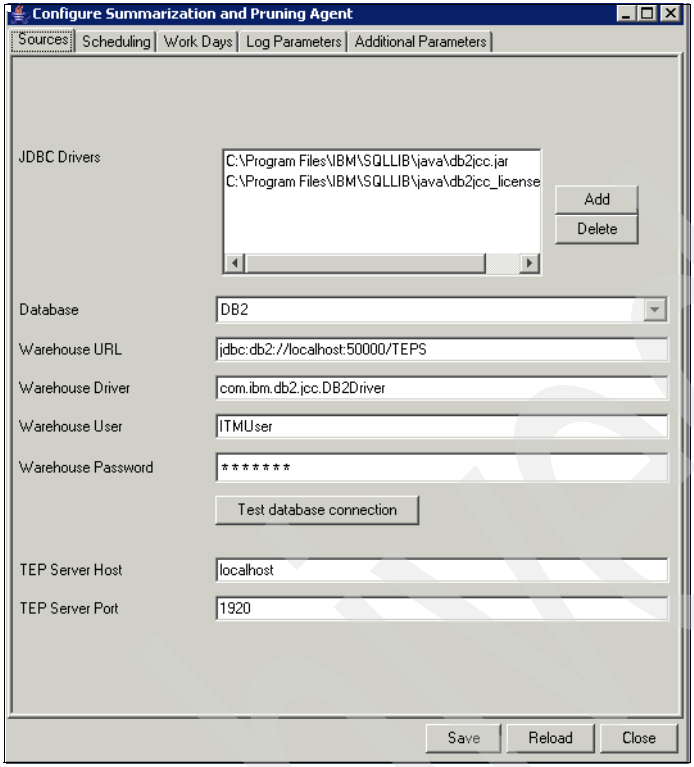


Figure 7-20 Configure Summarization and Pruning Agent

3. The following fields typically have valid default values listed:
   - JDBC Drivers
   - Database
   - Warehouse URL (be sure that this matches your database name)
   - Warehouse Driver
   - Warehouse User (be sure that this matches the user that was specified during installation)
   - Warehouse Password
   - TEP Server Host
   - TEP Server Port

Note: Note that the Default tab is no longer available in Summarization and Pruning Agent settings in IBM Tivoli Monitoring V6.2. This tab has been removed on purpose for performance reasons, because settings for each attribute group need to be set individually depending on the reporting requirements. You must not use a default value.

4. The Summarization and Pruning Agent is executed on a schedule. Use the Scheduling tab to set the schedule (Figure 7-21).

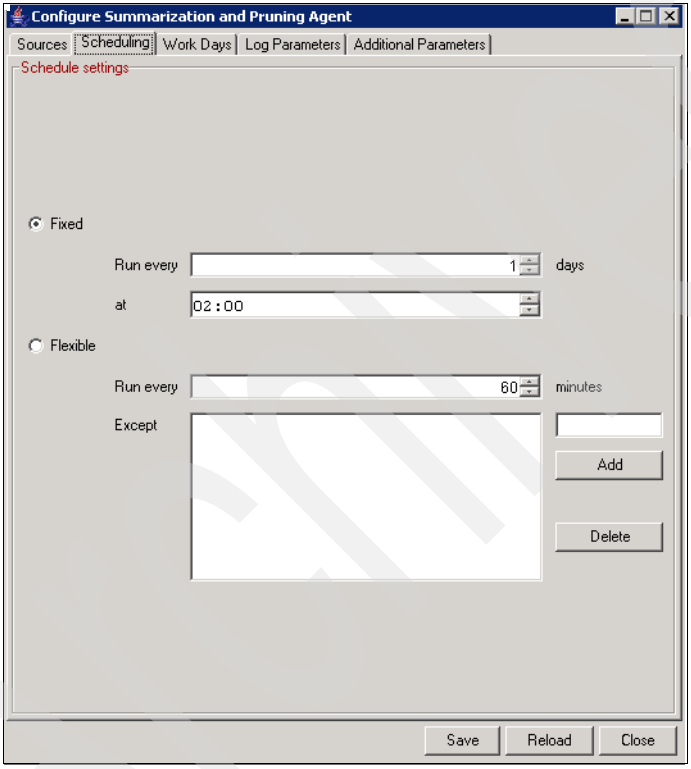


Figure 7-21 Scheduling

5. On the Work Days tab, you can specify the work days to run the Summarization and Pruning Agent (Figure 7-22).

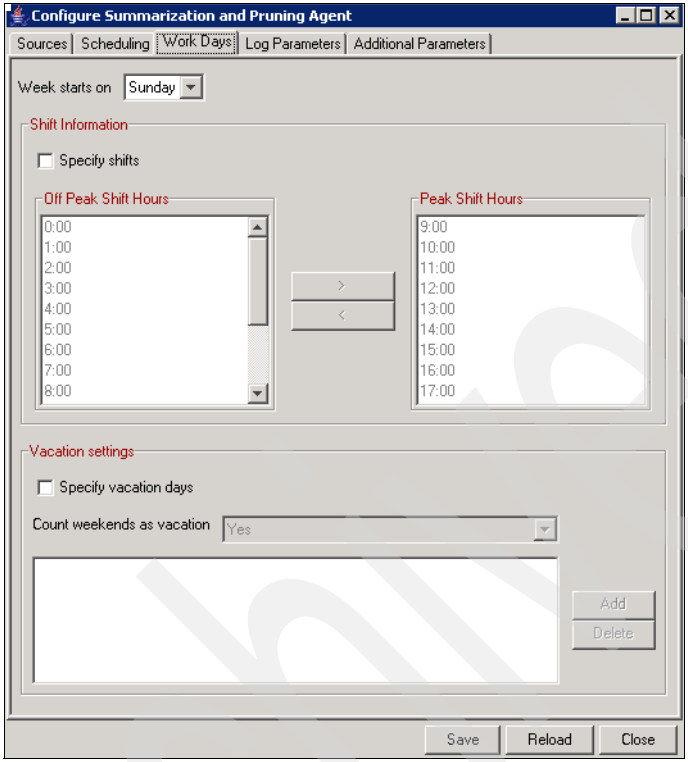


Figure 7-22 Work Days

6. The Log Parameters tab (Figure 7-23 on page 265) is new with IBM Tivoli Monitoring V6.2. The two options here are:
   - Keep WAREHOUSEAGGREGLOG data for:

     Select the unit of time (day, month, or year) and the number of units for which data must be kept.
   - Keep WAREHOUSELOG data for:

     Select the unit of time (day, month, or year) and the number of units for which data must be kept.

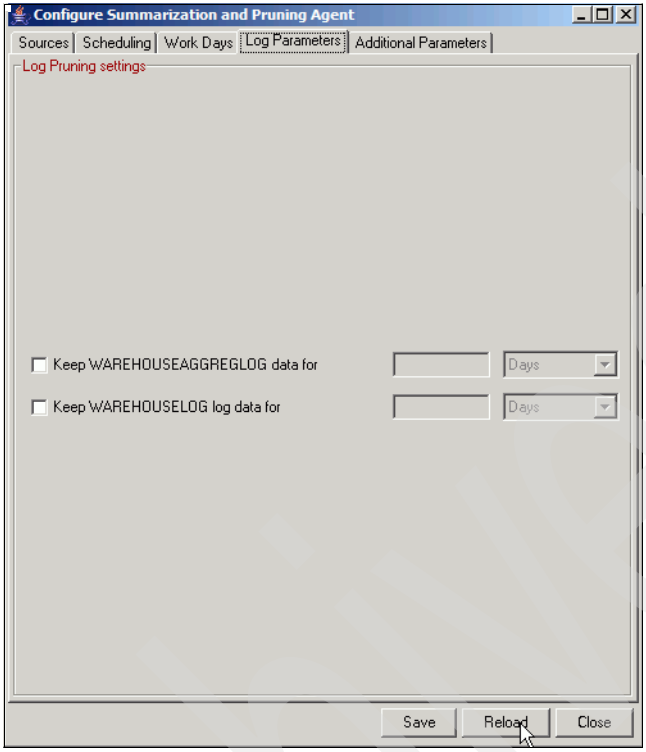


Figure 7-23 Log Parameters tab

7. The Additional Parameters tab (Figure 7-24 on page 266) provides the following options:
   - Number of worker threads to use
   - Maximum rows per database transaction
   - Use timezone to offset from (minus Greenwich Mean Time)
   - Summarize hourly data older than *x* hours
   - Summarize daily data older than *x* days

