Tivoli software

IBM

Deployment Guide Series: IBM Tivoli Monitoring 6.1

- Step-by-step deployment guide for IBM Tivoli Monitoring 6.1
- Covers small to large environments
- Discusses best practices for a deployment plan

Vasfi Gucer
Ana Godoy

Redbooks

ibm.com/redbooks

International Technical Support Organization

Deployment Guide Series: IBM Tivoli Monitoring 6.1

December 2005

SG24-7188-00

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

First Edition (December 2005)

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

Contents

Figures

Tables

Examples

Notices

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

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

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

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

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

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

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

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

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

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

Trademarks

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

AIX®
AS/400®
Candle®
DB2®
i5/OS®
IBM®
iSeries™
NetView®
OMEGAMON®
OS/390®
OS/400®
Redbooks™
Redbooks (logo) ™
Tivoli Enterprise™
Tivoli Enterprise Console®
Tivoli®
WebSphere®
z/OS®
zSeries®

The following terms are trademarks of other companies:

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

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

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

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

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

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

Preface

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

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

IBM Tivoli Monitoring 6.1 is easily customizable and provides real-time and historical data that enables you to quickly diagnose and solve issues with the new GUI via the IBM Tivoli Enterprise™ Portal component. This common, flexible, and easy-to-use browser interface helps users to quickly isolate and resolve potential performance problems.

The target audience for this book is IT Specialists who will be working on new IBM Tivoli Monitoring 6.1 installations.

The team that wrote this redbook

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

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

Ana Godoy has worked for IBM Brasil since 1996. She started working with hardware support for PC Company, worked two years as technical support, then become Leader of Product Support for products such as Aptiva, Desktos, ThinkPad, and ViaVoice. In January 2002, she joined the Tivoli Support group in Brazil, specializing in Tivoli Management Framework, Remote Control, and Tivoli Workload Scheduler. Currently, she works as a Tivoli Support Specialist for Distributing Monitoring, IBM Tivoli Monitoring, Tivoli Data Warehouse, and the new IBM Tivoli Monitoring 6.1 products.

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

Betsy Thaggard
International Technical Support Organization, Austin Center

Charles Beganskas
IBM USA

Mamadou Toure
CGI Canada

Become a published author

Join us for a two- to six-week residency program! Help write an IBM Redbook dealing with specific products or solutions, while getting hands-on experience with leading-edge technologies. You'll team with IBM technical professionals, Business Partners, and/or customers. Your efforts will help increase product acceptance and customer satisfaction. As a bonus, you'll develop a network of contacts in IBM development labs, and increase your productivity and marketability.

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

ibm.com/redbooks/residencies.html

Comments welcome

Your comments are important to us!

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

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

  ibm.com/redbooks

- Send your comments in an e-mail to:

  redbook@us.ibm.com

- Mail your comments to:

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

1

Architecture and planning

This chapter explains the IBM Tivoli Monitoring 6.1 architecture and how each component operates within an IBM Tivoli Monitoring installation. We explore four architectural designs for IBM Tivoli Monitoring 6.1 using scenarios based on several factors: number of agents, hardware availability, and network restrictions. In addition, an overview section covers IBM Tivoli Monitoring 6.1 agent deployment using several unique strategies.

This chapter discusses the following:

- IBM Tivoli Monitoring 6.1 components
- IBM Tivoli Monitoring 6.1 deployment scenarios
- Scalability
- Agent deployment architecture

1.1 IBM Tivoli Monitoring 6.1 components

An IBM Tivoli Monitoring 6.1 installation consists of various components collectively labeled the Tivoli Monitoring Services framework. This framework is a combination of several vital components. Additionally, optional components can be installed which extend the monitoring functionality of this framework. For platform support details for all the major IBM Tivoli Monitoring 6.1 components, refer to “Platform support matrix for IBM Tivoli Monitoring 6.1” on page 7.

Every IBM Tivoli Monitoring 6.1 installation requires the following components:

- Tivoli Enterprise Monitoring Server (TEMS)

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

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

  The TEMS 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 Management Agent. Additionally, it is responsible for initiating and tracking all generated actions that invoke a script or program on the Tivoli Enterprise Management Agent.

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

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

  – <installation_dir/tables>/<tems_name>
  – <installation_dir>: IBM Tivoli Monitoring 6.1 home directory
  – <tems_name>: Tivoli Enterprise Monitoring Server name

  Note: <tems_name> is the monitoring server name, not necessarily the Tivoli Enterprise Monitoring Server host name.

  The primary TEMS is configured as a Hub(**LOCAL*). All IBM Tivoli Monitoring 6.1 installations require at least one TEMS configured as a Hub. Additional Remote(**REMOTE*) TEMS can be installed later to introduce a scalable hierarchy into the architecture.

  This Hub/Remote interconnection provides a hierarchical design that enables the Remote TEMS to control and collect its individual agent status and

propagate the agent status up to the Hub TEMS. This mechanism enables the Hub TEMS to maintain infrastructure-wide visibility of the entire environment. This visibility is passed to the Tivoli Enterprise Portal Server for preformatting, ultimately displaying in the Tivoli Enterprise Portal client.

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

- Tivoli Enterprise Portal Server (TEPS)

  The Tivoli Enterprise Portal Server (referred to as the *portal server*) is a repository for all graphical presentation of monitoring data. The portal server database also consists of all user IDs and user access controls for the monitoring workspaces. The TEPS provides the core presentation layer, which allows for retrieval, manipulation, analysis, and preformatting of data. It manages this access through user workspace consoles. The TEPS keeps a persistent connection to the Hub TEMS, and can be considered a logical gateway between the Hub TEMS and the Tivoli Enterprise Portal client. Any disconnection between the two components immediately disables access to the monitoring data used by the Tivoli Enterprise Portal client.

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

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

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

  In large installations, installing multiple TEPS that connect to one single Hub TEMS is recommended. See “Large installation (4000 agents maximum)” on page 13 for further details.

- Tivoli Enterprise Portal (TEP)

  The TEP client (referred to as the *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 TEP brings all of these views together in a single window so you can see when any component is not working as expected. The client offers two modes of operation: a Java desktop client and an HTTP browser.

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

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

Here, <hostname> is the host name of the Tivoli Enterprise Portal Server.

Important: IBM Tivoli Monitoring 6.1 supports only Internet Explorer on the Windows platform in browser mode.

The following products will have integrated interfaces into TEP:

- OMEGAMON Z
- OMEGAMON Distributed
- IBM Tivoli Monitoring 5.1.2
- IBM Tivoli Monitoring 6.1
- NetView® for z/OS (release 5.2)
- IBM Tivoli Enterprise Console
- IBM Tivoli Composite Application Manager for Response Time Tracking
- IBM Tivoli Composite Application Manager for WebSphere
- IBM Tivoli Composite Application Manager for SOA

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

- Tivoli Enterprise Management Agent (TEMA)

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

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

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

– Opening or refreshing a workspace that has data views (table or chart views)

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

– The sampling interval for a situation (a test taken at your monitored systems)

  The situation can have an interval as often as once per second or as seldom as once every three months. When the interval expires, the monitoring server requests data samples from the agent and compares the returned values with the condition described in the situation. If the values meet the condition, the icons change on the navigation tree.

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

Tivoli Enterprise Management Agents are grouped into two categories:

– Operating System (OS) Agents

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

– Application Agents

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

Common management agents packaged with IBM Tivoli Monitoring 6.1 include:

– Window OS Agent

– Linux® OS Agent

– UNIX® OS Agent

- UNIX Log Agent
- i5 OS Agent
- Universal Agent

  The Universal Agent is a special agent that leverages a full Application Programming Interface (API) to monitor and collect data for any type of software. Any application that produces data values, the Universal Agent can monitor and retrieve data from it. Essentially, IBM Tivoli Monitoring 6.1 can now monitor any unique application regardless of whether the base product supports it.

Common optional management agents that are packaged separately include:

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

- Warehouse Proxy agent

  The Warehouse Proxy agent is a unique agent that performs only one task: collecting and consolidating all historical data collections from the individual agents to store in the Tivoli Data Warehouse. If using the Tivoli Data Warehouse, one Warehouse Proxy agent is required for each IBM Tivoli Monitoring 6.1 installation. It uses ODBC (Open Database Connectivity) to write the historical data to a supported relational database.

  Restriction: IBM Tivoli Monitoring 6.1 currently supports only the Warehouse Proxy agent under the Windows platform. A post-GA release of IBM Tivoli Monitoring 6.1 will include UNIX operating support.

- Warehouse Summarization and Pruning agent (S&P)

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

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

- Tivoli Data Warehouse (TDW)

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

An IBM Tivoli Monitoring 6.1 installation can contain these optional components:

- Monitoring Agent for IBM Tivoli Monitoring 5.x Endpoint

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

- Tivoli Enterprise Console event synchronization

  The TEC event synchronization component sends updates to situation events back to the monitoring server that are forwarded to the event server. Actions performed at the Tivoli Enterprise Console for IBM Tivoli Monitoring 6.1 situations are reflected in the Tivoli Enterprise Portal Server.

- IBM Tivoli Business Systems Manager (TBSM)

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

Note: IBM will provide a special program called TBSM feed from OMEGAMON (or XE Feed) for IBM Tivoli Monitoring 6.1 and IBM Tivoli Business Systems Manager integration. The XE Feed is planned to be made available as an LA fix to IBM Tivoli Business Systems Manager V3.1 in the first quarter of 2006, then rolled into the IBM Tivoli Business Systems Manager V3.2 release, which is scheduled for September 2006.

1.1.1 Platform support matrix for IBM Tivoli Monitoring 6.1

To get most up-to-date information about the platform support matrix for IBM Tivoli Monitoring 6.1, please refer to the following link:

http://www-306.ibm.com/software/sysmgmt/products/support/Tivoli_Supported_Platforms.html

1.1.2 Database support matrix

Table 1-1 shows the database support matrix for IBM Tivoli Monitoring 6.1.

Note: Database names and versions not listed in this table are not supported, including DB2 on mainframes (zLinux, OS/390®, z/OS, and so forth).

Table 1-1 Database support matrix

Database name	TEPS[1]	Data Warehouse
DB2 8.1	A	A
DB2 8.2	A	A
MS SQL 2000	A	A
Oracle 9.2	D	A
Oracle 10.1	D	A

1. Key: A – Indicates that the platform will be supported.
D – Indicates that the platform will not be supported in this release, but may be supported in a later release.

1.2 IBM Tivoli Monitoring 6.1 deployment scenarios

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

We cover four types of environments:

- “Demo installation (single machine)” on page 10
- “Small/medium installation (400 agents maximum)” on page 11
- “Large installation (4000 agents maximum)” on page 13
- “Huge installation (greater than 4000 agents)” on page 16

Note: Our classification here is based on the number of IBM Tivoli Monitoring 6.1 agents. In practice, sometimes the number of employees is used to define the size of a business; for example, companies with up to 1000 employees are considered as small-to-medium businesses.

Figure 1-1 on page 9 depicts the interconnections of the various components at their simplest. Other chapters in this book explain the interconnections in further detail. Any limitation with hardware or software is noted in the later chapters.

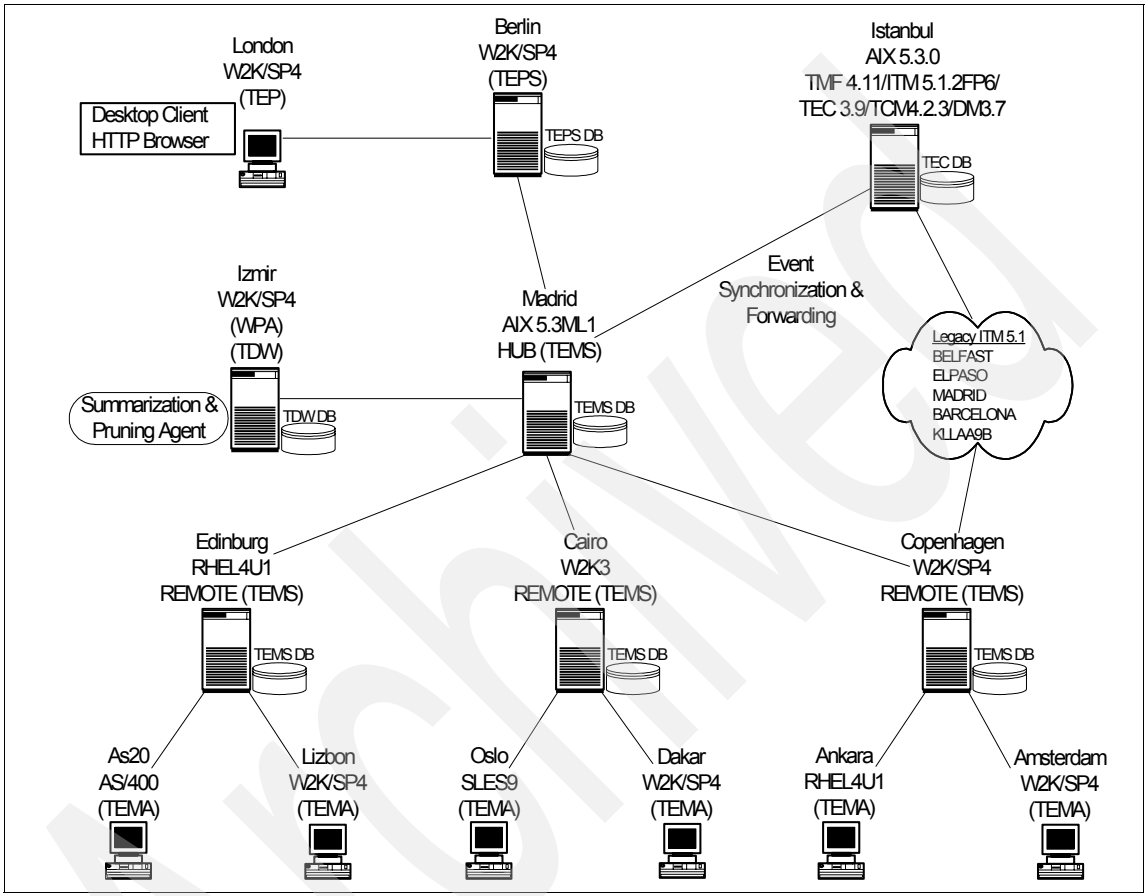

Figure 1-1 IBM Tivoli Monitoring 6.1 lab topology

Notes:

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

To cover various topics throughout this book's development, we implemented an IBM Tivoli Monitoring 6.1 installation that incorporates all related content. This

architecture covers all components that make up an IBM Tivoli Monitoring installation, including the built-in *Hot Standby* Hub Tivoli Enterprise Manager Server. Also, a legacy Tivoli Management Framework V4.1.1 connects to the infrastructure to demonstrate interoperability among IBM Tivoli Monitoring 6.1, IBM Tivoli Monitoring V5.1.2 Fix Pack 6, IBM Distributed Monitoring V3.7, and IBM Tivoli Enterprise Console V3.9. To ensure the accuracy of the implementation and best practices, the environment contains a proportionate selection of heterogeneous hardware configurations with varying degrees of operating system platforms and levels.

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

1.2.1 Demo installation (single machine)

For demonstration purposes, IBM Tivoli Monitoring 6.1 can be installed onto a single machine running Windows XP. *This IBM Tivoli Monitoring 6.1 installation should be used only for demonstration, and is not a supported implementation.* Using the Windows install shield, IBM Tivoli Monitoring 6.1 can be installed using the single CD. The minimum required software is:

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

Optionally, the Tivoli Warehouse Proxy, Tivoli Data Warehouse, Summarization and Pruning agent, and a DB2 installation can be installed on the same system to illustrate the historical data collection features of IBM Tivoli Monitoring 6.1.

1.2.2 Small/medium installation (400 agents maximum)

The small/medium installation is the fundamental design utilizing only the minimum required components. This scenario is perfect for prototyping IBM Tivoli Monitoring 6.1 or using it within a production installation consisting of 400 agents. In fact, IBM Tivoli Monitoring 6.1 by design excels in superiority for the small/medium installation. The out-of-box monitoring collections, GUI presentation layer, historical data collection, and robustness provide a full monitoring solution with a modest total cost of ownership (TCO).

It is implemented with the minimum hardware requirements necessary for a production IBM Tivoli Monitoring 6.1 installation.

The installation consists of the following components:

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

Figure 1-2 depicts the small/medium topology. The diagram provides an overview of each IBM Tivoli Monitoring 6.1 connected component. For a comprehensive architecture, the optional Hot Standby node is depicted in this diagram.