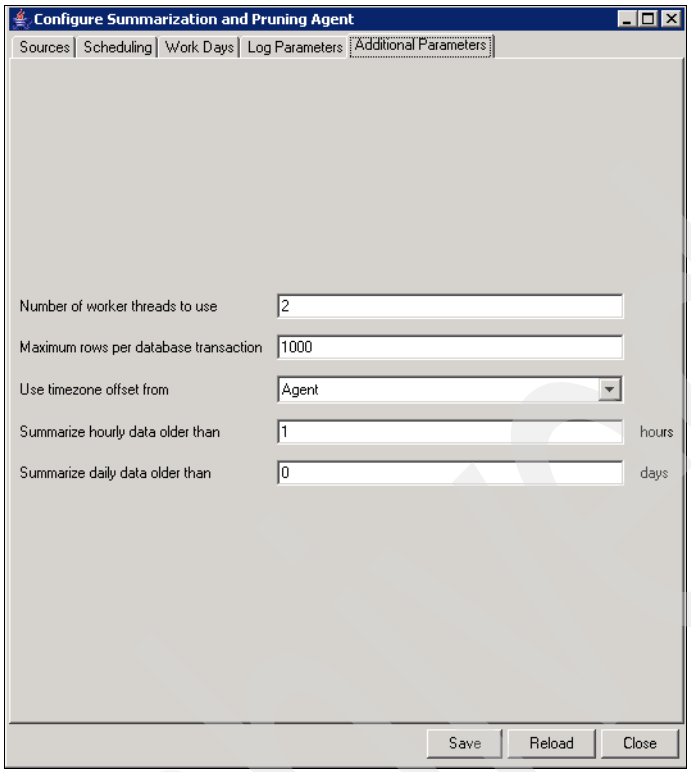


Figure 7-24 Additional Parameters

7.5 Integration with other Tivoli event systems

In this section, we will delve into the details of IBM Tivoli Enterprise Console and IBM Tivoli Netcool/OMNIbus integration.

7.5.1 IBM Tivoli Enterprise Console event viewer

You can configure IBM Tivoli Monitoring V6.2 to send events to IBM Tivoli Enterprise Console. You can also add Tivoli Enterprise Console views to your workspace.

Note: The event processing of IBM Tivoli Monitoring V6.2 is not intended to replace or be a substitute for IBM Tivoli Enterprise Console. IBM has the full intention of having these products be complementary and has plans to further integrate the tools in the future.

Adding Tivoli Enterprise Console views to your workspace

The toolbar in the Tivoli Enterprise Portal has a Tivoli Enterprise Console icon.

When this icon is selected and added to your workspace, you will be prompted to enter the IBM Tivoli Enterprise Console server credentials, as shown in Figure 7-25.

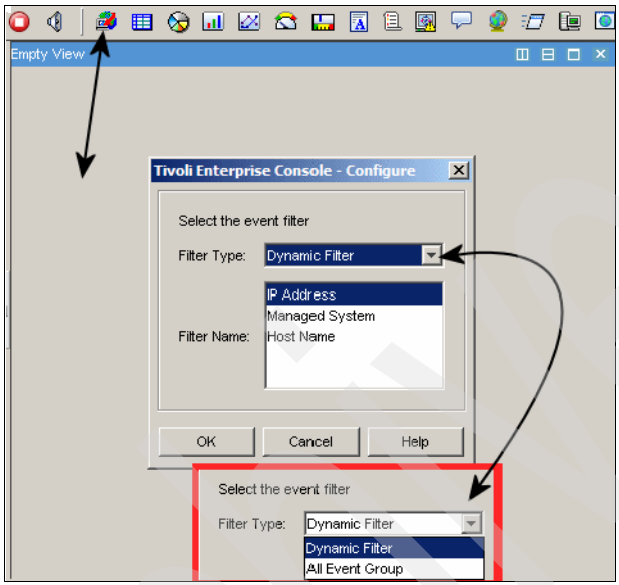


Figure 7-25 Adding Tivoli Enterprise Console views to your workspace

A single workspace can have multiple Tivoli Enterprise Console event viewer windows set up with different event filters. The dynamic filter is context-sensitive based on the navigation tree. The highlighted entry in the navigation view (Figure 7-26 on page 268) determines which events will be displayed, for example:

- To view all events, create the event view on the enterprise level.
- To view all UNIX events, create the event view on the agent type level UNIX.
- To view only events from a single system, create the event view on the agent level.

The Filter Type drop-down list shows all event groups that have been defined in your IBM Tivoli Enterprise Console server configuration. If you require new groups, define them using the IBM Tivoli Enterprise Console Java Console.

Events can be viewed, acknowledged, and closed in the same way as though you were using the Tivoli Enterprise Console Java Console.

Note: Avoid closing sampled events through event synchronization in the Tivoli Enterprise Console Event Server. Sampled events expect a natural closing event. Closing a sampled event manually on Tivoli Enterprise Console causes a callback to the Tivoli Monitoring Console message console in the portal and prematurely closes the alert there as well.

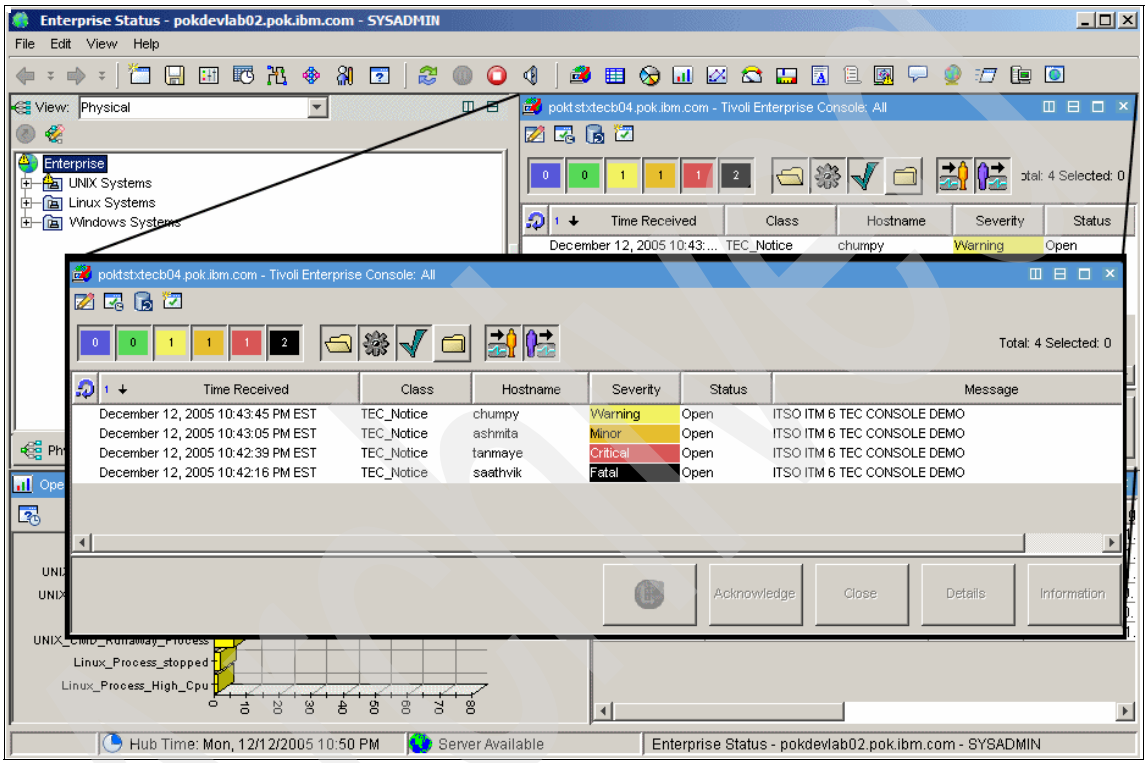


Figure 7-26 Tivoli Enterprise Console view

7.5.2 IBM Tivoli Enterprise Console event integration

If your monitoring environment includes the Tivoli Enterprise Console Event Server and situation event forwarding has been configured on the hub Tivoli Enterprise Monitoring Server, you can forward situation events to that server. The *IBM Tivoli Monitoring Installation and Setup Guide, Version 6.2.0*, GC32-9407, provides the instructions to enable situation event forwarding: configuring the event server to receive the events, installing the event synchronization component on the event server, enabling situation forwarding on

the hub monitoring server, and defining a default event integration facility (EIF) destination.

7.5.3 IBM Tivoli Netcool/OMNIbus event integration

If your monitoring environment includes the Tivoli Netcool/OMNIbus ObjectServer and situation event forwarding has been configured on the hub Tivoli Enterprise Portal Server, you can forward situation events to the ObjectServer. The *IBM Tivoli Monitoring Installation and Setup Guide, Version 6.2.0*, GC32-9407, provides the instructions to enable situation event forwarding: configuring the ObjectServer to receive the events, installing the event synchronization component on the ObjectServer, enabling situation forwarding on the hub monitoring server, and defining a default event integration facility (EIF) destination.