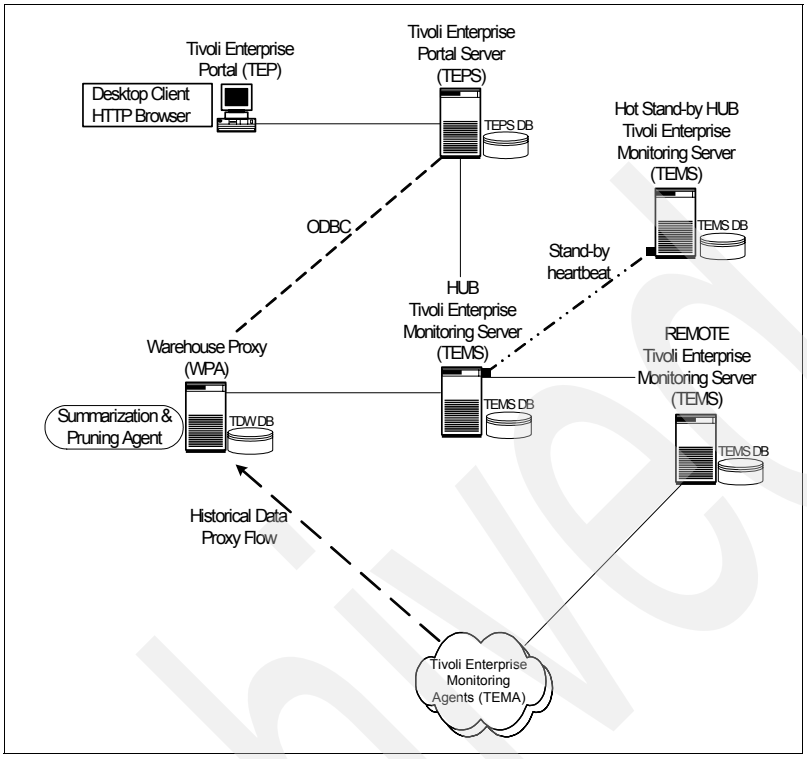

Figure 1-2 IBM Tivoli Monitoring 6.1, small/medium topology design

We recommend installing at least three TEMS (including the Hot Standby node) in this scenario, even though the small/medium installation allows the use of only one TEMS. Implementing a Hub/Remote architecture in the early stages allows for growth and scalability. Furthermore, this design builds around IBM Tivoli Monitoring 6.1 built-in failover capabilities. The small/medium installation supports approximately 250 managed systems. This estimate assumes that the managed systems will have two agents each. The actual distribution of agents will not necessarily be proportionate in a real installation, but this calculation provides the recommended total amount for one IBM Tivoli Monitoring 6.1 installation. All of the agents will connect to the Remote TEMS using the Hub TEMS as a failover monitoring server.

Optionally, you can install the Hot Standby node, This is recommended but not required for the small/medium installation, especially if cost restrictions exist for hardware deployment. The Hot Standby should always be considered because it offers failure protection with minimum increase in total cost of ownership.

Attention: A small/medium installation cannot use a Remote TEMS as a Hot Standby node. Hot Standby nodes always must be configured as *LOCAL.

Although it can handle agent tasks directly, we do not recommend using the Hub TEMS for this purpose. Rather, it should focus on data collecting and processing tasks between the TEPS and itself. If the environment expands, additional Remote TEMS should be installed to process the additional agent requirement. Additional agent deployments increase processing requirements for the Hub TEMS, which can degrade if the Hub is allowed to handle agent tasks directly.

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

1.2.3 Large installation (4000 agents maximum)

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

The installation consists of the following components:

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

Figure 1-3 depicts the comprehensive architecture for all interconnected components. It points out the recommended strategy for the Tivoli historical date collection. We highly advise structuring the historical collection flow as outlined in the diagram.

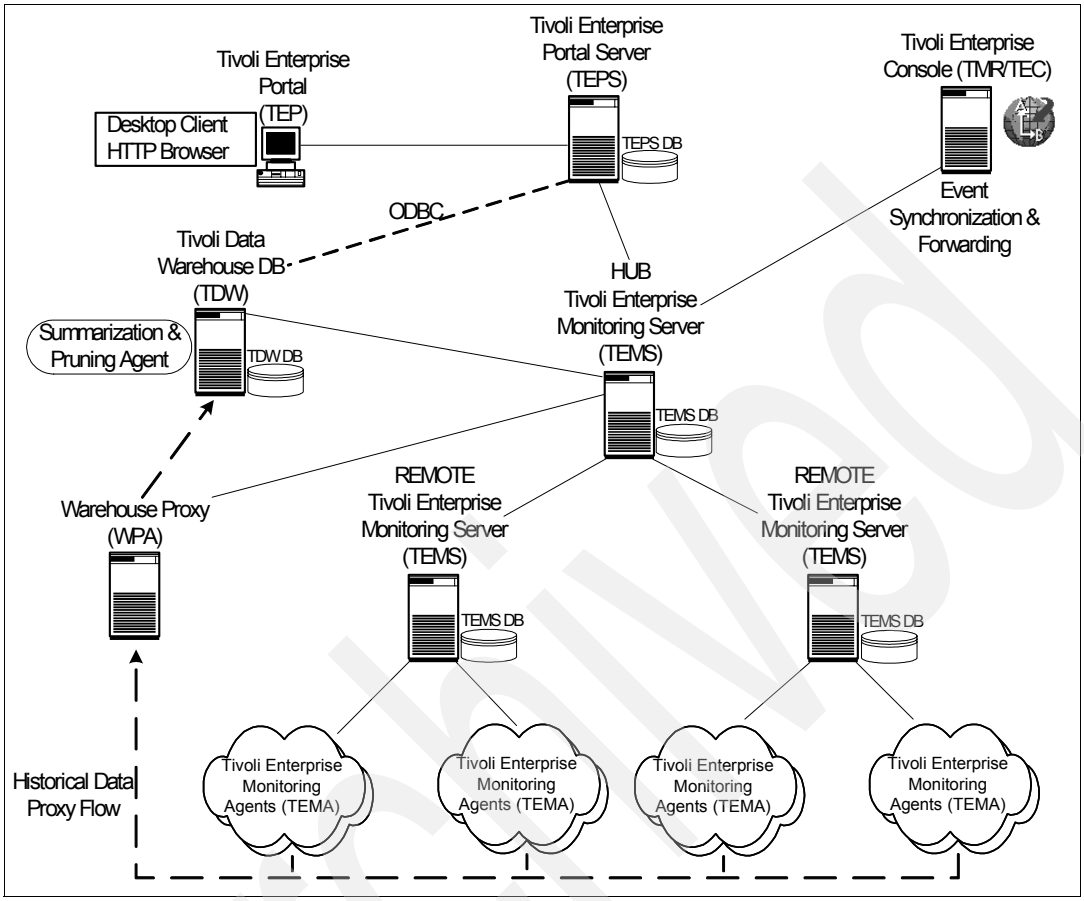

Figure 1-3 IBM Tivoli Monitoring 6.1 large topology design

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

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

the underlying network topology. Network bandwidth, latency, and firewall restriction all require assessment.

IBM Tivoli Monitoring 6.1 is ideal for small/medium installations. After installation, it begins leveraging the best practice functionality immediately. Default situations start running, and if historical data collection is turned on, the default attribute groups begin analysis and warehousing. These default services can impede the large installation performance throughput, especially if unnecessary attributed group collections are enabled. We highly suggest changing the *Run at Startup* property on all situations to `NO` immediately after the TEMS, TEPS, and TEP are deployed. This practice ensures the freedom to execute the business plan strategy (defining managed system list, customized situation, event mapping, date warehousing intervals, and so forth) that are generated from the assessment and planning phrase. It is vital to the health of the large installation that only the desired situations and attribute groups are enabled.

A large monitoring installation supports approximately 1,500 managed systems in an environment. For the large installation, the estimate is three agents per managed system. In this installation, a disproportionate distribution of agents is highly anticipated, and this scenario should complement your own environment analysis phrase. The recommended distribution is 400 agents across 10 Remote TEMSs. Keeping 400 agents as the high point per monitoring server allows for capacity expansion without exhausting the resources of the infrastructure. For further details about scaling a large installation, refer to “Scalability” on page 33.

Tip: Because IBM Tivoli Monitoring 6.1 supports primary and secondary communication paths, we suggest installing several backup Remote TEMSs that exist solely for TEMA failover capabilities. If a Remote TEMS fails, we do not advise doubling the maximum load of production Remote TEMSs. Best practices should direct these orphan Tivoli Enterprise Management Agents to idle Remote TEMS.

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

The large installation introduces the IBM Tivoli Enterprise Console as part of the topology. IBM Tivoli Monitoring 6.1 has built-in capabilities for event processing that work extremely well in the small/medium installation. However, the large installation can contain a reasonable increase in volume of event flow, and the Tivoli Enterprise Console is better adapted for large event flow management and

correlation. The Tivoli Enterprise Console can be considered an event consolidation Manager of Managers.

The TCO is still nominal compared to IBM Tivoli Monitoring 6.1 functionality, despite the large hardware requirements needed to scale this installation properly. The entire large installation can be managed from a single GUI presentation layer down to installing and upgrading agents.

1.2.4 Huge installation (greater than 4000 agents)

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

The installation consists of the following components:

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

Figure 1-4 on page 17 depicts the interconnections between two autonomous IBM Tivoli Monitoring 6.1 installations. It demonstrates the high-level component interaction between two installations that handle 4,000 agents each, totaling 8,000 agents entirely.

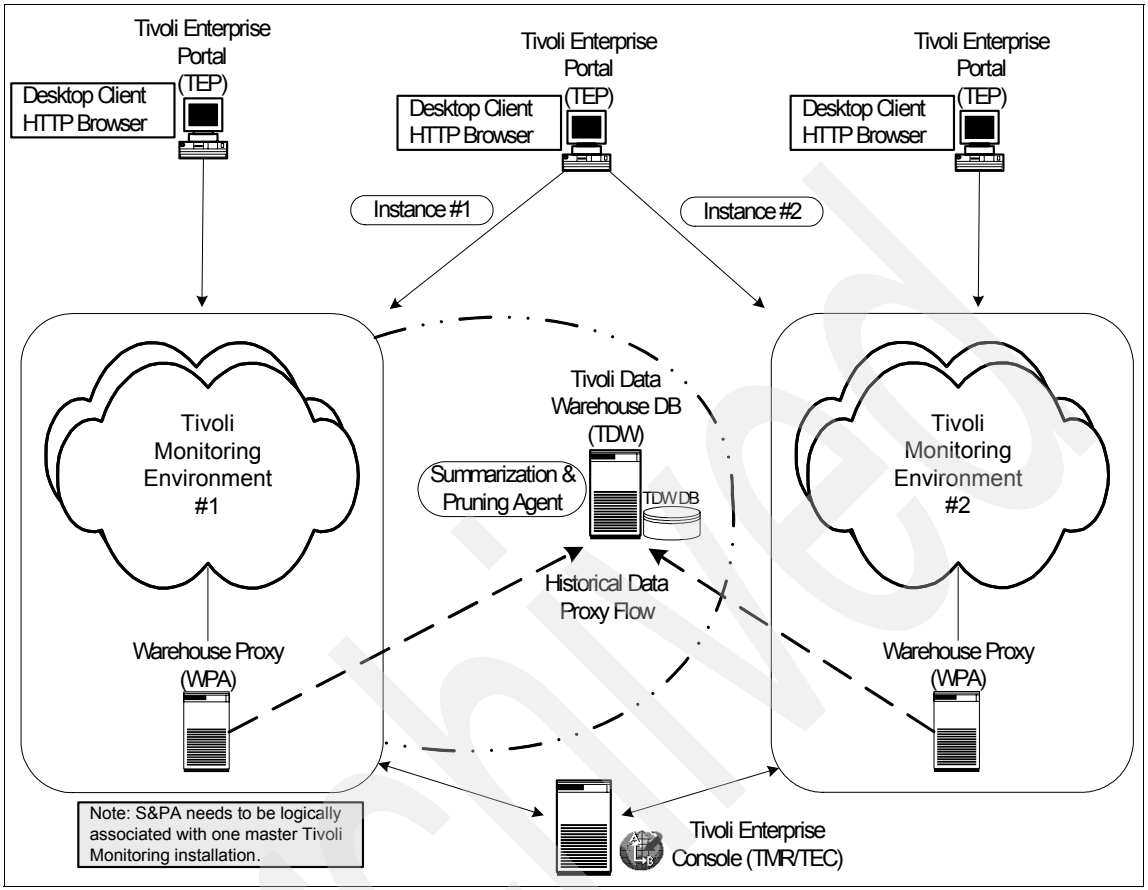

Figure 1-4 IBM Tivoli Monitoring 6.1 huge installation topology

The recommended deployment strategy is the same as for the large installation, except for the Tivoli Data Warehouse, and Summarization and Pruning agent. A huge installation can warehouse historical data collections to one single database server repository from two distinct IBM Tivoli Monitoring 6.1 installations.

Important: As noted in “Large installation (4000 agents maximum)” on page 13, 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 6.1 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 6.1 installation requires a logical association as the *master* control for the Summarization and Pruning agent.

Note: There can be only one Summarization and Pruning agent for a single Tivoli Data Warehouse. Because the Summarization and Pruning agent requires connections to a TEMS, one of the monitoring installations must be logically designated as the master. This is not a programmatic assignment, but a logical identification for configuration and management of the S&P.

A flexible feature that is needed in the huge installation is the ability to configure multiple TEP instances in a single TEP desktop client. If a single TEP desktop client has to connect to a separate autonomous IBM Tivoli Monitoring 6.1 installation, *instances* are created to associate the unique TEPS connection information.

Defining TEP instances via Tivoli Manage Service GUI

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

1. Start the Manage Tivoli Enterprise Monitoring Services GUI.

Windows	Click **Start** → **Programs** → **IBM Tivoli Monitoring** → **Manage Tivoli Enterprise Monitoring Services**.
UNIX/Linux	Type `itmcmd manage`

2. Right-click the Tivoli Enterprise Portal and click **Create Instance** as shown in Figure 1-5 on page 19.

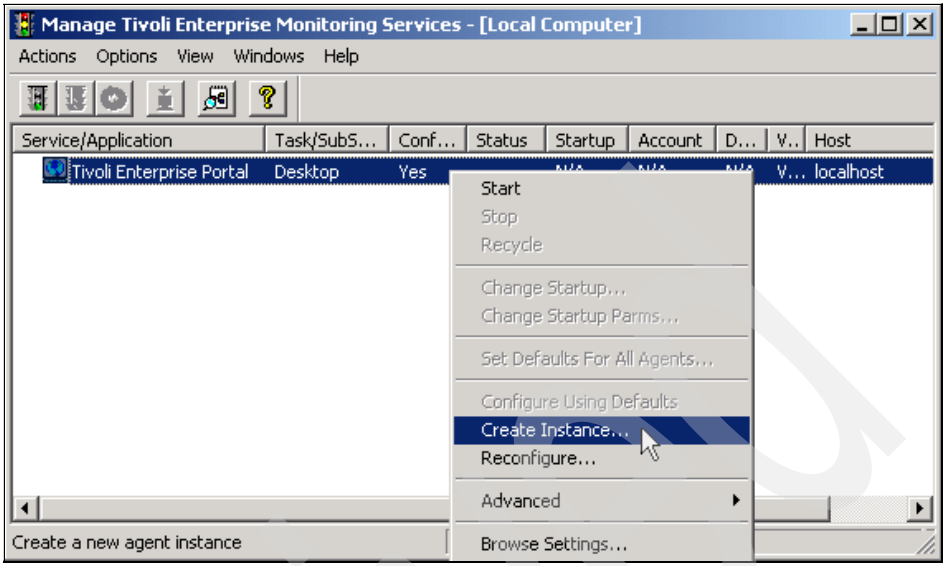

Figure 1-5 Right-click Tivoli Enterprise Portal for Create Instance option

3. Type the instance name and click **OK** (Figure 1-6).

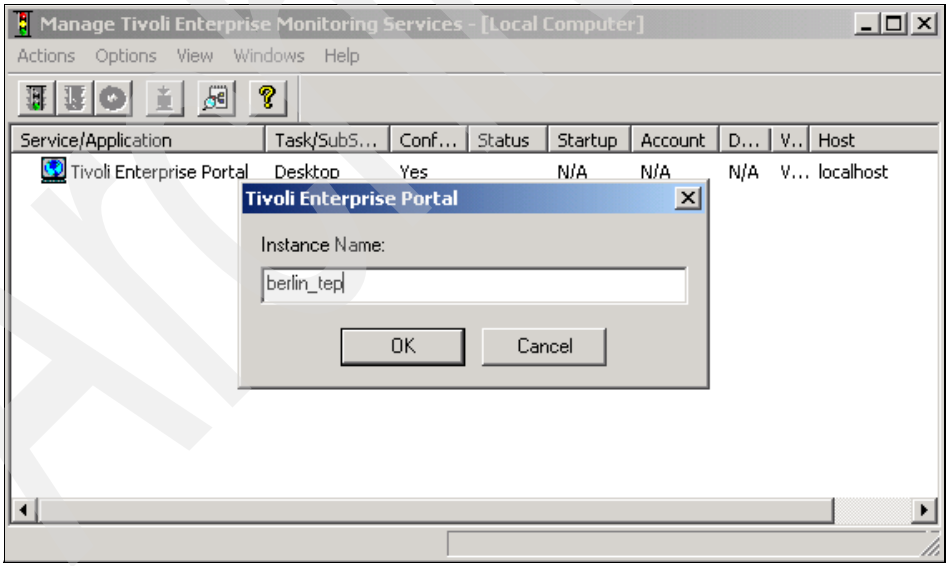

Figure 1-6 Entering the Instance Name into the dialog box

4. Type the Tivoli Enterprise Portal host name and click **OK** (Figure 1-7**)**.

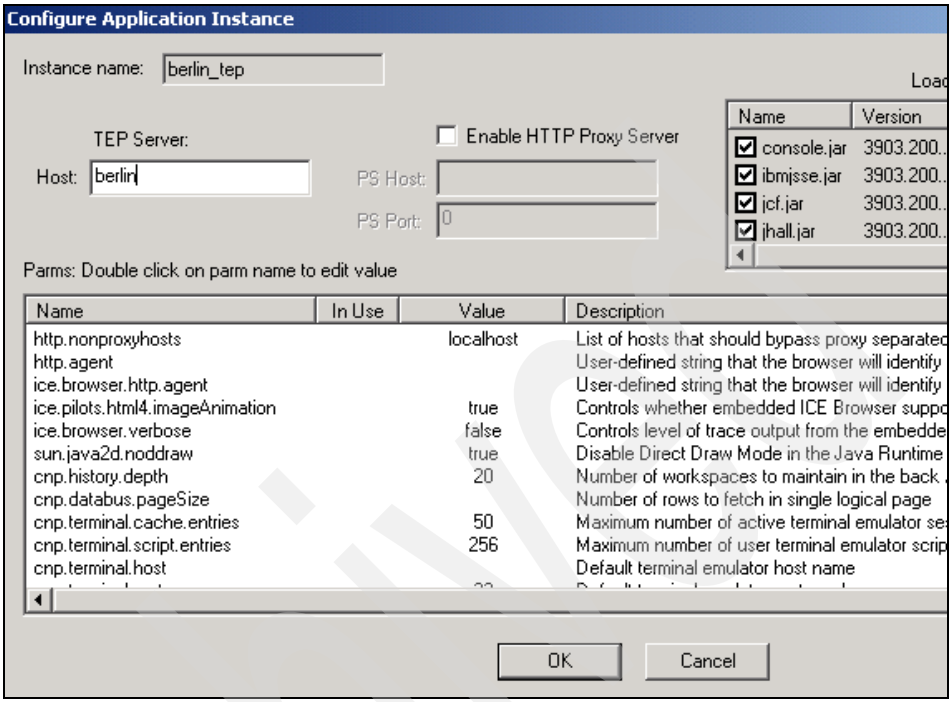

Figure 1-7 Entering Tivoli Enterprise Portal host name into TEP Server field

5. The new Tivoli Enterprise Portal is now displayed in the Manage Tivoli Enterprise Monitoring GUI (Figure 1-8).

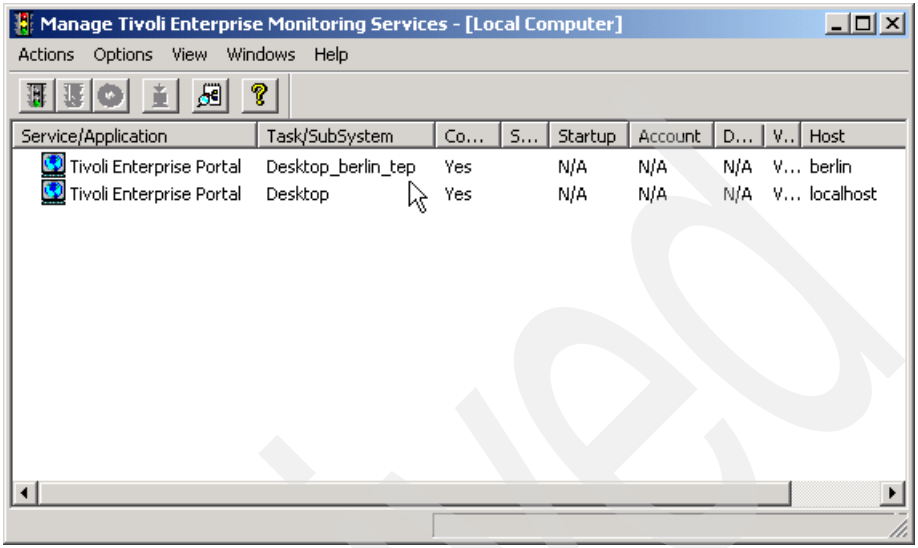

Figure 1-8 The newly defined Tivoli Enterprise Portal instance

Subsequent Tivoli Enterprise Portal instances are defined repeating steps 1 - 4 (Figure 1-9).

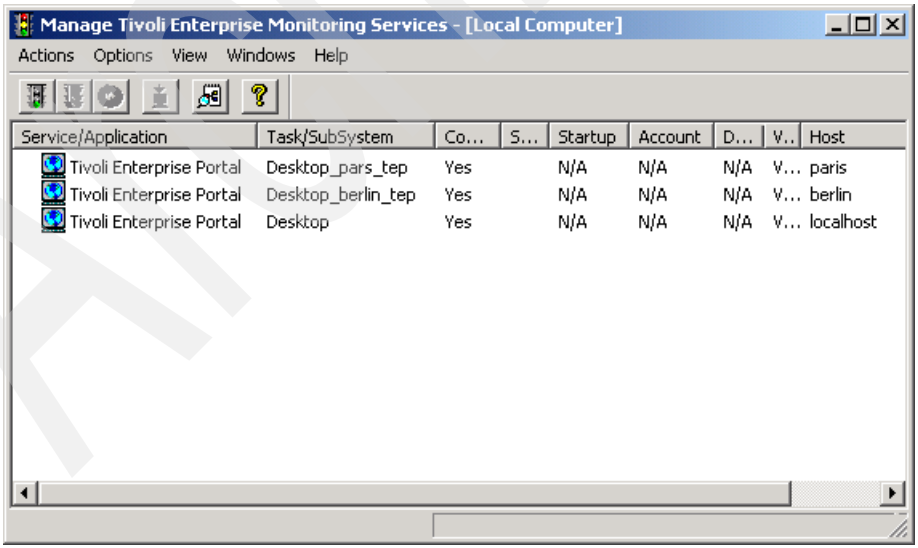

Figure 1-9 Example of additional Tivoli Enterprise Portal instances

1.2.5 Advanced large installation with firewall scenarios

In most IBM Tivoli Monitoring 6.1 implementations, firewalls play an important role throughout the architecture. For a successful implementation, it is important to understand the component communication flow. The configuration to support IBM Tivoli Monitoring 6.1 within firewalls has two major parts:

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

Tip: Refer to the *IBM Tivoli Monitoring Installation and Setup Guide*, GC32-9407, for expert advice about firewall scenarios. This book has several excellent examples using firewalls involving the TEP and TEPS.

Communications protocol selection

If installing IBM Tivoli Monitoring 6.1 components across firewalls, the recommendation is to configure the *IP.PIPE* (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 individual IBM Tivoli Monitoring 6.1 component. For example, a TEMA communicating to the TEMS using IP (UDP communication) protocol requires multiple ports to operate properly. Also, using the IP.PIPE (TCP communication) enables the *Ephemeral pipe* operation automatically if certain conditions match.

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

The IP.PIPE protocol has some notable limitations:

- Only 16 IBM Tivoli Monitoring 6.1 processes on a single system can share the base listening port (default port 1918) on a single network interface card when using the protocol. Any processes above 16 will fall back to using the IP protocol (only if configured). This mainly is a restriction when running large numbers of Tivoli Enterprise Management Agents on one physical system. It is not a limitation for the total amount of TEMA connecting to one TEMS. This may occur only when a system is required to run more than 16 Universal Agents or has more than 16 Database Agent instances. If firewall restrictions force the use of the IP.PIPE protocol, the only workaround is to move excess Tivoli Enterprise Management Agents above 16 to another system.

- The TEMS may run out of sockets (listen threads). The TEMS log shows evidence of this:

  ```
  message KDSMA010 – Communication did not succeed.
  ```

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

Table 1-2 depicts the *default* listening ports for the IBM Tivoli Monitoring 6.1 components. Use this table as a quick reference to understand the standard ports for an installation. Although modifying these default values is supported, it is not recommended.

Table 1-2 Default port usage for IBM Tivoli Monitoring 6.1

IBM Tivoli Monitoring 6.1 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[1]

1. Refer to Example 1-1 on page 24.

Tip: Do not deviate from the default listening ports without a valid reason, even though this is supported. Listening port modification was not tested by IBM Tivoli Software Group.

Using IP.PIPE enables a few well-known ports to be open through the firewall. You can use Example 1-1 on page 24 to calculate which port to open. If the firewall is not using NAT (Network Address Translation), the computation should be sufficient to have the components connect through the firewall.

Every system that has IBM Tivoli Monitoring 6.1 installed will automatically reserve the well-known port (default 1918) for the Tivoli Enterprise Monitoring Server communication. No matter what order components start up on a system that has several IBM Tivoli Monitoring 6.1 components installed, the default well-known port is only used by the TEMS.

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

For all components other than the TEMS, the calculation in Example 1-1 is used internally by IBM Tivoli Monitoring 6.1 to reserve the listening ports.

Example 1-1 IBM Tivoli Monitoring 6.1 algorithm to calculate listening port

```
"reserved port" = well-known port + (N*4096)
where:
N= startup sequence
```

For example, the IBM Tivoli Monitoring 6.1 component startup on the system Izmir follows this sequence:

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

Not all communication is through the firewall

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

This is accomplished by specifying the SKIP and COUNT parameters on the KDC_FAMILIES environment variable for the individual IBM Tivoli Monitoring 6.1 component. (See Example 1-2 on page 25.)

For example:

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

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

Example 1-2 Example for KDC_FAMILIES=IP.PIPE COUNT

```
The system Izmir has installed:
-Tivoli Enterprise Monitoring Server
-Windows OS Agent
-Warehousing Proxy agent

The well-known port is the default port 1918.
The Tivoli Enterprise Monitoring Server always uses port 1918.
The Windows OS agent does not require firewall access and should be coded with
KDC_FAMILIES=IP.PIPE SKIP:2 (port 10110).
If the Windows OS agent fails to open port 10110, it will try SKIP:3 attempting
to bind now to port 10370. A failure will result in trying SKIP:4 continuing to
exhaust all possibilities with any subsequent failures.
The Warehouse Proxy does require firewall access and should coded with
KDC_FAMILIES=IP.PIPE COUNT:1 (port 6014).
If the Warehouse Proxy fails to open port 6014, start up fails.
```

Multiple network interface cards

Whenever an IBM Tivoli Monitoring 6.1 component starts up, by default it discovers all available network interfaces on the system and actively uses them. This may not always produce the desired results.

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

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

To avoid this problem, you can specify an environment parameter on all of the IBM Tivoli Monitoring 6.1 components to force it to use a specific network interface rather then using any available.

This can be accomplished by passing either of these keywords:

- KDCB0_HOSTNAME: You can specify either the host name, corresponding to the NIC to be used, or its IP address in dotted decimal format. If specified, it will take priority over the KDEB_INTERFACELIST parameter. KDCB0_HOSTNAME should be used only in an environment without NAT

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

- KDEB_INTERFACELIST: The NIC must be specified as dotted decimal IP addresses. This keyword is recommended when IBM Tivoli Monitoring 6.1 is installed in a environment with NAT.

Regardless, this technique is still a good practice to ensure that the Tivoli Enterprise Management Agents connect to the proper TEMS interface.

Installations with firewalls

The best practice with Tivoli Enterprise Management Agents on the less secure zone of the firewall is to deploy a Remote TEMS on the same firewall side. This enables all TEMAs to connect to the Remote TEMS and have only the Remote TEMS connect through the firewall.

This minimizes the number of systems that need firewall access and keeps port restrictions in place. Refer to Figure 1-10 on page 28 and Figure 1-11 on page 29 for a visual diagram.

Special cases

- Firewall with NAT — Ephemeral Pipe

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

  – KDC_PARTITION definition file is not present; if KDC_PARTITION is used, it inactivates the Ephemeral Pipe.

  – KDCB0_HOSTNAME parameter should not be specified; instead use the KDEB_INTERFACELIST variable.

  – The initial communication must come from the agents, not by the TEMS. Older configurations may still have a KDSSTART LBDAEMON command for the Location Broker at the TEMS. This command should be removed to active the Ephemeral Pipe.

  If these conditions are met, TEMA-to-TEMS communication automatically tries to create an Ephemeral Pipe connection and no further configuration actions are required. The main advantage of using Ephemeral Pipe is that no special configuration is required, so you do not have to *manually* update the

configuration parameters at possibly hundreds of TEMAs that run outside of the firewall.

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

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

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

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

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

- Firewall with NAT – Partitioning

  If Ephemeral Pipe fails to establish a connection between the agents and the Hub TEMS, the only alternative with this IBM Tivoli Monitoring 6.1 release is to use partition files. This is fully documented in the *IBM Tivoli Monitoring Installation and Setup Guide*, GC32-9407.

Large installation with firewall architectures

Keep in mind that security guidelines in a specific environment may be inflexible when dealing with the location of some of the IBM Tivoli Monitoring 6.1 components. Accurate comprehension of the communication flows and ports enable any installation to be customized to meet the underlying security policies.

The following recommended architectures provide visual guidance in understanding the communication flow among the IBM Tivoli Monitoring 6.1 components. Mastery of IBM Tivoli Monitoring 6.1 communication protocol provides the architect control over the entire network topology. We now describe two common designs.

Warehouse Proxy agent in less secure zone

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

Figure 1-10 depicts one recommended architecture for a IBM Tivoli Monitoring 6.1 installation with firewall restrictions enabled and with the Warehouse Proxy agent located in the less secure zone.

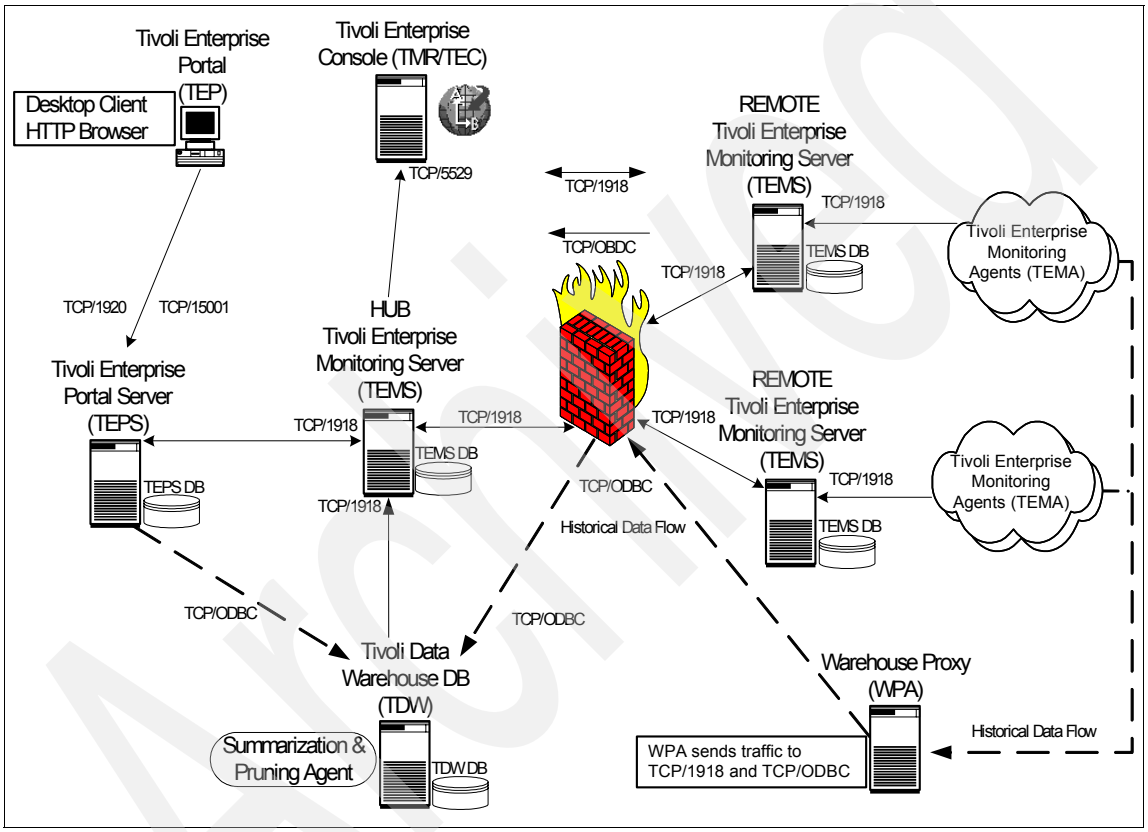

Figure 1-10 Advanced installation on less secure side

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

unique to each RDBMS. Consult the database product manuals or your local database administrator.

Warehouse Proxy agent in more secure zone

In this second scenario, the firewall restrictions are expanded to prevent any warehousing traffic on the less secure side of the firewall.

Figure 1-11 depicts the recommended architecture for an IBM Tivoli Monitoring 6.1 installation with firewall restrictions increased, and the Warehouse Proxy agent located in the more secure zone.