7.5.4 Common Event Console view

The Common Event Console view provides a single, integrated display of events from multiple event repositories, including Tivoli Monitoring, Tivoli Enterprise Console, and Tivoli Netcool/OMNIbus. This view presents normalized events from these sources in one table; you can sort and filter the listed events and perform actions on selected events.

Note: The events included in the Common Event Console view depend upon which common event connectors are configured. Each connector retrieves event data from a specific event repository (for example, a specific Tivoli Enterprise Console event server). The Common Event Connector Status window shows the current status of all configured connectors.

The *common event connector* (frequently called a *connector*) is software that enables the integrated display of events from multiple event systems in the common event console. A connector retrieves event data from an event system and sends user-initiated actions to be run in that event system. For example, if you perform an action on a Tivoli Enterprise Console or Netcool/OMNIbus event in the common event console, the associated common event console connector sends that action to the originating event system (Tivoli Enterprise Console or Netcool/OMNIbus) for execution. To have the events from a specific event system displayed in the common event console, you must configure a connector for that event system.

To configure connectors, open the Common Event Console Configuration window:

- **ITM Connector**: Click the ITM Connector tab to view or change the information for the IBM Tivoli Monitoring V6.2 connector. Because you have only the hub Tivoli Enterprise Monitoring Server in the Tivoli Monitoring event system, you configure only one IBM Tivoli Monitoring V6.2 connector.
- **TEC Connector**: Click the TEC Connector tab to view or change the information for an IBM Tivoli Enterprise Console connector. To have the events from a Tivoli Enterprise Console server displayed in the common event console, you must configure an IBM Tivoli Enterprise Console connector. To configure a connector, click New.
- **OMNIbus Connector**: Click the OMNIbus Connector tab to view or change the information for an IBM Tivoli Netcool/OMNIbus connector. To have the events from a Tivoli Netcool/OMNIbus ObjectServer displayed in the common event console, you must configure an IBM Tivoli Netcool/OMNIbus connector. To configure a connector, click New.

7.6 IBM Tivoli Monitoring V6.2 command line

The command line in IBM Tivoli Monitoring V6.2 is a simplified wrapper for many of the Candle prefixed commands that exist in the same directory. The two major commands are:

- **`tacmd`**: Tivoli agent command
- **`itmcmd`**: IBM Tivoli Monitoring command

This section also describes:

- **`cinfo`**: UNIX-only command
- **`kincinfo`**: Windows-only command
- **`setparm`**: UNIX-only command
- Multiplatform backup and restore commands

For more information about these commands, see *IBM Tivoli Monitoring User's Guide, Version 6.2.0*, SC32-9409, and *IBM Tivoli Monitoring Administrator's Guide, Version 6.2.0*, SC32-9408. This section focuses on providing the essentials for these commands.

7.6.1 The tacmd command

Administrative **`tacmd`** commands are available on both Windows and UNIX computers. The basic usage of this command is:

```
tacmd command [option [operand ...]] ...
```

You must log in for the majority of the functions that this command provides. When logged in, you have full access to the commands until you log off the OS or until a timeout occurs. The timeout is 15 minutes by default. However, it can be set to a maximum of 1440 minutes (24 hours) with the **-t|-timeout** flag.

Note: On Windows, several **tacmd** commands exist. Be sure to use the command under *$install_dir*/CLI, where the *$install_dir* is the directory in which IBM Tivoli Monitoring V6.2 is installed.

Using the other **tacmd** commands results in an entry point failure for kui62.dll.

Basic commands

The following list describes the basic **tacmd** commands:

- **help**

  Prints the full help text for the specified command or summary help text for all commands if no command is specified.

- **login**

  Authenticates a user with a server and creates a security token that is used by subsequent **tacmd** commands.

- **logout**

  Invalidates the security token created by the **tacmd login** command.

- **refreshTECinfo**

  Triggers the Event Forwarder to reprocess any updated event destinations, EIF configurations, and custom event mapping files without recycling the hub Tivoli Enterprise Monitoring Server.

Installation commands

The following list describes the installation **tacmd** commands:

- **createNode**

  Creates a node by installing an OS agent into a new directory on the local machine and starting that OS agent.

- **viewNode**

  Displays the details of a node, including what components are installed on it.

Depot commands

The following list describes the depot **tacmd** commands:

- **viewDepot**

  Displays the types of agents that can be installed from the (currently logged in) server's agent depot or from the named remote server's depot.

- **listBundles**

  Displays the details of one or more deployment bundles that are available for installation from the specified directory into the local deployment depot.

- **addBundles**

  Installs one or more deployment bundles from the specified directory into the local deployment depot. This command must be executed locally on a Tivoli Enterprise Monitoring Server containing a depot.

- **removeBundles**

  Removes one or more deployment bundles from the local deployment depot. This command must be executed locally on a Tivoli Enterprise Monitoring Server containing a depot.

Agent commands

The following list describes the agent **tacmd** commands:

- **startAgent**:
  - Starts the given agents or the agents for the given managed systems if they are not already running.
  - OS agents (nodes) can be started on the local system only.
  - The agent is marked online in the Tivoli Enterprise Portal client.
- **stopAgent**:
  - Stops the given agents or the agents for the given managed systems if they are running.
  - OS agents (nodes) can be stopped on the local system only.
  - The agent is marked offline in the Tivoli Enterprise Portal client within the next heartbeat interval.
- **restartAgent**:
  - Starts or restarts the given agents or the agents for the given managed systems.
  - OS agents (nodes) can be restarted on the local system only.
  - If the agent is already started, it is stopped before being restarted.

- **viewAgent**:
  - Displays the details of the given agent or the agent for a given managed system.
  - Details include the agent version, agent status (running or not), and all of the configuration data for the agent.
- **updateAgent**

  Enables users to install an agent update to a specified node.

System commands

The following list describes the system **tacmd** commands:

- **describeSystemType**

  Displays the configuration options that are required for a given managed system type.
- **addSystem**:
  - Enables a user to add managed systems to the monitoring system.
  - Deploys an agent and other needed components if they are not already installed on the node.
- **configureSystem**:
  - Enables the user to change the configuration options of an existing managed system.
  - The user also has the option to restart the managed system's monitoring agent in order for the new configuration parameters to take effect.
- **listSystems**:
  - Displays a list of known managed systems.
  - The results can optionally be filtered to display only those results on a given node, only those results for given product types, or both.

Server command

The following list describes the server **tacmd** command:

- **configurePortalServer**:
  - Adds, configures, or removes a portal server datasource from the portal server configuration.
  - This command must be executed locally to the portal server.
  - Uses NAME=VALUE options.

Situation commands

The following list describes the situation **tacmd** commands:

- **createSit**

  Creates a new situation, based on an existing situation.

- **editSit**:

  - Edits an on-server or exported situation definition.
  - If a **–force** parameter is specified, it disables the message that asks if you are sure that you want to edit the situation.

- **deleteSit**:

  - Deletes a situation from the server.
  - If a **–force** parameter is specified, it disables the message that asks if you are sure that you want to delete the situation.

- **listSit**

  Lists the defined situations, optionally filtering for a given managed system or for a given managed system type.

- **viewSit**

  Allows the configuration of a situation to be displayed or saved in an export file.

Event destination definition commands

The following list describes the event destination definition **tacmd** commands:

- **createEventDest**

  Creates a new event destination definition on the server.

- **deleteEventDest**

  Deletes an event destination server definition from the server.

- **editEventDest**

  Modifies an existing event destination server definition on the server.

- **listEventDest**

  Displays the server ID, name, and type for every event destination definition on the server.

- **viewEventDest**

  Displays all properties for the specified event destination definition on the server.

Import/export commands

The following list describes the import/export **tacmd** commands:

- **bulkExportPcy**

  Exports all the available policies from the Tivoli Enterprise Monitoring Server.

- **bulkExportSit**

  Exports all the available situations from the Tivoli Enterprise Monitoring Server.

- **bulkImportPcy**

  Imports all the available policy objects to the Tivoli Enterprise Monitoring Server from BULK_OBJECT_PATH.

- **bulkImportSit**

  Imports all the available objects to the Tivoli Enterprise Monitoring Server from BULK_OBJECT_PATH.

Managed system list commands

The following list describes the managed system list **tacmd** commands:

- **createsystemlist**

  Creates a new managed system list.

- **deletesystemlist**

  Deletes a managed system list.