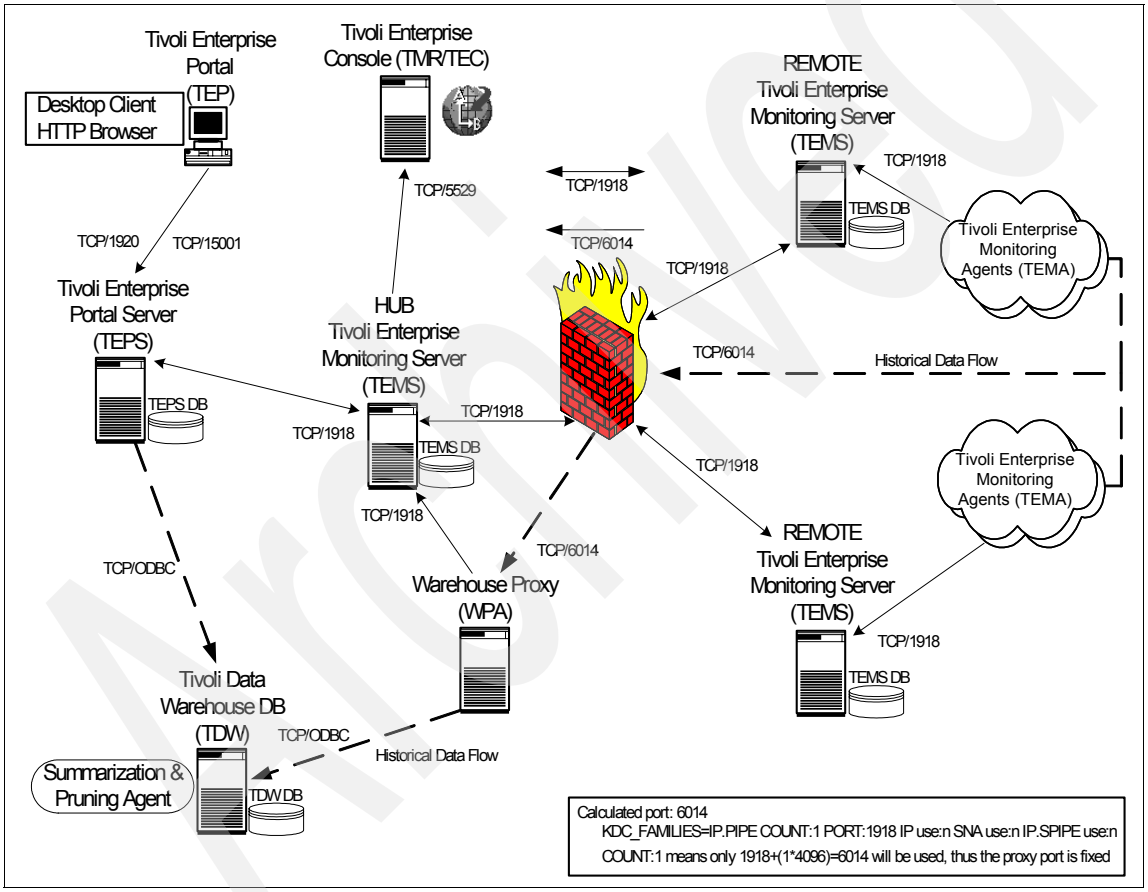

Figure 1-11 Advanced installation on more secure side

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

To open the proper ports so that the TEMA can warehouse the historical data through the firewall, the Warehouse Proxy agent must establish a well-known listening port. This well-known port is calculated through the KDC_FAMILIES mechanism.

Tip: The Warehouse Proxy agent calculated port is significant only when:

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

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

- Accurately calculate the collection amount of historical data. Firewall traffic can increase excessively when historical data collection is enabled.
- Only collect the critical attribute groups, being careful not to turn on unnecessary attribute groups.
- Historical data roll-up can be stored on the Remote TEMS. However, it is severely limited to 250 TEMAs per Remote TEMS.
- Windows has a limit of a maximum 2,000 sockets open simultaneously. Within a firewall environment, IP.PIPE is required. This limits the warehousing of historical data to only 1,500 TEMAs (500 sockets are reserved for internal processing) per IBM Tivoli Monitoring 6.1 installation.

Important: If you are familiar with the functions of Tivoli Firewall Security Toolbox (TFST), IBM Tivoli Monitoring 6.1 firewall support currently does not provide all of the functions of the TFST, particularly to be able to start the connection from the secure site and proxying between multiple firewalls (to be able to use different ports between multiple firewalls). These functions are expected to be available with a post-GA fix pack for IBM Tivoli Monitoring 6.1.

1.2.6 Advanced huge installation: multiple TEMS processes

This advance deployment scenario illustrates the power, flexibility, and capabilities of IBM Tivoli Monitoring 6.1. This deployment strategy requires double the recommended hardware specifications but less physical hardware deployment. This deployment exposes the technical capacity of running multiple

monitoring server (TEMS) processes on one physical system. It certifies the adaptability of IBM Tivoli Monitoring 6.1, but acknowledges the extreme complexity that can occur within an installation.

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

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

The installation consists of the following components:

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

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

Figure 1-12 on page 32 demonstrates a simple architecture to present the underlying theory. IBM Tivoli Monitoring 6.1 can expand farther and run more than two kdsmain processes per system. This technique accomplishes a larger implementation with less physical hardware. To keep the diagram intelligible, the Remote TEMS have been stacked for brevity. Even though this strategy is similar to the large installation (the implementation is exactly the same), we do not recommend loading this IBM Tivoli Monitoring 6.1 installation to its maximum throughput.

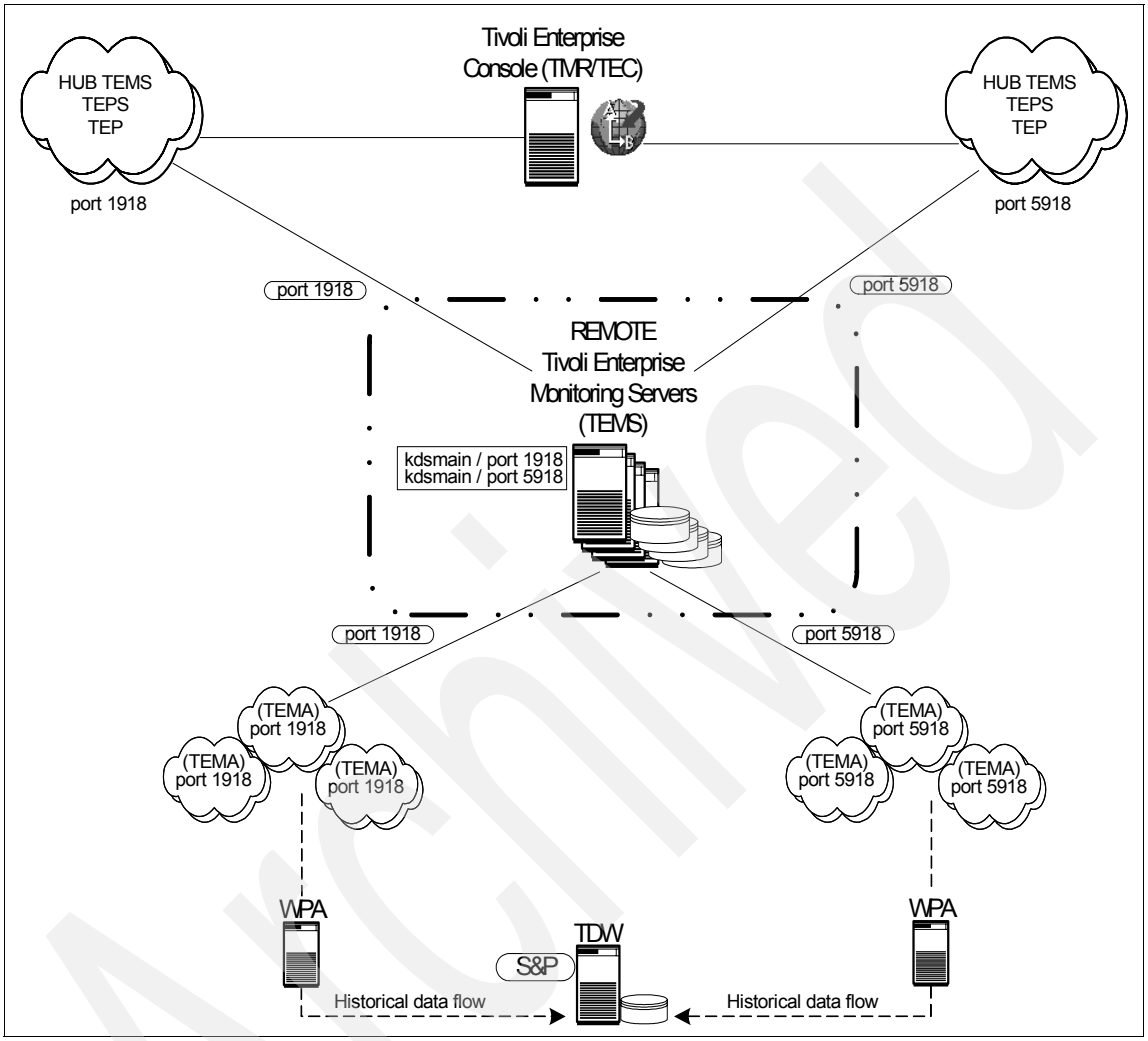

Figure 1-12 Large installation with multiple TEMS processes on single system

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

IBM Tivoli Monitoring 6.1 has a software limitation that permits only a single TEMS process to listen on the well-known port (default port 1918). To achieve this design, any additional TEMS processes on the exact system must be configured to use an unused port. This process essentially doubles the IBM Tivoli Monitoring 6.1 capacity without additional hardware. We advise running only one

Hub TEMS per physical system. Although supported, multiple TEMS processes on a single system all configured as (*HUB) is not suggested.

To accomplish this installation, separate IBM Tivoli Monitoring 6.1 install directories are necessary. These installations will be completely separate despite the binaries existing on the same physical system. Follow the normal installation procedures for a single large installation environment. The only necessary installation procedure change is the configuration of the well-known listening port for each running TEMS process. For historical data collection, it is exactly the same as a huge installation: one Tivoli Data Warehouse repository with multiple Warehouse Proxy agents.

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

One thought to keep in mind: These multiple TEMS processes are still logically independent installations that each require separate maintenance. The infrastructure systems will have distinct CANDLEHOME installation directories. The IBM Tivoli Monitoring 6.1 code on every system will require maintenance to every separate installation directory.

Attention: Running multiple TEMSs on a single system is technically supported by IBM Tivoli Monitoring 6.1. However, all alternatives should be given careful consideration. The total cost of ownership to maintaining this complex environment can be higher than the cost of additional hardware capacity.

1.3 Scalability

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

No single analysis of scalability and performance can determine the absolute hard limits of a distributed product. A distributed system in theory should extend to infinity. However, as distributed systems increase in scalability, performance loss may increase to an unsustainable boundary. IBM Tivoli Monitoring 6.1 follows the basic scalable characteristic in this design. Adding hardware capacity in the form of remote TEMS distributes the load and allows more connected agents. This methodology represents a foundation that is built upon using the

actual calculated values from the physical environment. Note that IBM Tivoli Monitoring 6.1 constitutes vast improvements in scalability and performance from OMEGAMON XE, highlighting the union between the mature code of Candle Corporation and the enterprise qualification of IBM Tivoli Software.

Figure 1-13 depicts a great universal example of many unique sources of information pertaining to scalability and performance metrics. It exposes the issues related to scalability and performance expectations.

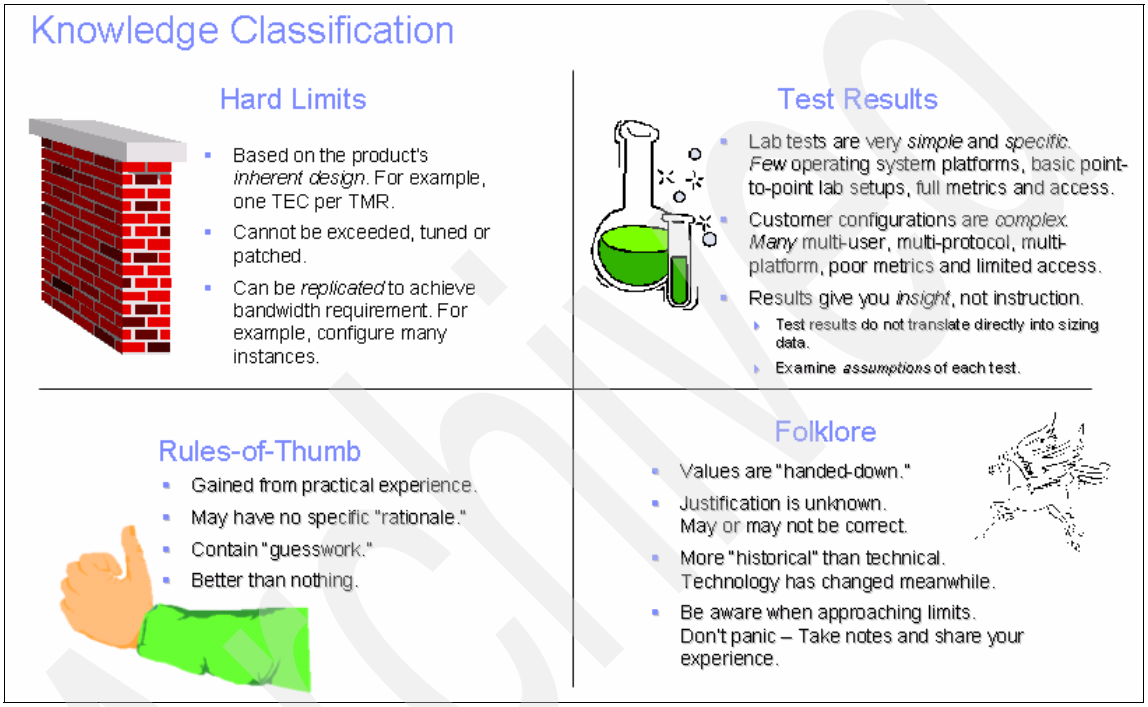

Figure 1-13 Universal sources of scalability and performance numbers

For example:

- User Guide says “unlimited”
- Support said “no more than n …”
- Development said “n*3 …”
- Early Support Program said “n^3 …”
- Services said “n/3 ...”
- Performance said “we didn’t test that.”

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

For IBM Tivoli Monitoring 6.1, analysis of all of these sources, including an in-depth knowledge of the monitoring environment, assists in scaling the installation properly. Understanding the limitations of IBM Tivoli Monitoring 6.1 and strategically working through them will facilitate obtainable goals.

From a scalability standpoint, the TEMS plays the key role. As the architect of an IBM Tivoli Monitoring 6.1 implementation, consider the following factors:

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

The information generated from these points above can then be combined with the scalability guidelines that have been established for the initial release of IBM Tivoli Monitoring 6.1.

The following scalability metrics are from verification testing performed on IBM Tivoli Monitoring 6.1 (GA). These numbers represent actual test synopsis validation. These numbers are not definitive declarations of scalability and performance. This data displays achievable goals that have been proven in a test/development environment. All IBM Tivoli Monitoring 6.1 installations are unique and require surveillance during the deployment.

Table 1-3 classifies the extensive metrics for IBM Tivoli Monitoring 6.1. These metrics measure the apex for the IBM Tivoli Monitoring 6.1 components with respect to load quantity. Each metric represents one installation instance.

Table 1-3 Extensive metrics

IBM Tivoli Monitoring 6.1 component	Verified metric
Remote TEMS	15 (Windows and UNIX)
Managed Systems	5,000
Managed Systems per Remote TEMS	500
Heartbeating agents per TEMS	500

IBM Tivoli Monitoring 6.1 component	Verified metric
Simultaneous agent startup/logins to a TEMS	1,000
Agents storing historical data at Remote TEMS	250
Consoles per TEPS	50
Total situations	1,500 (30/agent)

Important: These metric values do not represent actual hard limits in IBM Tivoli Monitoring 6.1. These numbers are derived from what was actually tested, not necessarily product limitation.

The Tivoli Data Warehouse scalability and metrics are beyond the scope of this chapter.

1.4 Agent deployment architecture

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

All three scenarios include the positives and negatives of an established solution. Proper assessment of the physical environment is part of the decision of which solution best fits.

Tips to keep in mind:

- Total number of physical systems and the total amount of agents deployed to each of those systems
- Network bandwidth and latency between TEMS and TEMA
- Size of the IBM Tivoli Monitoring 6.1 installation
- Connectivity to the managed systems

1.4.1 IBM Tivoli Monitoring 6.1 built-in deployment controller

IBM Tivoli Monitoring 6.1 offers an easy, efficient deployment mechanism to push Operating System Agents and Applications Agents to remote systems. This mechanism also offers agent upgradability. IBM Tivoli Monitoring 6.1 provides a powerful built-in tool for intelligent agent upgrades via the GUI or command line.

Figure 1-14 shows the architecture of IBM Tivoli Monitoring 6.1 agent components. The functionality of the agent components is divided among the TEPS, TEMS, and OS Agent, respectively.