- **editsystemlist**

  Adds or deletes managed systems to or from an existing managed system list on the server.

- **listsystemlist**

  Lists the available managed system lists.

- **viewsystemlist**

  Lists the configuration of a managed system list to be displayed or saved in an export file.

Workspace commands

The following list describes the workspace **tacmd** commands:

- **exportworkspaces**

  Exports one or more portal server workspaces to a file.

- **importworkspaces**

  Imports the workspaces contained in a file into the portal server.

- **listworkspaces**

  Lists all of the portal workspaces on the server.

7.6.2 The itmcmd command

This command is only available on UNIX or Linux. The **itmcmd** command has the following format:

```
itmcmd command [option [operand ...]] ...
```

The following list describes the **itmcmd** commands:

- **itmcmd agent**:
  - Starts and stops most agents.
  - You can start or stop one agent, all agents, or multiple agents.
  - You can also start the portal server and portal desktop client using this command.
  - You must run the **itmcmd agent** command on the architecture for which the agent is installed.
- **itmcmd audit**

  Manages log files from the command line. The default logs are in /opt/IBM/ITM/logs.

- **itmcmd config**:
  - Configures or reconfigures the following items for IBM Tivoli Monitoring on UNIX:
    - The IP port that the hub monitoring server uses to listen for requests
    - The hosts that can run a product
    - The location of the hub monitoring server in the network
    - The monitoring server to which an agent connects
    - Whether a monitoring server is a hub or remote server
  - You can only configure one product at a time. If you reconfigure a monitoring server, you must stop and restart that monitoring server before the changes take effect.
- **itmcmd dbagent**

  Starts the IBM Tivoli Monitoring for Sybase and IBM Tivoli Monitoring for Oracle monitoring agents.

- **itmcmd dbconfig**

  Configures the execution environment for a distributed database agent.

- **itmcmd execute**:
  - Runs a script or command when its execution requires the same environment settings as a particular IBM Tivoli product. The **itmcmd execute** command runs this script or command by building the necessary environment settings for the intended script or command and then combining them into a temporary shell script before running it.
  - You must run the **itmcmd execute** command on the platform architecture for which the agent is installed. To use this command, make sure that you are in the correct directory: cd *$install_dir*/bin, where *$install_dir* is the location where you installed your IBM Tivoli software.

- **itmcmd history**

  Manages the roll-off of history data into delimited text files.

- **itmcmd manage**

  Starts Manage Tivoli Enterprise Monitoring Services on a UNIX or Linux computer. You can start, stop, and configure monitoring components in Manage Tivoli Enterprise Monitoring Services.

- **itmcmd server**

  Starts and stops monitoring servers that are defined in directories under the install_dir/tables subdirectory. You must run the **itmcmd server** command from the host computer.

- **itmcmd support**:
  - Adds agent-specific information to the monitoring server. You need to run this command one time during the initial installation of the monitoring server to add data for the components installed from the same installation CD.
  - Whenever you add a new monitoring agent type to your monitoring environment, run the **itmcmd support** command again on the monitoring server to add the new agent information to the monitoring server.

7.6.3 The cinfo command (UNIX-only)

Use the **cinfo** command to view the following information for your monitoring server:

- An inventory of installed IBM Tivoli products
- The configuration settings for products
- The installed CD versions in the current $candlehome directory

- The configuration settings for products in the context of the actual variables that are used by the installation program
- A list of running IBM Tivoli processes (such as agents or monitoring server)
- A validated list of running IBM Tivoli processes, after first performing an update on the tracking database to remove stale PIDs (processes logged as **ps** but not found when attempting to verify using the **ps** command)

This command can be menu-driven (run with no flags) or controlled by passing flags, as shown in Example 7-2.

Example 7-2 The cinfo command

```
cinfo [-h candle_directory] [-c product] [-i] [-r] [-s product] [-R]
[-v]
        -c <product> Displays configuration prompts and values
        -i Displays an inventory of installed products
        -r Shows running processes
        -s <product> Displays configuration parameters and settings
        -R Shows running processes, after updating a tracking database
        -v Shows the installed CD versions in this CandleHome
        -p <product> Shows associated platform codes for the specified
           product
        -d Dumps an inventory of installed products
```

For example, if you run **cinfo -p lz**, you get the output that is shown in Example 7-3.

Example 7-3 cinfo -p lz output

```
********** Wed Dec 14 01:06:57 EST 2005 *****************
User     : root        Group: root
Host name : pokdevlab05  Installer Lvl: 400 / 100
CandleHome: /opt/IBM/ITM
***********************************************************
Platform codes:
ls3263 : Current machine
ls3263 : Product (lz)
tmaitm6/ls3263 : CT Framework (ax)
```

Note: The usage statement shows two usable, but undocumented, commands:

```
-p <product> Shows associated platform codes for the specified
product

-d Dumps an inventory of installed products
```

7.6.4 The kincinfo command (Windows-only)

Use the **kincinfo** command to validate your installation. The command-line interface syntax is:

```
kincinfo
        [-d]
        [-i]
        [-r]
        [-l]
```

where:

-d Displays a list of installed products, which can be parsed.

-i Lists the inventory in English.

-r Displays a list of running agents.

-l Displays the log switch.

The following command shows all installed products:

```
kincinfo -i
```

7.6.5 The setperm command (UNIX-only)

Use the **setperm** command to set file permissions to ensure that the permissions were set properly during the installation procedure. To run this command, you must be logged in to the UNIX computer as root.

When you run the **setperm** command, a product selection list is displayed. This list is sorted and contains the run architectures within each product description. From the list of installed products, enter a valid number or numbers separated by commas or spaces. The CLI syntax is:

```
setperm -s
        [-h install_dir]
```

where:

-s Used to set security validation on selected monitoring servers.

-h *install_dir*

(Optional) Identifies the installation directory if it is not the directory in which the script is located.

Also, use this option to take action on an IBM Tivoli Monitoring installation directory other than the directory in the current system.

The following example starts the **setperm** utility:

```
setperm -s
```

7.6.6 Backup and restore commands

You can use the following backup and restore commands with IBM Tivoli Monitoring.

Replicating the Tivoli Enterprise Portal Server database

With the exception of situations, policies, and managed system lists, Tivoli Enterprise Portal customizations are stored at the Tivoli Enterprise Portal Server in the Tivoli Enterprise Portal Server database. The portal customizations include user IDs, Navigator views, custom workspaces, and custom queries.

This section describes how to replicate the Tivoli Enterprise Portal Server database, which is necessary for moving from a test environment to a production environment. You can also use this procedure for backing up and restoring the database before applying a fix pack or upgrading to a new version.

Running the migrate-export script

On the computer where the source Tivoli Enterprise Portal Server is installed, take these steps to create a copy of the Tivoli Enterprise Portal Server database for applying to a portal server on another computer.

Windows

The steps are:

1. Open a command prompt window: **Start** → **Run**, enter **CMD**.
2. Change to the cnps directory of the IBM Tivoli Monitoring installation:

   `cd c:\ibm\itm\cnps (default directory)`
3. Enter **`migrate-export`**.

This script generates a file named saveexport.sql in the c:\ibm\itm\cnps\sqllib subdirectory. It contains all of the Tivoli Enterprise Portal Server data.

UNIX

The steps are:

1. Stop the Tivoli Enterprise Portal Server on the source system.
2. Open a terminal window.
3. In the terminal window, change the directory to the bin subdirectory of your IBM Tivoli Monitoring installation: **`cd /opt/IBM/ITM/bin`** (default directory).
4. In the terminal window, enter **`./itmcmd execute cq "runscript.sh migrate-export.sh"`** and press Enter.

Be sure to use the (") double quotation mark and not the (') single quotation mark. This command generates a file named saveexport.sql in the /opt/IBM/ITM/$platform/cq/sqllib subdirectory that contains all of the Tivoli Enterprise Portal Server data.

Running the migrate-import script

On the computer where the target Tivoli Enterprise Portal Server is installed, take these steps to import the Tivoli Enterprise Portal Server database that you copied with the migrate-export script. This procedure overwrites the Tivoli Enterprise Portal Server database on the target computer.

Windows source portal server to Windows target portal server

The steps are:

1. Stop the Tivoli Enterprise Portal Server on the destination system.
2. At the command prompt, **Start** → **Run**, enter **CMD**.

3. Copy the file saveexport.sql, which was generated by the migrate-export.bat script, from the source system to c:\ibm\itm\cnps\sqllib on the destination system:

   ```
   copy <mapped drive on destination system>:\ibm\itm\cnps\sqllib
   \saveexport.sql c:\ibm\itm\cnps\sqllib
   ```

   where ***<mapped drive on destination system>*** is the drive on the source system where this file resides. If a drive is not already defined, you need to map a drive to the source system from the destination system with the **net use** command.

4. Type **cd \ibm\itm\cnps.**
5. Enter **migrate-import**.

   Depending on the contents of the saveexport.sql file , this process can completely replace the existing Tivoli Enterprise Portal Server database.

6. Restart the Tivoli Enterprise Portal Server.

Windows source portal server to UNIX target portal server

The steps are:

1. Stop the Tivoli Enterprise Portal Server on the destination system.
2. At the command prompt, **Start** → **Run,** enter **CMD**.
3. In the command prompt window, copy the file saveexport.sql, which was generated by the **migrate-export.bat** script, from the source system to the destination system's /opt/IBM/ITM/*$platform*/cq/sqllib directory, where $platform is li6243 for Intel Linux or ls3263 for System z Linux on the destination system.
4. Open a terminal window on the destination system.
5. Change to the bin subdirectory of the IBM Tivoli Monitoring installation: **cd /opt/IBM/ITM/$platform/bin**.
6. In the terminal window, enter: **./itmcmd execute cq "runscript.sh migrate-import.sh"**

   Be sure to use the (") double quotation mark and not the (') single quotation mark. The script processes a file named saveexport.sql in the IBM/ITM/$platform/cq/sqllib subdirectory. Depending on the contents of the saveexport.sql file, this process can completely replace the existing Tivoli Enterprise Portal Server data.

7. Restart the Tivoli Enterprise Portal Server.

UNIX source portal server to Windows target portal server

The steps are:

1. Stop the Tivoli Enterprise Portal Server on the destination system.
2. Open a terminal window.
3. Copy the file saveexport.sql, which was generated by the migrate-export.sh script, from the source system to the destination system in the c:\ibm\itm\cnps\sqllib directory.
4. At the command prompt on the destination system, **Start** → **Run,** enter **CMD**.
5. Type **`cd \ibm\itm\cnps`**.
6. In the command window, enter **`migrate-import`** and press Enter. Depending on the contents of the saveexport.sql file, this process can completely replace the existing Tivoli Enterprise Portal Server data. Running the migrate-export process stops the Tivoli Enterprise Portal Server if it is currently started.
7. Restart the Tivoli Enterprise Portal Server.

UNIX source portal server to UNIX target portal server

The steps are:

1. Stop the Tivoli Enterprise Portal Server on the destination system.
2. Open a terminal window.
3. Copy the file saveexport.sql, which was generated by the migrate-export.sh script, from the source system to /opt/IBM/ITM/*$platform*/cq/sqllib where *$platform* is the operating system identifier, such as li6243 for Intel Linux.
4. Change the directory to the bin subdirectory of the IBM Tivoli Monitoring installation: **`cd /opt/IBM/ITM/bin`**.
5. In the terminal window, enter **`./itmcmd execute cq "runscript.sh migrate-import.sh"`**.

   Press Enter. This script processes a file named saveexport.sql in the IBM/ITM/$platform/cq/sqllib subdirectory. Depending on the contents of the saveexport.sql file, this process can completely replace the existing Tivoli Enterprise Portal Server data.
6. Restart the Tivoli Enterprise Portal Server.

Tivoli Enterprise Monitoring Server backup and restore

There are two types of monitoring servers: the hub monitoring server and the remote monitoring server. The hub monitoring server is the focal point for the entire Tivoli Monitoring environment.

The hub monitoring server is under a significant load. Work on the hub includes connections from the remote monitoring server, authentication, situations, policies, and workflows. The hub monitoring server stores, initiates, and tracks all situations and policies and is the central repository for storing all active conditions and short-term data on every Tivoli Enterprise Monitoring agent (monitoring agent). The hub monitoring server is also responsible for initiating and tracking all generated Take Action commands.

The monitoring server storage repository is a proprietary database format, referred to as the *Enterprise Information Base (EIB)*, that is grouped as a collection of files located on the monitoring server. These files start with a file name prefix `qa1` and are located in the following directories:

- On UNIX and Linux: <*installation_dir*>/tables/<*tems_name*>
- On Windows: <*installation_dir*>\cms

In these directories, <*installation_dir*> specifies the Tivoli Monitoring installation directory and <*tems_name*> specifies the Tivoli Enterprise Monitoring Server name.

These files can be backed up and restored using traditional file copy commands available on the same platform on which the Tivoli Enterprise Monitoring Server is installed.

Note: Unlike the Tivoli Enterprise Monitoring Server, the Tivoli Enterprise Portal Server and Tivoli Data Warehouse use relational databases to store critical files. Currently, the Tivoli Enterprise Portal Server supports the use of DB2 and MS SQL databases. The Tivoli Data Warehouse supports DB2, MS SQL, and Oracle databases.

A

Sample Certification Test questions

In this appendix, we provide several sample questions for the Certification Test. These are representative of the questions that you will see in the Certification Test. We recommend that you take this sample test after studying the previous chapters in this book.

Questions

We provide the following questions to assist you in studying for the Certification Test:

1. Which two operating systems are supported as the monitoring server?
   a. AIX 5L V5.1 (32/64 bit)
   b. Microsoft Windows 2000 Professional
   c. AIX 5L V5.3 (32/64 bit)
   d. Red Hat Enterprise Linux 2.1 Intel
   e. Red Hat Enterprise and Desktop Linux 4 Intel
2. Which database is not supported in the IBM Tivoli Monitoring implementation of Tivoli Enterprise Monitoring Server and Tivoli Enterprise Portal?
   a. DB2
   b. Oracle
   c. Microsoft SQL
   d. Sybase
3. What are the minimum requirements to install the hub monitoring server (for RISC architectures)?
   a. Processor 1 GHz, memory 256 MB, and hard disk 300 MB
   b. Processor 1 GHz, memory 512 MB, and hard disk 650 MB
   c. Processor 750 MHz, memory 256 MB, and hard disk 100 MB
   d. Processor 2 GHz, memory 1 GB, and hard disk 400 MB
4. How many agents can be supported (maximum) for a single remote monitoring server?
   a. 500
   b. 1500
   c. 1000
   d. 2000
5. Which protocol is not supported when we run OMEGAMON V350 and V360 agents with IBM Tivoli Monitoring V6.2?
   a. IP.UDP
   b. IP.SPIPE
   c. IP.PIPE
   d. SNA

6. When migrating an existing Warehouse Proxy database, which files are *not* part of warehouse migration tool files installed with the Warehouse Summarization and Pruning Agent? (choose two)
   a. khdmig.jar
   b. KHDENV_MIG
   c. classes12.zip
   d. db2java.zip
   e. migratewarehouse.bat
7. When installing a hub monitoring server, what is the default IBM Tivoli Monitoring home directory?
   a. /usr/IBM/ITM
   b. /opt/IBM/ITM61
   c. /opt/IBM/ITM
   d. /usrt/IBM/ITM61
8. How can you configure an AIX 5L hub monitoring server?
   a. Running the tacmd configureSystem -t <*tems_name*> command from /opt/IBM/ITM
   b. Running the ./itmcmd config -S -t <*tems_name*> command from /opt/IBM/ITM/
   c. Running the tacmd configureSystem -t <*tems_name*> command from /opt/IBM/ITM/bin
   d. Running the ./itmcmd config -S -t <*tems_name*> command from /opt/IBM/ITM/bin
9. Which of the following monitoring agents are part of the IBM Tivoli Monitoring installation base package? (choose three)
   a. Linux OS
   b. DB2
   c. UNIX OS
   d. Exchange
   e. Windows OS
   f. Sybase

10. You need create a user on the Tivoli Enterprise Portal, select the required steps to create it:
    a. Enable security on the hub monitoring server.
    b. Right-click **Tivoli Enterprise Portal Server** in Manage Tivoli Enterprise Monitoring Services, select **Advanced** → **Edit Env File**, and add the user in the KFWENV file.
    c. Use the itmcmd AddUser command.
    d. Create a user on Tivoli Enterprise Portal.
    e. Enable security on Tivoli Enterprise Portal.
    f. Define a matching user ID with password to the network domain user accounts.
11. Which is the default heartbeat interval used by monitoring agents to communicate their status to the monitoring server?
    a. 5 minutes
    b. 3 minutes
    c. 10 minutes
    d. 20 minutes
12. Which of the following statements is false?
    a. You can start IBM Tivoli Monitoring components from Manage Tivoli Enterprise Monitoring Services.
    b. You can start the UNIX monitoring server using the **`itmcmd`** command.
    c. You can start both Windows and UNIX monitoring agents using the **`tacmd`** command.
    d. You can start the UNIX monitoring server using the **`tacmd`** command.
13. Where can you find the IBM Tivoli Enterprise Console Situation Update Forwarder logs in UNIX-based systems?
    a. /tmp/TEC/logs
    b. /tmp/itmsynch/logs
    c. /opt/IBM/ITM/logs
    d. /tmp/TEC/logs