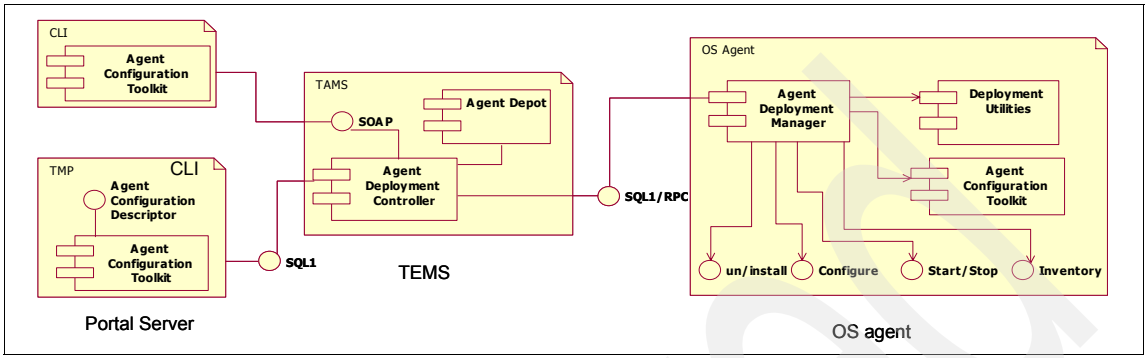

Figure 1-14 Agent deployment architecture

IBM Tivoli Monitoring 6.1 OS Agents, implemented as a DLL, can handle agent deployment activities at the agent end.

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

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

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

Each agent bundle in the Agent Depot can be determined by its product ID and platform characteristics. The Agent Depot can also contain MDL files and scripts used in the deployment of the Universal Agent. You can customize the Agent Depot based on the types of bundles that you want to deploy and manage from that monitoring server.

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

Notes:

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

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

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

Agents vary greatly in how they are configured depending on the agent type and the OS platform. The Agent Configuration Toolkit collects and transfers configuration data. It provides a set of utilities that enable the agent deployment to configure agents. The Agent Configuration Toolkit and the deployment controller communicate via SOAP (Simple Object Access Protocol).

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

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

1.4.2 Tivoli Configuration Manager V4.2

Most IBM Tivoli Software customers already have an investment in Tivoli Management Framework V4.1.1 and IBM Tivoli Configuration Manager V4.2. IBM Tivoli Monitoring 6.1 Agents can be deployed using IBM Tivoli Configuration Manager V4.2 as the delivery mechanism.

It is cost-effective to leverage IBM Tivoli Configuration Manager V4.2 as a solution to deliver IBM Tivoli Monitoring 6.1 Agents. IBM Tivoli Configuration Manager V4.2 is robust and designed for large-volume software pushes, which dominates over IBM Tivoli Monitoring 6.1 Deployment Controller.

1.4.3 Operating system image deployment

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

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

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

Operating system imaging is beyond the scope of this book. This is an alternate method that can be employed and is another recommended deployment solution.

2

Demonstration, Proof of Concept, and small-size installation

This chapter describes how to install IBM Tivoli Monitoring 6.1 and related components, and PoC (Proof of Concept) and demonstration purposes. You can also use this type of installation for small-size environments.

The following topics are covered:

- DB2 Workgroup Server Edition installation and configuration
- IBM Tivoli Monitoring 6.1 components installation

2.1 DB2 Workgroup Server Edition installation and configuration

Before we install IBM Tivoli Monitoring 6.1, we need to install a database. The *Tivoli Enterprise Portal Service (TEPS)* requires one relational database to store all user data, user IDs, workspaces, links, queries. The *Tivoli Data Warehouse (TDW)* requires another relational database to store the historical data. The IBM Tivoli Monitoring 6.1 is shipped with IBM DB2 Workgroup Server Enterprise Server Edition, for demonstration and installation purposes, so we are going to install that version. Refer to Version 6.1.0 of *IBM Tivoli Monitoring Installation and Setup Guide*, GC32-9407, for supported databases and hardware and software requirements.

The next steps describe how to install DB2 Workgroup Server Edition in Windows 2000 and how to set up the required databases components.

2.1.1 Installing DB2 Workgroup Server Edition

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

1. Log on to the system with the Administrator account.
2. To start the installation, go to the installation image location. In our case this was C:\ITM61_image\db2_image.
3. Launch **setup.exe**.
4. In IBM DB2 Setup Launchpad, click **Install Product**.
5. Click **Next** in DB2 Workgroup Server Edition to start the DB2 Setup Wizard.
6. Read and accept the terms in the license agreement, select **I accept the terms in the license agreement**, and click **Next**.

7. Select **Typical** and click **Next** under Select the installation type as shown in Figure 2-1.

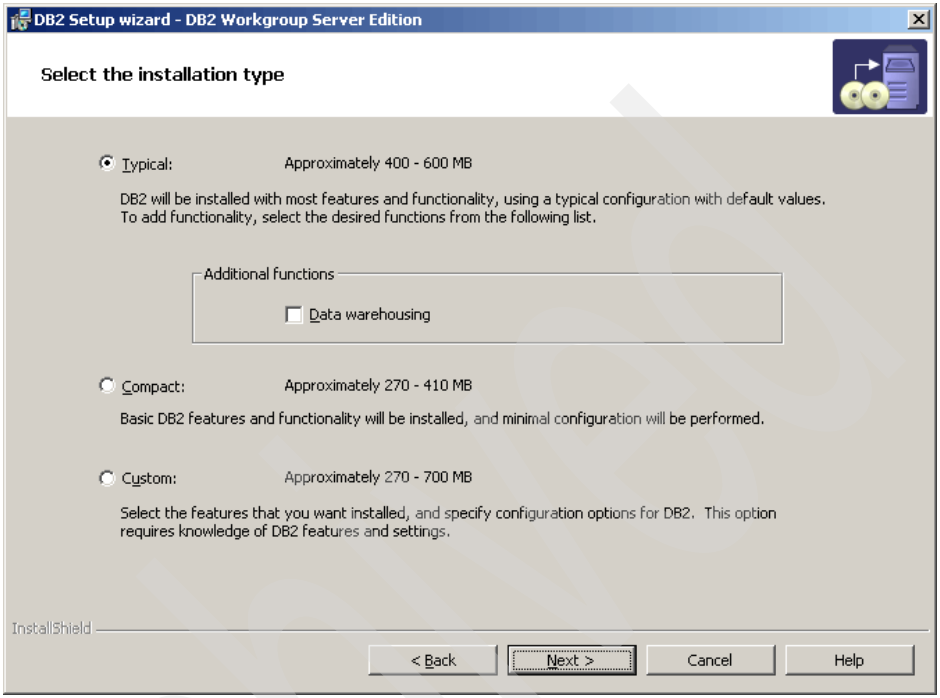

Figure 2-1 DB2 Setup wizard - Select the installation type

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

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

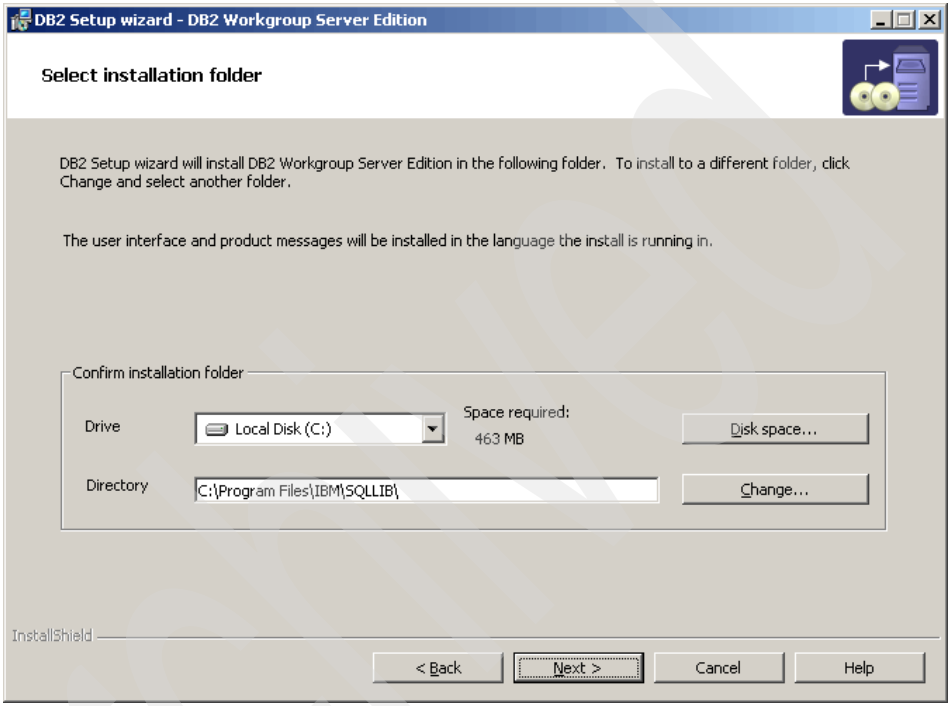

Figure 2-2 DB2 Setup wizard - Select installation folder

9. The DB2 Setup wizard creates a user for DB2 administration purposes. In the window Set user information for the DB2 Administration Server, select **Local user or Domain user account** and **Use the same user name and password for the remaining DB2 services**. For User Information, do this:

   Domain (Leave blank unless you are using domain user.)

   User name db2admin

   Password itm61dgrb

   Confirm password itm61dgrb;

   Click **Next**.

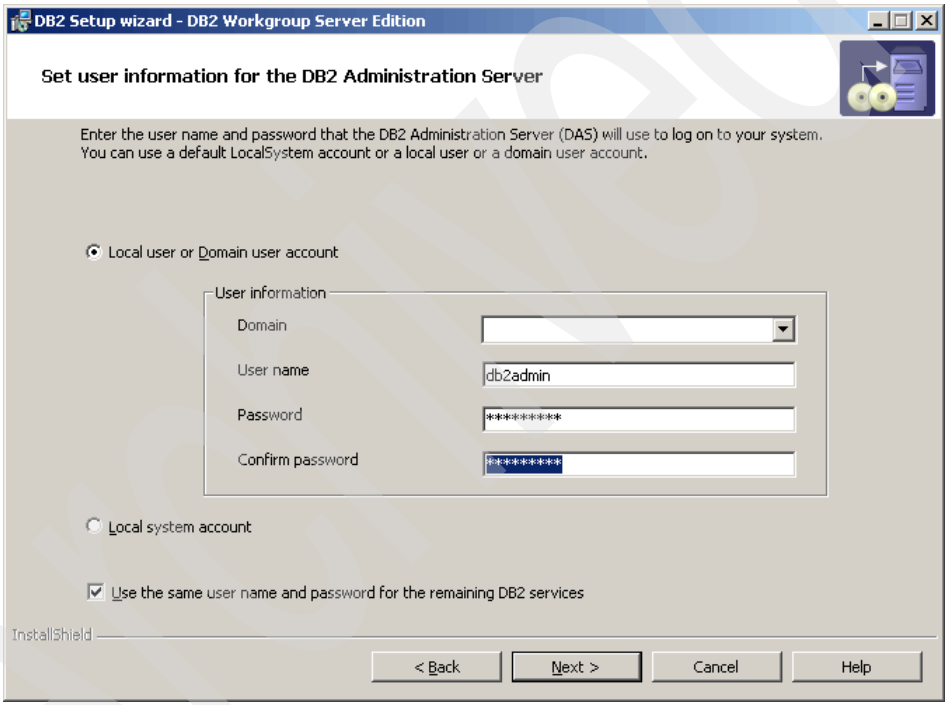

Figure 2-3 Set user information for the DB2 Administration Server

10. Click **Next** in Set up the administration contact list. We did not configure that for this installation.
11. Click **OK** in the Warning window.
12. Click **Next** in Configure DB2 instances.
13. In Prepare the DB2 tools catalog, select **Do not prepare the DB2 tools catalog on this computer** and click **Next**.

14. Select **Defer the task until after installation is complete** in Specify a contact for health monitor notification.

15. The last window shows the current settings. Click **Install** to start copying files as shown in Figure 2-4.

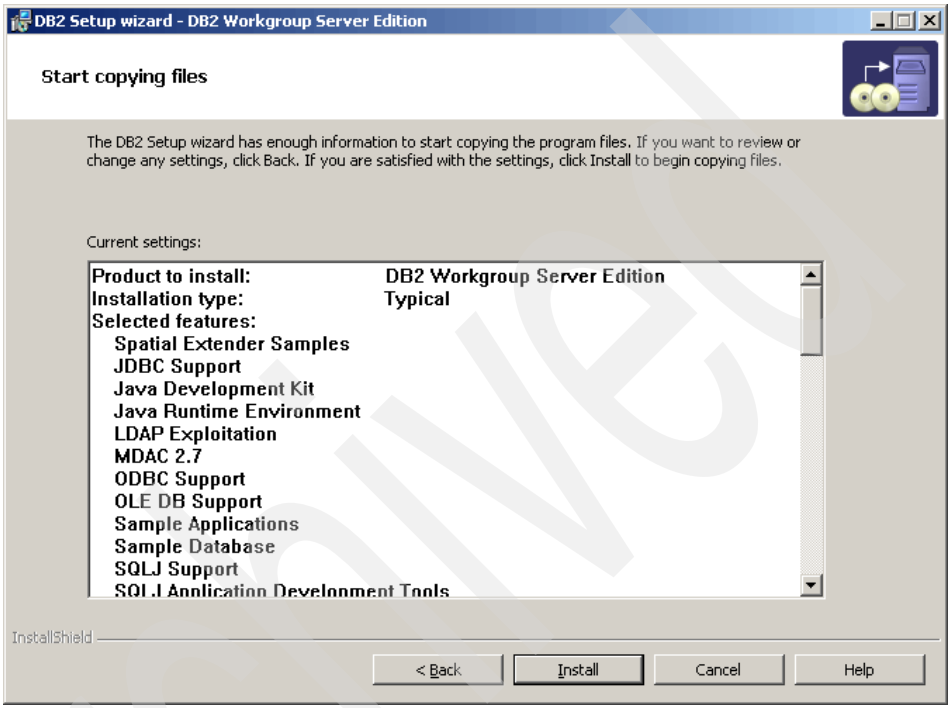

Figure 2-4 DB2 Setup wizard - Start copying files

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

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

2.1.2 Creating the Tivoli Datawarehouse database

In this section, we create the database for Tivoli Enterprise Portal Server.

First we should verify whether the database server is running by checking the DB2 services states: **Start** → **Setting** → **Control Panel** → **Administrative Tools** → **Services**.

These services started with DB2 should be running. (They are turned off by default as shown in Figure 2-5.)

- DB2 Governor Service
- DB2 License Server

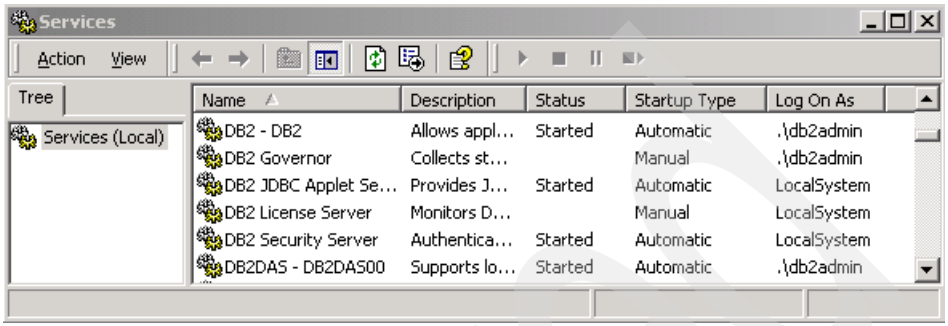

Figure 2-5 Services management console

Now we can create the database. Click **Start** → **Run,** type `db2cmd` in the Open box, and click **OK** to open a DB2 command line prompt.

To create the DB2 database, type the following command in DB2 CLP:

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

It takes some time to create the tdw21 database, and the following message shows the end of database creation:

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

2.1.3 Creating the database user

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

Use the following steps to create the user:

1. Click **Start** → **Settings** → **Control Panel** → **Administrative Tools** → **Computer Management,** expand **Local Users and Groups**, and click **Users**.

2. In the menu bar, click → **Action** → **New User** as shown in Figure 2-6.

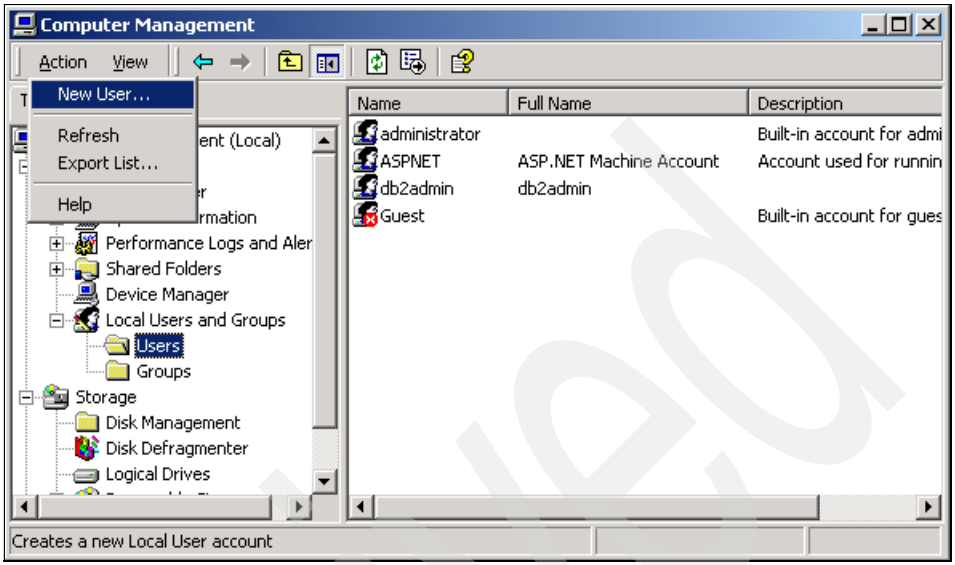

Figure 2-6 Computer Management, adding a New User

3. Enter the New User information as follows:

   User name itm61

   Password itm61dgrb

   Confirm Password itm61dgrb

4. Uncheck **User cannot change password** and check **Password never expires**.

5. Click **Create** and then **Close** as shown in Figure 2-7.

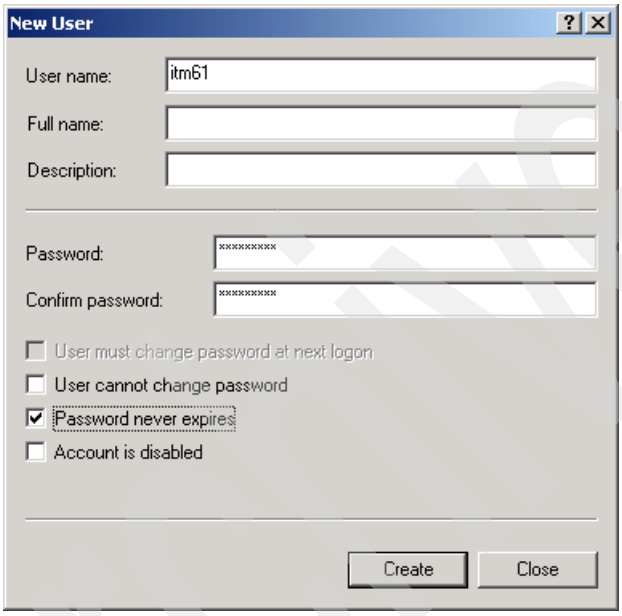

Figure 2-7 New User interface

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

1. In Computer Management, expand the **Local Users and Groups** then expand **Users**.

2. In the right plane, select the **itm61** user.

3. In the menu bar, click **Actions** → **Properties.**

4. Select the **Member Of** tab and click **Add** as shown in Figure 2-8.

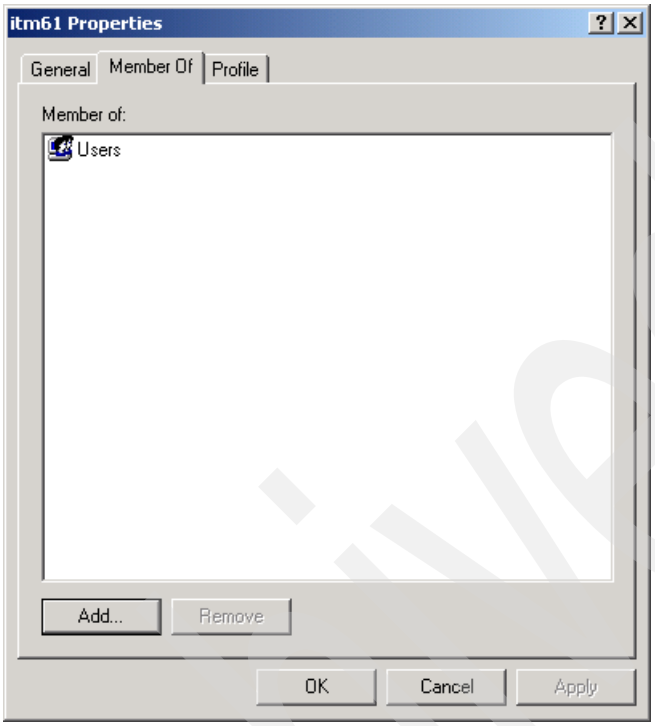

Figure 2-8 Adding Groups to itm61 user

5. Select **Administrators** in the top plane and click **Add**. The Administrators group goes to the bottom pane (Figure 2-9). Click **OK**, and **OK** again to close the itm61 Properties window, and close the Computer Management console.

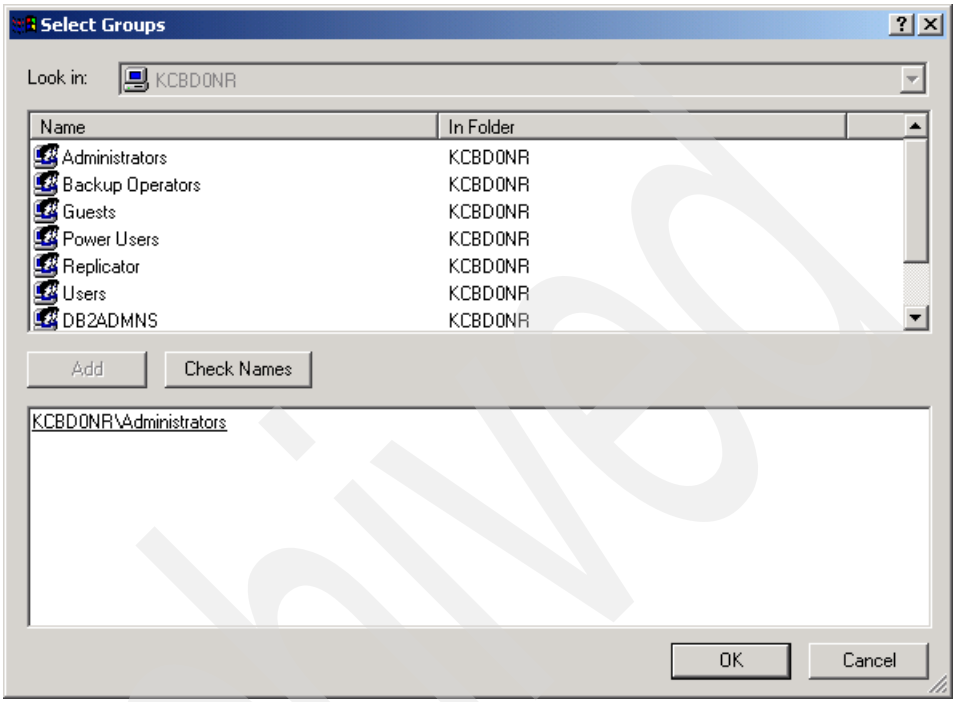

Figure 2-9 Adding Administrators group

2.1.4 Setting up ODBC connection for Tivoli Data Warehouse Proxy

To move data from Tivoli Enterprise Portal Server to Tivoli Data Warehouse, IBM Tivoli Monitoring 6.1 uses Warehouse Proxy agent. This agent uses an ODBC connection to transfer historical data collected from agents to a database.

To create this ODBC connection:

1. Click **Start** → **Settings** → **Control Panel** → **Administrative Tools** → **Data Sources (ODBC)**.
2. Select the **System DNS** tab and click **Add.**

3. Select **ODBC IBM DB2 DRIVER** and click **Finish** as shown in Figure 2-10.

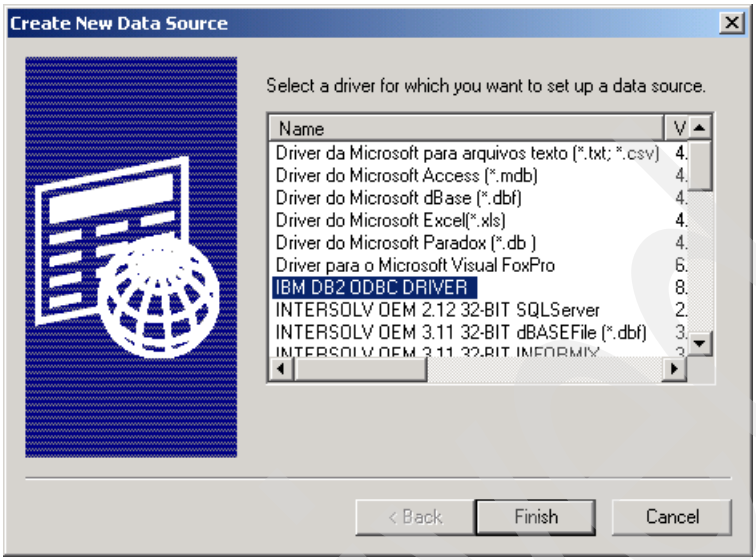

Figure 2-10 Create New Data Source

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

2.2 IBM Tivoli Monitoring 6.1 components installation

This section describes the installation process of several components: Tivoli Enterprise Monitoring Server, Tivoli Enterprise Portal Server, Tivoli Enterprise Monitoring Agents, and Tivoli Enterprise Portal.

2.2.1 Installing IBM Tivoli Monitoring 6.1

Follow these steps to install IBM Tivoli Monitoring 6.1:

1. Log on to the system with the Administrator account.
2. Access the IBM Tivoli Monitoring 6.1 installation image. In our case, it was under C:\ITM61_image\itm61_image.

> **Note:** You can also install IBM Tivoli Monitoring 6.1 from the CD image.

3. Open the **Windows** folder and launch **setup.exe**. This launches the IBM Tivoli Monitoring - InstallShield Wizard.
4. In the Welcome to IBM Tivoli Monitoring window (Figure 2-11), click **Next**.

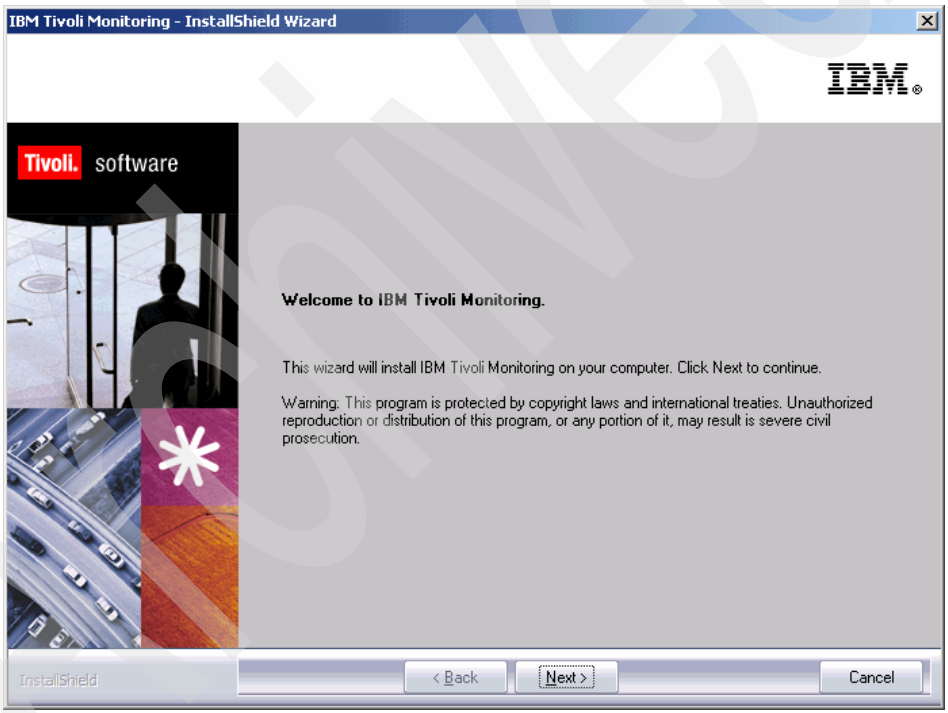

Figure 2-11 Welcome to IBM Tivoli Software

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

Figure 2-12 Software License Agreement

6. After accepting the License Agreement, the install shield wizard checks for a valid database installation and the existence of a specific version of JRE as shown in Figure 2-13. In our case, the JRE was installed as part of the installation process. Click **Next** to continue with the installation process.

> **Note:** If you have the correct JRE installed and a valid database installation, the Figure 2-13 will not appear.

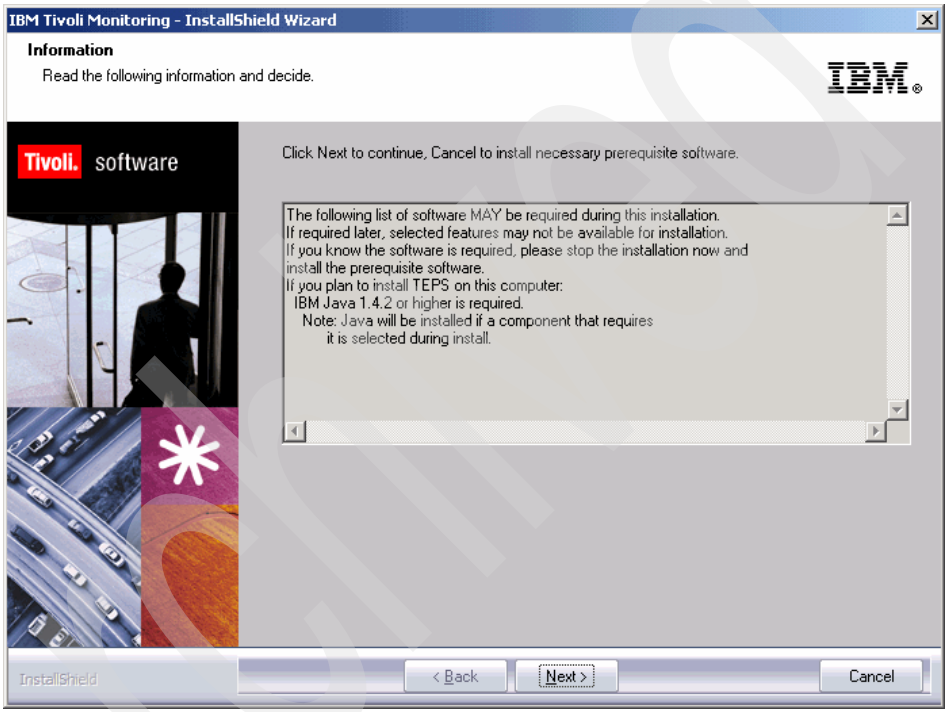

Figure 2-13 Checking necessary prerequisite software

7. In Choose Destination Location (Figure 2-14), accept the default directory by selecting **Next**.

Figure 2-14 Choose Destination Location

8. Now we have to set up an SSL encryption key. Click **Next** to leave the default key `IBMTivoliMonitoringEncryptionKey` as shown in Figure 2-15.

Figure 2-15 User Data Encryption Key

9. Click **OK** in Encryption Key as shown in Figure 2-16.

Figure 2-16 Encryption Key

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

10. In the window shown in Figure 2-17, we select the components that we want to install.

Figure 2-17 Selecting IBM Tivoli Monitoring 6.1 components

11. Click the plus (+) sign to expand **Tivoli Enterprise Monitoring Agents**, and select **Warehouse Proxy** and **Summarization and Pruning Agent** as shown in Figure 2-18. *Do not* click **Next** yet.

> **Important:** Do not check the box next to Tivoli Monitoring Agents because this would install *all* available agents. Tivoli Enterprise Monitoring Agent Framework was included when we selected the other agents.

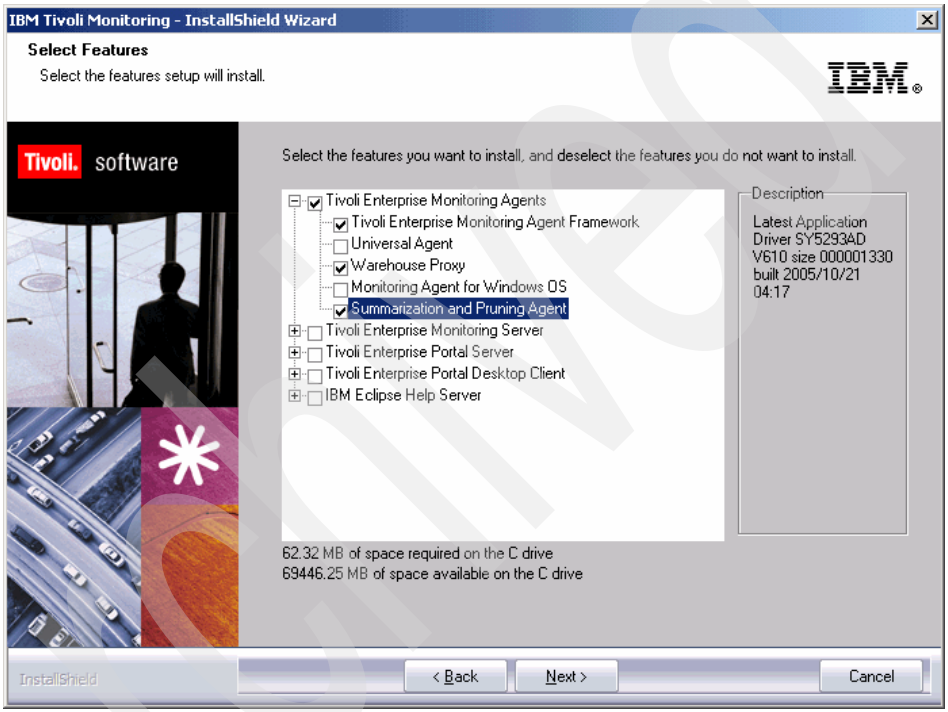

Figure 2-18 Selecting Tivoli Enterprise Monitoring Agents

12. Put a check box mark in **Tivoli Enterprise Monitoring Server**, **Tivoli Enterprise Portal Server**, and **Tivoli Enterprise Portal Desktop Client**, as shown in Figure 2-19.