14. How can you roll back an endpoint upgrade from Tivoli Distributed Monitoring?
    a. Using the **witmupgrade** command
    b. Using the **tacmd removeBundles** command
    c. Using the **witm61agt** command
    d. Using Manage Tivoli Enterprise Monitoring Services
15. You installed Monitoring Agent for IBM Tivoli Monitoring V5.X Endpoint component and distributed it onto the Austin Endpoint. After the distribution, it seems that you have problems related to gathering the data. Which of the following files do you need to check?
    a. $LCF_DATDIR/LCFNEW/AMW/logs (UNIX)
    b. $LCF_DATDIR/LCFNEW/AMG/logs
    c. $LCF_DATDIR/LCFNEW/KTM/logs
    d. $LCF_DATDIR/LCFNEW/Tmw2k/Tmw2k.log
16. How should you configure the security for a local intranet zone in order to access Tivoli Enterprise Portal Server?
    a. High
    b. Medium
    c. Medium-low
    d. Low
17. What is the initial user ID for Tivoli Enterprise Portal Server?
    a. Administrator
    b. SYSADMIN
    c. TEPS
    d. ITMUser
18. Which of the following actions should *not* be done to perform a silent installation of IBM Tivoli Monitoring?
    a. Edit the silent.txt file from the product installation CD in a temporary directory on your system.
    b. Edit the setup.iss file from the product installation CD in a temporary directory on your system.
    c. Install using Software Management Services (SMS).
    d. Run the silent installation from the command line with parameters.

19. In a Tivoli Enterprise Console integration, which command can you use to check the Tivoli Enterprise Console event cache?
    a. The **sitconfig.sh** command
    b. The **wsetesvrcfg** command
    c. The **wlookup** command
    d. The **wlsesvrcfg** command
20. How can you turn off summarization and pruning for a particular product or set of attribute groups?
    a. Using the history collection configuration to stop the collection
    b. Stopping the Summarization and Pruning Agent
    c. Removing the product table from the database
    d. Using the **itmcmd history -h** command
21. Which of the following information is not relevant to gather prior to a hub monitoring server installation on Windows?
    a. Host name of computer
    b. Encryption key
    c. Simple Mail Transfer Protocol (SMTP) server name
    d. Monitoring server name
22. You are willing to upgrade your environment to IBM Tivoli Monitoring V6.2. Which of the following monitoring applications can be upgraded to that version?
    a. IBM Tivoli Distributed Monitoring V3.6
    b. IBM Tivoli Monitoring V5.1.1
    c. IBM Tivoli Monitoring V5.1.2
    d. IBM Tivoli Distributed Monitoring V3.7
23. Which of the following components or variables are required to enable Warehouse Proxy agent to export data to a local warehouse database? (choose two)
    a. Database client
    b. Open Database Connectivity (ODBC) connection
    c. KHD_TARGET_JDBC_DRIVER variable
    d. MSDE connection

24. Which of the following components is not a Tivoli Management Framework component?
    a. Endpoints
    b. Monitoring agent
    c. Profiles
    d. Profile managers
25. What kind of host systems can you connect using the terminal view? (choose two)
    a. Xterminal
    b. TN3270
    c. SSH
    d. VT100
    e. FTP
26. Which view does *not* have a tool for setting a time span that causes previous data samples to be reported within the time range?
    a. Table view
    b. Bar chart
    c. Pie chart
    d. Situation view
27. How can you improve DB2 performance after many INSERT, DELETE, and UPDATE changes to table data?
    a. Running the DB2 RUNSTATS command
    b. Moving database log files to the same database disk
    c. Running the DB2 REORG command
    d. Decreasing the SORTHEAP value
28. Which of the following commands can be used to perform a Tivoli management region scan using the scan tool in order to produce an XML baseline file?
    a. **`witmscantmr`** command
    b. **`cinfo`** command
    c. **`witmassess`** command
    d. **`itmcmd config`** command

29. What platforms are supported for the Tivoli Enterprise Portal client? (choose three)
    a. Windows 2003 Standard
    b. Windows NT
    c. Red Hat Enterprise Linux (RHEL) 2.1
    d. Windows XP Professional
    e. Red Hat Enterprise Linux (RHEL) 4
    f. Red Hat 7.0
30. When using the Windows Manage Tivoli Enterprise Monitoring Services to configure the Summarization and Pruning (S&P) agent, why should the "Schedule" settings be set to at least 10 minutes in the future?
    a. Enough time must be given for the S&P's UADVISOR situation to hit its five minute interval to pick up its new schedule.
    b. The clock for the scheduler only allows ten minute increments in the hour regardless of the time selected, such as 3:05 = 3:10, 3:12 = 3:20.
    c. The Summarization and Pruning agent takes ten minutes to complete its work.
    d. The scheduler only allows entering time in ten minute increments, such as 03:00, 03:10, or 03:20.
31. What is the purpose of the command "**tacmd addSystem**"?
    a. Install an operation system Tivoli Enterprise Monitoring agent
    b. Install Tivoli Monitoring Server
    c. Install Tivoli Enterprise Portal client
    d. Install a non-operational system Tivoli Enterprise Monitoring agent
32. What is the default DB2 database name used by Warehouse Proxy agent?
    a. ITM Warehouse
    b. Warehouse
    c. Warehous
    d. ITM Warehous

33. Summarization and pruning settings can be configured for which aggregation levels? (choose three)
    a. Seconds
    b. Minutes
    c. Hours
    d. weekends
    e. Quarters
    f. Years
34. What is the command to uninstall IBM Tivoli Enterprise Console event synchronization on UNIX?
    a. <*tec_installdir*>/TME/TEC/OM_TEC/_uninst/uninstaller.bin
    b. <*tec_installdir*>/ITM/TEC/OM_TEC/_uninst/uninstaller.bin
    c. tec_installdir>/TME/TEC/uninst/uninstaller.bin
    d. tec_installdir>/ITM/TEC/uninst/uninstaller
35. What is the command to configure options within the Tivoli Enterprise Monitoring Server (TEMS)?
    a. tacmd configureSystem -t <*tems_name*>
    b. itmcmd config -S -t <*tems_name*>
    c. tacmd config -S -t <*tems_name*>
    d. itmcmd configureSystem -S -t <*tems_name*>
36. What prerequisites are required before installing Monitoring Agent for IBM Tivoli Monitoring V5.X Endpoint? (choose two)
    a. IBM Tivoli Monitoring V5.1.2 Fix Pack (FP) 6
    b. Tivoli Enterprise Console V3.9 FP3
    c. Distribution Monitoring 3.7
    d. IBM Tivoli Monitoring Component Services Version 5.1.1 Fix Pack 2 or Version 5.1.3
    e. Distribution Status Console V4.1.1

37. Which command will direct the data logging to IBM Tivoli Monitoring V6.2 and IBM Tivoli Monitoring 5.x from the Monitoring Agent for IBM Tivoli Monitoring V5.X Endpoint given the endpoint labeled chicago?

    a. **wdmepconfig –h chicago –D DataSeeding**

    b. wdmepconfig –h chicago –D DataSeeding=BOTH

    c. wdmepconfig –e chicago –D DataSeeding=BOTH

    d. wdmepconfig –e chicago -D BOTH

38. What is the command to add application support for the Tivoli Enterprise Monitoring Server (TEMS)?

    a. ./tacmd support -t tems_name *pc pc pc*

    b. ./itmcmd support -t tems_name *pc pc pc*

    c. ./itmcmd addsupport -t tems_name *pc pc pc*

    d. ./tacmd support tems_name *pc pc pc pc* Red Hat 7.0

39. What is the command to uninstall IBM Tivoli Monitoring 6.2 components on UNIX?

    a. remove.sh

    b. install.sh -r

    c. uninstall.sh

    d. itmcmd uninstall

Answers

1. c, e
2. d
3. b
4. b
5. b
6. c, d
7. c
8. d
9. a, c, e
10. a, d, f
11. c
12. d
13. b
14. a
15. c
16. c
17. b
18. b
19. d
20. a
21. c
22. d
23. a, b
24. b
25. b, d
26. d
27. c
28. a
29. a, d, e
30. a

31.d

32.c

33.c, e, f

34.a

35.b

36.a, d

37.c

38.b

39.c

Related publications

The publications listed in this section are considered particularly suitable for a more detailed discussion of the topics covered in this book.

IBM Redbooks publications

For information about ordering these publications, see “How to get IBM Redbooks publications” on page 298. Note that several of the documents referenced here might be available in softcopy only:

- *Getting Started with IBM Tivoli Monitoring Version 6.1 on Distributed Environments*, SG24-7143
- *Deployment Guide Series: IBM Tivoli Monitoring 6.2*, SG24-7444
- *IBM Tivoli Monitoring: Implementation and Performance Optimization for Large Scale Environments*, SG24-7443

Other publications

These publications are also relevant as further information sources:

- *Introducing IBM Tivoli Monitoring, Version 6.2.0,* GI11-4071
- *IBM Tivoli Monitoring User’s Guide, Version 6.2.0*, SC32-9409
- *IBM Tivoli Monitoring Administrator’s Guide, Version 6.2.0*, SC32-9408
- *Upgrading from IBM Tivoli Monitoring V5.1.2, Version 6.2.0,* GC32-1976
- *IBM Tivoli Monitoring Installation and Setup Guide, Version 6.2.0*, GC32-9407
- *IBM Tivoli Monitoring Problem Determination Guide, Version 6.2.0*, GC32-9458
- *IBM Tivoli Monitoring Upgrading from Tivoli Distributed Monitoring, Version 6.2.0*, GC32-9462
- *Monitoring Agent for IBM Tivoli Monitoring 5.x Endpoint User’s Guide*, SC32-9490
- *Configuring IBM Tivoli Enterprise Monitoring Server on z/OS*, SC32-9463
- *Tivoli Management Framework Reference Manual, Version 4.1.1*, SC32-0806

Online resources

These Web sites and URLs are also relevant as further information sources:

- The IBM Professional Certification Program Web site

  http://www.ibm.com/certify/index.shtml

- Test 870: IBM Tivoli Configuration Manager V4.2.2 Implementation test information

  http://www.ibm.com/certify/tests/obj870.shtml

- Link to the IBM Tivoli Monitoring V6.1 Implementation Certification Test

  http://www.ibm.com/certify/certs/tvdpitm6.shtml

- IBM IT Training

  http://ibm.com/training

- IBM Tivoli Monitoring Version 6.1.0 information center

  http://publib.boulder.ibm.com/infocenter/tivihelp/v3r1/index.jsp?toc=/com.ibm.itm.doc/toc.xml

How to get IBM Redbooks publications

You can search for, view, or download IBM Redbooks publications, Redpapers, Hints and Tips, draft publications and Additional materials, as well as order hardcopy IBM Redbooks publications or CD-ROMs, at this Web site:

ibm.com/redbooks

Help from IBM

IBM Support and downloads

ibm.com/support

IBM Global Services

ibm.com/services

Index

Symbols
.baroc files 128

A
Additional Parameters tab of Summarization and Pruning Agent configuration window 95
administrator privileges 59
Agent Builder 17
API-Socket-File-Script (ASFS) 175
Application Agent 14
application support 64, 101, 128, 160–161, 163–164
Assess tool 142, 145
attribute group 216
ATTRLIB directory 105

B
backup monitoring server 160–161
  host name 162
  identical protocols 162
baroc file 128
base event 122
baseline file 143–144
binary file 121

C
C++ 219
Candle Management Server (CMS) 100, 103
Candle Management Workstation (CMW) 102, 104
Candle Monitoring agent (CMA) 104
CandleNet Portal
  database 102
  Server 100, 103
CaptionFigColumn
  Figure 4-9 Additional Parameters tab of Summarization and Pruning Agent co 95
CaptionTabColumn
  Table 4-10 New in IBM Tivoli Monitoring V6.2 130
Certification
  benefits 3
  checklist 5
  IBM Professional Certification Program 2
  IBM Tivoli Monitoring V6.1 7
  process 7
  Tivoli Certification 4
cinfo 182, 270, 277, 279
command line 118–119, 204
config 204
configuration file 199
courses 9
createEventDest 274
creating situations
  best practices 215
  building in the right order 218
  critical performance factors 215
  evaluation of the situation 218
  realistic alert values 216
  several levels of severity 216
  situations grouping 216

D
data collection 14, 17, 217
data source 218
DataSeeding 117, 120
DB2 database 102, 135
default baseline file 144, 147

E
Eclipse based 17
encryption key 62, 64–65
endpoint 145
Enterprise Information Base (EIB) 13
environment variable 202–203
event groups 267
event server 125, 127, 129, 136
  baroc files 128
  event synchronization 136
event synchronization 122, 125–126, 268
Expert Advice 241
exportworkspaces 275

F
failover 160

failover capability 18
Firewall 41

G

gateway 118
graphical user interface (GUI) 121

H

HeapDumps 208
heartbeat 214
heartbeat interval 214
historical data types 259
  long-term data 260
  short-term data 259
host name 238, 278
Hot Standby
  configuring 161
  feature 161
  verifying the failover 163
  what is it? 161
HTTP data provider 203
hub monitoring server 41, 59, 62, 64, 157, 160, 259, 276
  backup protocols 162
  host name 165
  installation 62
    ./install.sh 64
    communications protocol 63
    Linux or UNIX 64
    maxfiles 61
    setup.exe 62
    Windows 62
  IP address 162–163
  naming 59
  ports 165
  same protocol 162
  uninstallation 131
hub Tivoli Enterprise Monitoring Server 218, 259

I

IBM Certification Agreement 6
IBM Tivoli
  RAS1 service log 206
IBM Tivoli account 60
IBM Tivoli Enterprise Console 64, 257, 266–267
IBM Tivoli Monitoring
  agent 135
  Certification 7
  CLI 117
  command 270
  component 59, 64, 103, 116, 143, 154, 156
  courses 9
  deployment 40, 143
  directory 103, 132
  engine 115, 119–120, 189
  environment 102, 116, 131, 145
  infrastructure 142–143
  infrastructure component 7
  installation directory 60, 65, 69, 132, 184–185
  installation medium 125
  installation program 103
  instance 259
  log facilities 199
  message console 268
  performance tuning 193
  previous versions 234
  product 245
  profile 120, 188
  profile collection option 117
  publication 9
  recommended resources for study 8
  Redbooks 9
  situation 146
  software 45
  tracing 199
  uninstallation 131
  upgrade tool 145, 148
  V6.2 Certification 7
  V6.2 implementation 58
  V6.2 Implementation Certification 8
  V6.2 solution 7
  V6.2 Tools 109
  Version 5.1 7, 115
  Version 5.X 187
  wdmepconfig command 188
IBM Tivoli Monitoring Agent 115
IBM Tivoli Monitoring deployment 143
IBM Tivoli Monitoring V5.1 115
IBM Tivoli Monitoring V5.x upgrade 105
IBM Tivoli Monitoring V5.x upgrade toolkit 106
  installation procedure 106
    from the Tivoli command line 106
    from the Tivoli desktop 108
  installation requirements 106
  phases and steps 112
  product prerequisites 106

supported platforms 106
IBM Tivoli Monitoring V6.2
components 12
installation
software prerequisites
supported databases 52
monitoring agent 13
monitoring server 12
portal 13
portal server 13
IBM Tivoli Universal Agent 174
benefits 174
data source 175
generic agent 174
metafiles 175
generating a metafile 176
importing a new metafile 176
refreshing a metafile 176
validating a metafile 176
TTL value 175
IBM_Tivoli_Monitoring_Certificate 159
idx799 153
importworkspaces 276
install_dir 132, 155, 164, 183, 200–201, 204
installation directory 60, 62, 64, 184
integration agent 115
Intel architecture 43
intelligent remote agent (IRA) 174
Internet Explorer browser 13
IP address 41, 162–163
IP.UDP 63
iSeries 47
Itanium 47
ITM61AGT product 118
itmcmd 276
itmcmd config 64–65, 67, 156, 183

J

Java desktop client 13
Java Web Start capability 13
JAVACore 208
JavaScript 219
JMX (Java Management Extensions) 17
JSCRIPT 219

K

k.baroc 122
kbb.env 63
kui61.dll 271

L

log file 203
maximum number 203
total number 203
long-term data 260

M

Manage Tivoli Enterprise Monitoring Services 257–258
console 81
managed node 118–119
managed system 119, 135, 187, 203, 216, 235–236, 240
data collection 119, 187
warehousing requests 259
managed system lists 216
MDist 2 log 207
metadata 121
metafile 174–175
Microsoft SQL 165
Migration Toolkit 112
monitoring agent 14, 17, 63, 66–67, 146, 187, 200, 204, 234, 241
base software 187
components 187
multiple versions 241
monitoring server 12, 45, 58, 61, 149, 155, 234, 240, 242
application support 64
basic configuration 155
communications protocol 155
communications protocol fields 155
initial installation 277
portal server connection 69
MtkJavaDir 108
multiple Warehouse Proxy agents 14