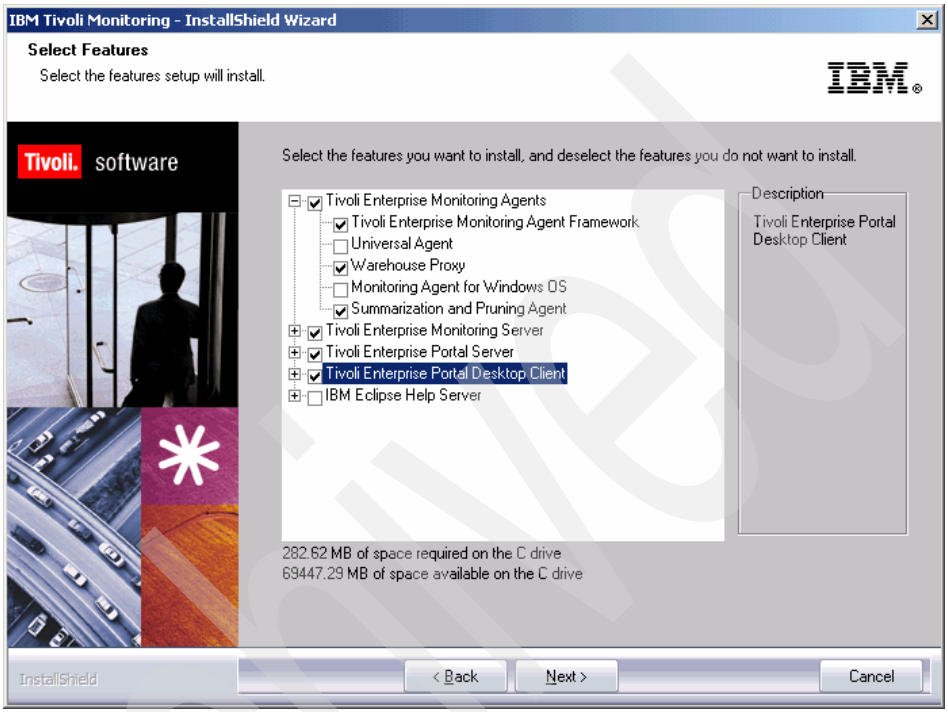

Figure 2-19 Selecting other IBM Tivoli Monitoring Components.

Note: Selecting the entire component as we did installs support for all different agents, thus enabling the Tivoli Enterprise Monitoring Server to work with data from several kinds of agents.

13. Select **Next** to continue.

14. In Agent Deployment, select **Universal Agent** and **Monitoring Agent for Windows OS** (Figure 2-20) and click **Next** to allow these agents to be deployed to a remote location.

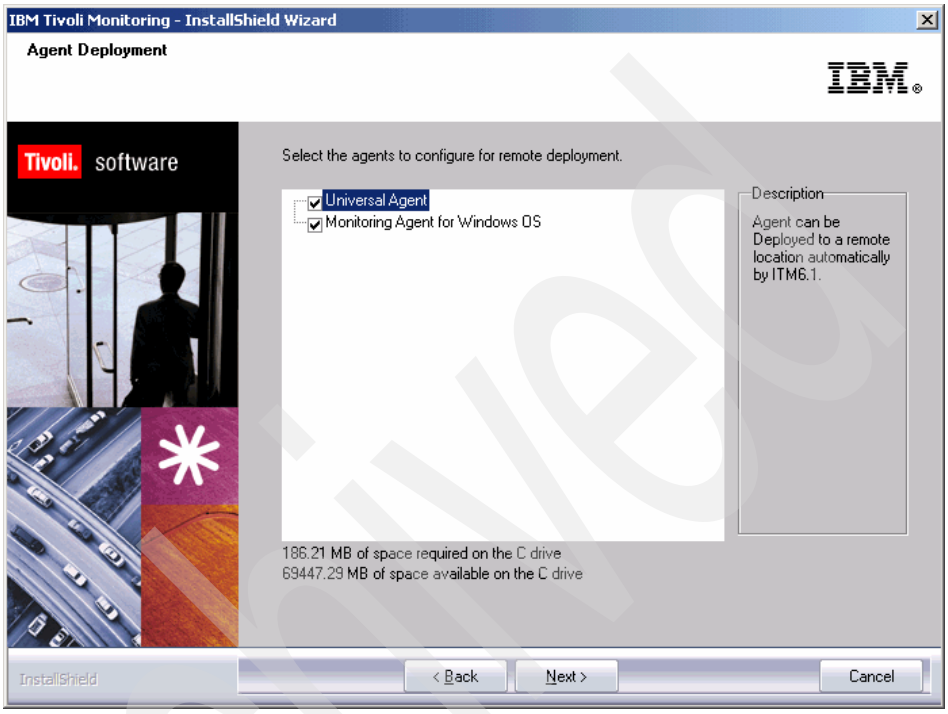

Figure 2-20 Agent Deployment

15. Click **Next** In Select Program Folder.

16. The next window (Figure 2-21) shows the Current Settings. Click **Next** to start copying files. The IBM Tivoli Monitoring - InstallShieldWizard installs the IBM Java2 Runtime Environment 1.4.2 and starts to copy files.

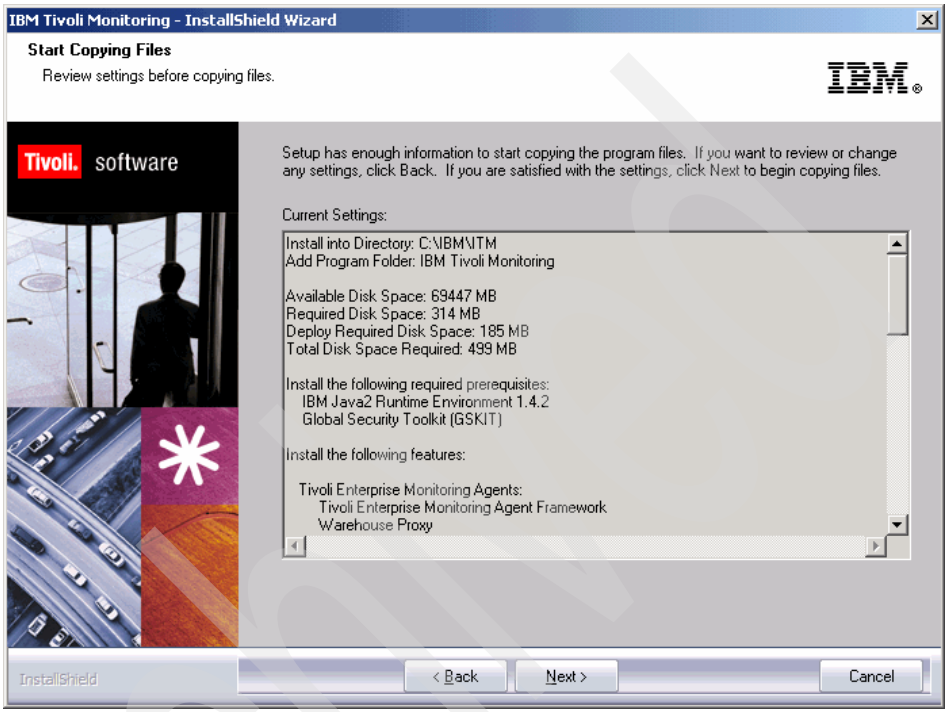

Figure 2-21 Start Copying Files

17. The Setup Type window appears (Figure 2-22) when the copy files have finished. Keep all check boxes selected and click **Next** to begin configuring the IBM Tivoli Monitoring components.

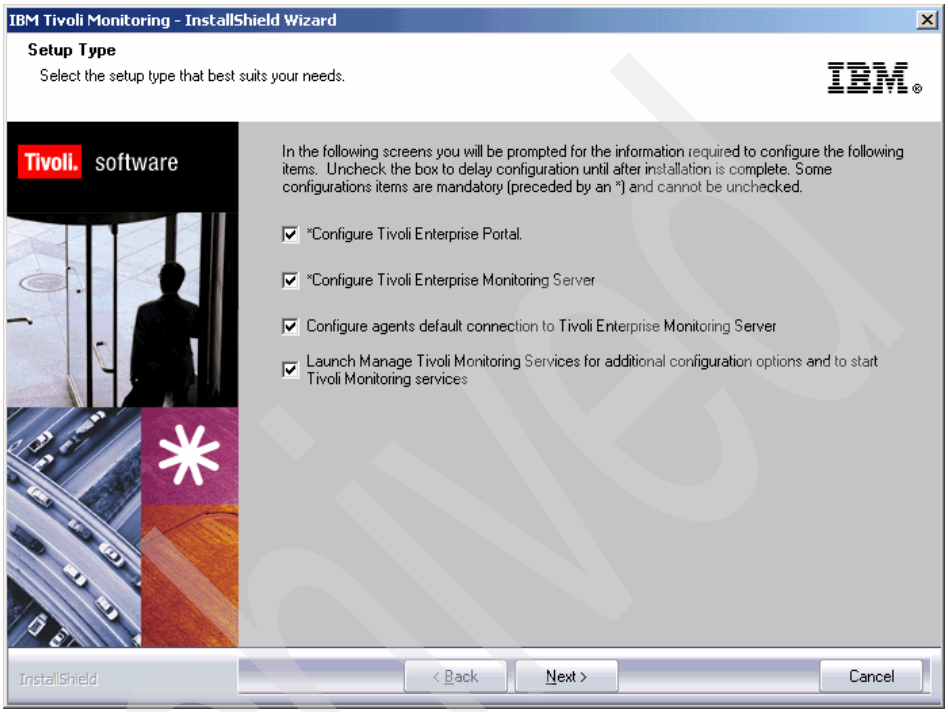

Figure 2-22 Setup Type

18. Click **Next** in Define TEP Host Information (Figure 2-23) to accept the detected host name.

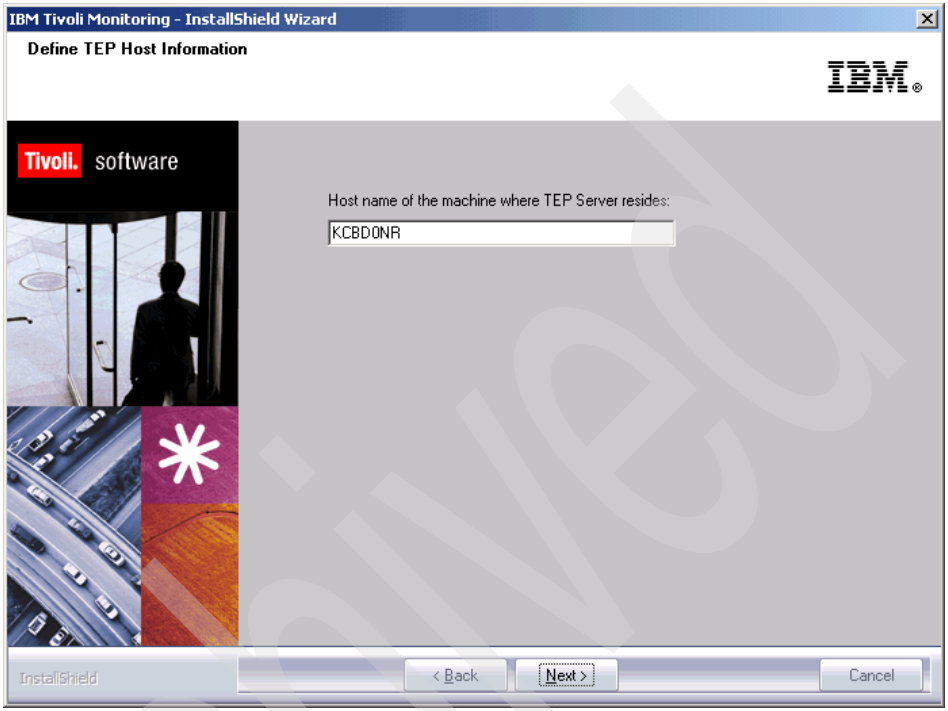

Figure 2-23 Define TEP Host Information

19. In the TEPS Data Source Config Parameters - DB2 window (Figure 2-24), enter:

Admin User ID	db2admin
Admin Password	itm61dgrb
Database User ID	TEPS
Database Password	itm61dgrb
Reenter Password	itm61dgrb

Click **OK**.

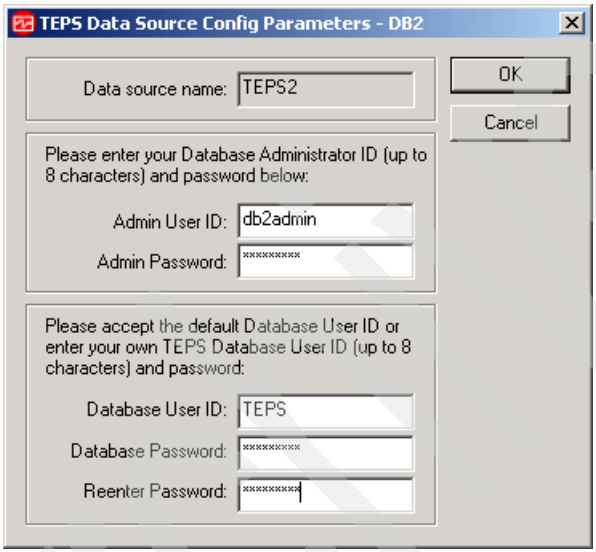

Figure 2-24 TEPS Data Source Config Parameters - DB2

20. Click **OK** (Figure 2-24) and **OK** to finish Tivoli Enterprise Portal Server configuration.

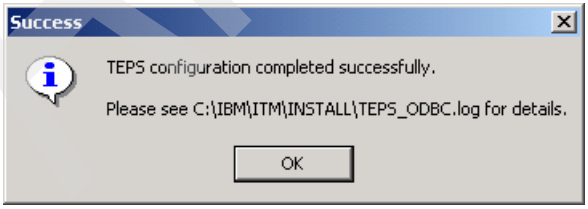

Figure 2-25 TEPS configuration completes successfully

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

21. In Warehouse ID and Password for TEP Server (Figure 2-26), we configure the credentials for the Tivoli Data Warehouse database. Type the user created in ODBC connection in page 2.1.4, “Setting up ODBC connection for Tivoli Data Warehouse Proxy” on page 51, as follows:

    ID itm61

    Password itm61dgrb

    Confirm Password itm61dgrb

    Click **Next**.

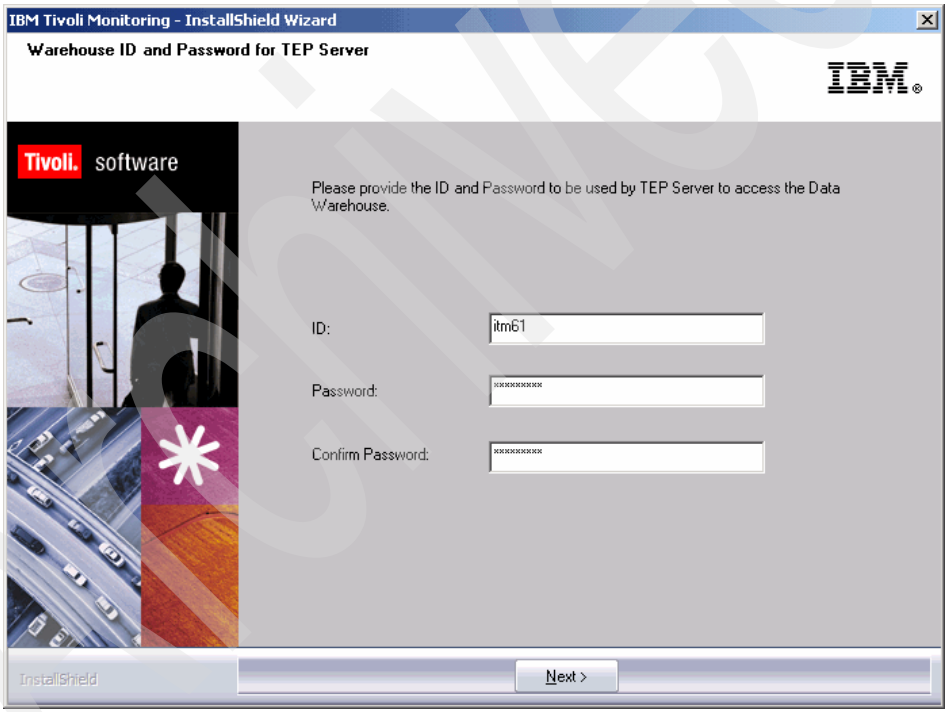

Figure 2-26 Warehouse ID and Password for TEP Server

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

> **Note:** You can specify whether you want to go through a firewall and specify the communications parameters:
>
> - **IP.PIPE** uses unsecured TCP communications.
> - **IP.SPIPE** uses SSL secure TCP communications.
> - **SNA** uses SNA for mainframe environments.
> - **IP.UDP** uses unsecured UDP communications.