N

Navigator item 234, 236–237
Navigator view
default view 210
Netcool/OMNIbus 19
Netcool/OMNIbus integration 122
network address translation (NAT) 41

O

ObjectServer 269
ODBC Data Provider 203
OMEGAMON Monitoring agent (OMA) 100, 104
OMEGAMON Tivoli Event Adapter (OTEA) 122
OMEGAMON XE 7, 100, 102
omegamon.baroc 122
omegamon.rls 122
OMNIbus events 19
Open Process Automation Library (OPAL) 15, 17
operating system 41, 45, 61, 64–65, 146–147
  monitoring collection 147
Operating System (OS) Agents 14
Oracle 165
order of installation 59
orphan Tivoli Enterprise Monitoring Agents 25
OS agent 271

P

path name 61
pc 64, 67, 134, 161, 164
port number 120
portal server 55, 58–60, 156, 163, 244, 247, 273
portal server on Linux 60
primary monitoring server 13
prioritize situations 215
profile 145
profile manager 142, 145–146
  subscriber list 146
pSeries 47
publications 9

Q

Query editor 247

R

reconfigure 81
Redbooks Web site 298
  Contact us xiii
refreshTECinfo 271
regexp 184
reliability, availability, and serviceability (RAS) 199, 203
Remote monitoring server 13
remote Tivoli Enterprise Monitoring Server 25
required order of installation 59
return on investment (ROI) 5
RISC architecture 43
rpm package 49
rule base 127–128
  baroc files 129
  existing rule base 127
rulebase 127

S

sample questions 285
sampling interval 214, 216
saveexport.sql 282
Scan tool 142
ScanValue 108
secondary Tivoli Enterprise Monitoring Server 163
Sentry.baroc 122
setperm command 279
short situation sampling interval 215
short-term data 259
silent installation 128
Simple Object Access Protocol (SOAP) 219
situation 235
  Action feature 241
  association 243
  building in the right order 218
  creating 235
  creating the formula 236
  Expert Advice 241
  grouping 216
  modify authority 235
  naming 235–236
  Sampling Interval 239
  selecting systems for distribution 240
  Until 243
  View authority 235
  where is it evaluated? 218
Situation editor 235
Situation Update Forwarder (SUF) 122
SNMP (Simple Network Management Protocol) 17
SOAP methods 219
  predefined 219
SOAP requests 219
Solaris 51
SQL statement 217
Summarization and Pruning Agent 101, 165, 168, 258, 261
Summarization and Pruning agent (S&P) 14
summarization and pruning process 169
system list 216

T

table name 217
tacmd addBundles 63, 177
tacmd command 270–271
  agent commands 272
  basic commands 271
  depot commands 272
  return codes 179
  server commands 273
  situation commands 274
  system commands 273
tacmd editSit 180
take action 200, 241
template account 208
template user IDs 209
TEMS support 72
Thomson Prometric 6
time frames 214
timeout 271
Tivoli Certification benefits 4
Tivoli Data Warehouse 14, 41, 58, 79, 104–105, 120, 173
  historical data 14
  historical raw data 14
  logging 117
Tivoli Data Warehouse integration 165
Tivoli Data Warehouse V1.2 117
Tivoli Data Warehouse V2.1 117
Tivoli Enterprise
  Monitoring Server 155, 175
  Monitoring Services utility 154–155
  Portal 217–218
  Portal client 102
  Portal Server 59
Tivoli Enterprise Monitoring Agent 58, 63, 104, 174
  installation
    on Linux or UNIX 67
    on Windows 67
Tivoli Enterprise Monitoring Agent (monitoring agent) 12–14
Tivoli Enterprise Monitoring Agent Framework 59, 103
Tivoli Enterprise Monitoring Server 58–59, 62, 149, 177, 199, 209, 216, 260–261
  installation 62
Tivoli Enterprise Monitoring Server (monitoring server) 12–13
Tivoli Enterprise Monitoring Service 81, 205
Tivoli Enterprise Monitoring Services utility 135
Tivoli Enterprise Portal 64–65, 79, 163, 174, 216
  client 102
  database 132
  desktop client 58
  installation
    On Linux or UNIX 69
    On Windows 68
Tivoli Enterprise Portal (portal) 13
Tivoli Enterprise Portal paging 230
Tivoli Enterprise Portal Server 58, 64, 156
  installation
    on Linux or UNIX 66
    on Windows 65
  process 67
Tivoli Enterprise Portal Server (portal server) 13
Tivoli environment 5, 108, 141–142
Tivoli Event Integration Facility (EIF) 19
Tivoli Management Framework
  environment 128
  V4.1.1 7
Tivoli management region (TMR) 200
Tivoli Monitoring Services 31
Tivoli Monitoring V5.x upgrade 105
Tivoli Netcool/OMNIbus ObjectServer 269
Tivoli server 118, 142–144
  prerequisite software 106
Tivoli software education 9
Tivoli Universal Agent 14
tmroid.xml 144
trace and log facilities 199
trace settings 202

U

Universal Agent 7, 67, 174–175, 239
Universal Agent (UA) 14–15
UNIX Agent 202
Unix Agent Zone Support 17
UNIX system 121, 210
Upgrade tool 143
Upgrade Toolkit 142
upgradetools.tar 142
upgradetools.zip 142
user ID 208
user name 209

V

VBSCRIPT 219
viewEventDest 274

views 245
chart views 245
creating views with the Query editor 247
data views 245
graphic views 252
table views 245

W

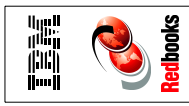
Warehouse Proxy 45, 58, 67, 79, 165–166, 200–201, 259, 261
Agent 14, 58, 79, 101, 260
Agent installation 81, 86
configuration 166
Warehouse Proxy agent 14
wchkdb –u 112
wdmepconfig 121
wdmepconfig command 119
Web Health Console 120
Web Services 219
Web-based courses 8
wenblprb command 150
wep 34
Windows domain account 209
winstall command 118
witm61agent command 121
witm61agt command 121, 187
witmassess 33
witmassess command 142, 145–146
witmjavapath 33
witmmtk scantmr 108
witmscantmr 33
witmscantmr command 142–144, 148
witmupgrade 33
witmupgrade command 143, 145–146, 148–149
wlookup 33
workspace 244
workspaces 230
wq381 223
wq382 224
wq383 224
wq384 225
wq385 226
wq386 226
wq387 227
wq388 227
wq389 227
wq390 227
wq391 228

X

XML file 117
Xms 208
Xmx 208

Z

zSeries 47



Certification Study Guide Series: IBM Tivoli Monitoring V6.2

(0.5” spine)
0.475”<->0.875”
250 <-> 459 pages

Certification Study Guide Series: IBM Tivoli Monitoring V6.2

Helps you achieve IBM Tivoli Monitoring Version 6.2 certification

Explains the certification path and prerequisites

Introduces useful tips and best practices

This IBM Redbooks® publication is a study guide for IBM Tivoli Monitoring Version 6.2 and is aimed at the people who want to get an IBM Professional Certification for this product.

The IBM Tivoli Monitoring Version 6.2 Certification, offered through the Professional Certification Program from IBM, is designed to validate the skills required of technical professionals who work in the implementation of the IBM Tivoli Monitoring Version 6.2 product.

This book provides a combination of theory and practical experience needed for a general understanding of the subject matter. It also provides sample questions that will help in the evaluation of personal progress and provide familiarity with the types of questions that will be encountered in the exam.

This publication does not replace practical experience, nor is it designed to be a stand-alone guide for any subject. Instead, it is an effective tool that, when combined with educational activities and experience, can be a very useful preparation guide for the exam.

For your convenience, we structure the chapters based on the sections of the IBM Tivoli Monitoring V6.2 Implementation Certification test, such as Planning, Prerequisites, Installation, and so on, so studying each chapter will help you prepare for one section of the exam.

INTERNATIONAL TECHNICAL SUPPORT ORGANIZATION

BUILDING TECHNICAL INFORMATION BASED ON PRACTICAL EXPERIENCE

IBM Redbooks are developed by the IBM International Technical Support Organization. Experts from IBM, Customers and Partners from around the world create timely technical information based on realistic scenarios. Specific recommendations are provided to help you implement IT solutions more effectively in your environment.

For more information:
ibm.com/redbooks

SG24-7456-00 ISBN 0738485209