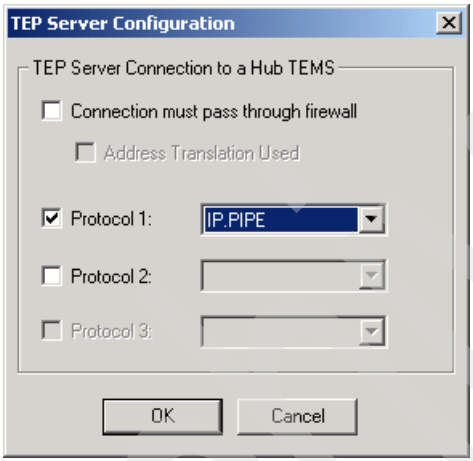

Figure 2-27 TEP Server Configuration

23. Click **OK** to accept the default settings of Tivoli Enterprise Monitoring Server as shown in Figure 2-28.

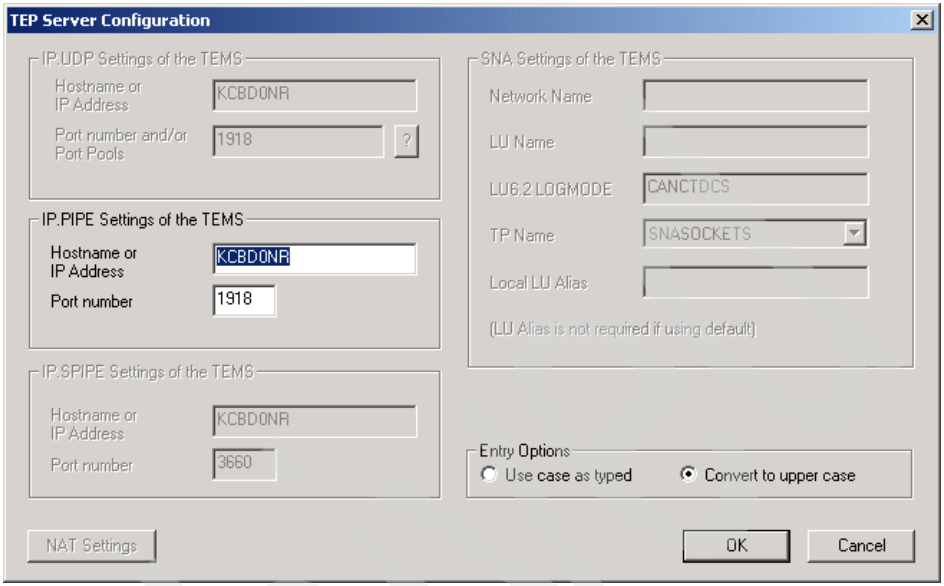

Figure 2-28 TEP Server Configuration

24. Click **Yes** when asked whether to reconfigure the warehouse connection information for the Tivoli Enterprise Portal Server as shown in Figure 2-29.

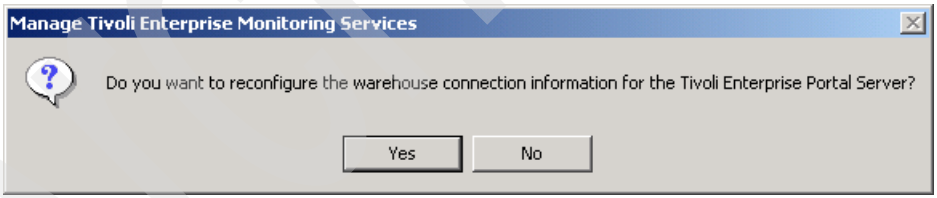

Figure 2-29 Reconfigure warehouse connection information

25. Select **DB2** in Configure DB2 Data Source for Warehouse Proxy as shown in Figure 2-30.

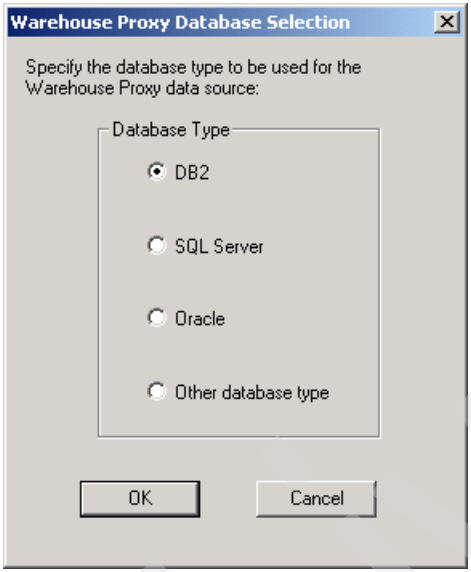

Figure 2-30 Warehouse Proxy Database Selection

26. Enter this information in Configure DB2 Data Source for Warehouse Proxy (Figure 2-31):

Data Source Name	ITM Warehouse
Database Name	tdw21
Admin User ID	db2admin
Admin Password	itm61dgrb
Database User ID	itm61
Database Password	itm61dgrb
Reenter Password	itm61dgrb

Click **OK**.

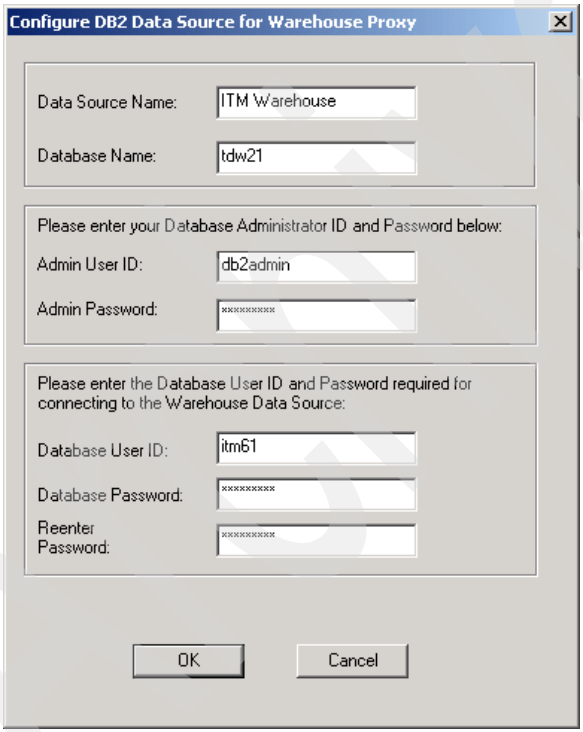

Figure 2-31 Configure DB2 Data Source for Warehouse Proxy

27. Click **OK** to finish the warehouse data source configuration as shown in Figure 2-32.

Figure 2-32 Manage Tivoli Enterprise Monitoring Services

28. After some time the IBM Tivoli Monitoring builds the Tivoli Enterprise Portal presentation files as shown in Figure 2-33.

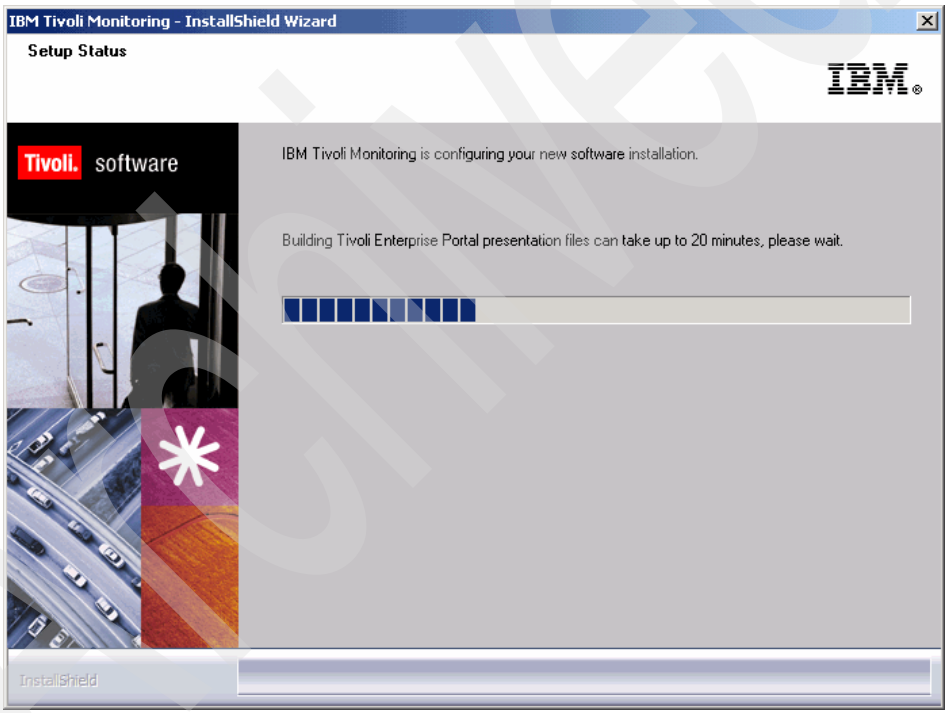

Figure 2-33 Tivoli Enterprise Portal presentation files

29. In the next window (Figure 2-34), we configure the Tivoli Enterprise Monitoring Server: Select the TEMS Type **Hub**, check the **TEMS Name**, check the protocol (for this TEMS, **Protocol 1** and **IP.PIPE**). Click **OK**.

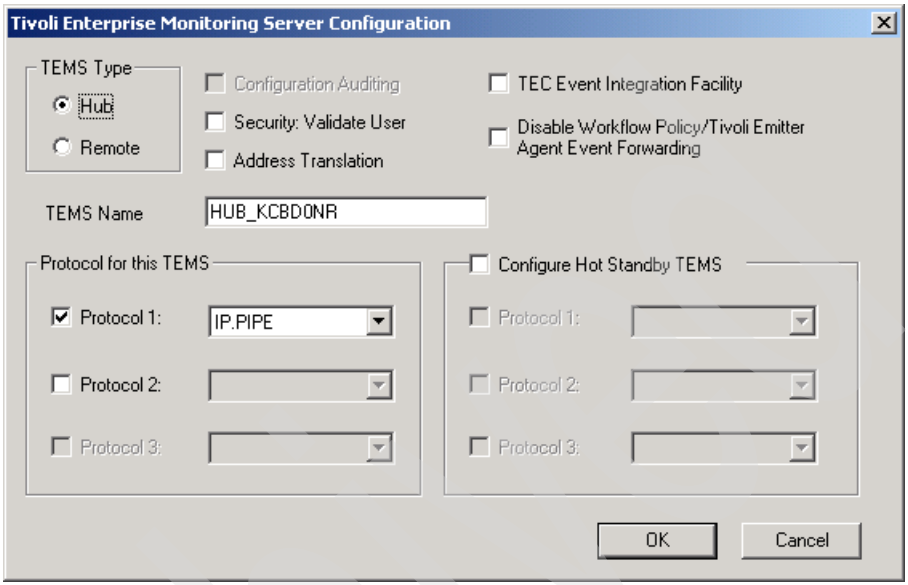

Figure 2-34 Tivoli Enterprise Monitoring Server Configuration

30. In Hub TEMS Configuration, click **OK** to accept the default configuration for IP.PIPE Settings: Hub as shown in Figure 2-35.

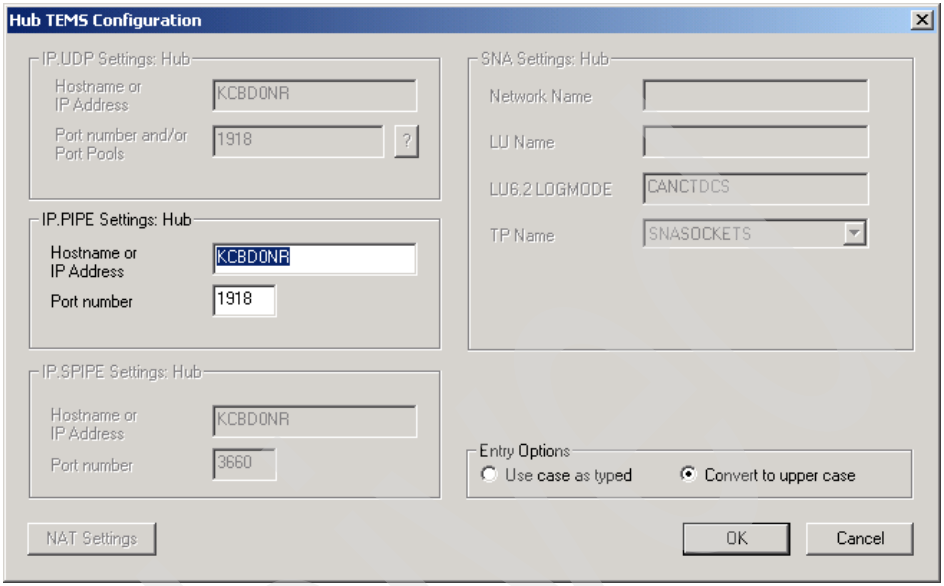

Figure 2-35 Hub TEMS Configuration

31. In the next step we add application support to the monitoring server, such as the workspaces and situations for agents. Select the TEMS Location as **On this computer** and click **OK** as shown in Figure 2-36.

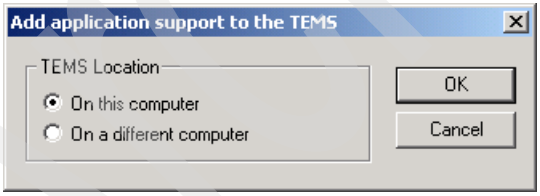

Figure 2-36 TEMS Location

32. Because the monitoring server is not running currently, it is started automatically before the process begins. Click **OK** to start it and perform the application support operation as shown in Figure 2-37.

Figure 2-37 Manage Tivoli Enterprise Monitoring Services

33. In Figure 2-38. select the data that you want to add to the monitoring server. Verify that all available application support is selected and click **OK**.

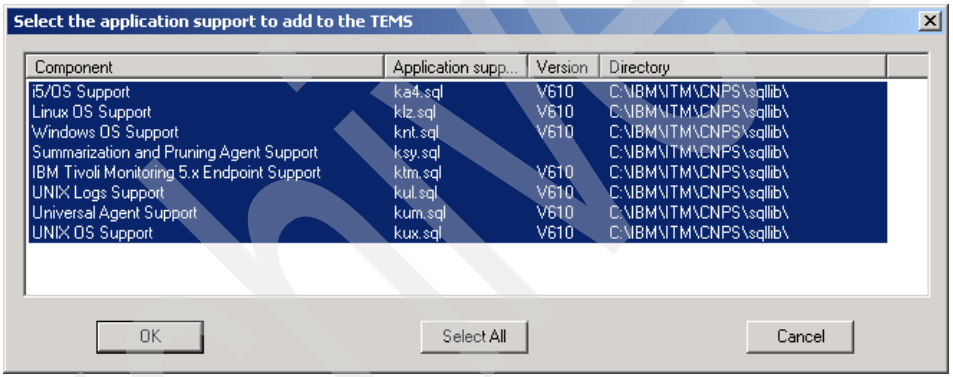

Figure 2-38 Select the application support to add to the TEMS

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

35. Configure the communication between any IBM Tivoli Monitoring component and the hub monitoring server: Verify that **Protocol 1** is selected and configured as **IP.PIPE**, and click **OK** as shown in Figure 2-39.

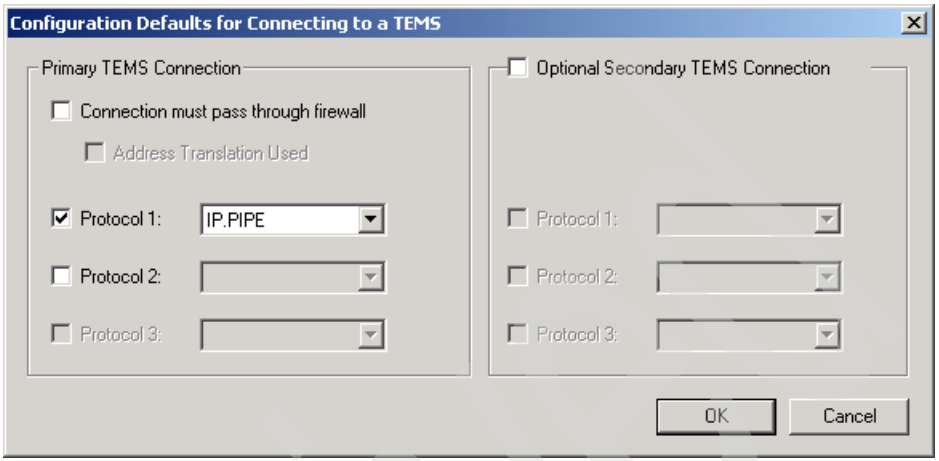

Figure 2-39 Configuration Defaults for Connecting to a TEMS

36. After a while, the IBM Tivoli Monitor - InstallShield Wizard prompts a window informing that services are being recycled, and the final completion screen pops up as shown Figure 2-40. Click **Finish** to end IBM Tivoli Monitoring 6.1 component installation.

Figure 2-40 InstallShield Wizard Complete

37. Two text files open: IBM Tivoli Monitoring Readme.txt and Post_Install_Info.txt. The most important thing to note is the warning about Java 2 v1.4.2, as shown in Example 2-1.

Example 2-1 Readme.txt

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

38. Finally, the Manage Tivoli Enterprise Monitoring Services - TEMS Mode - [Local Computer] opens as shown in Figure 2-41.

    In this console, you can:

    – See the services status
    – Recycle the services
    – Reconfigure the services
    – Launch Tivoli Enterprise Portal

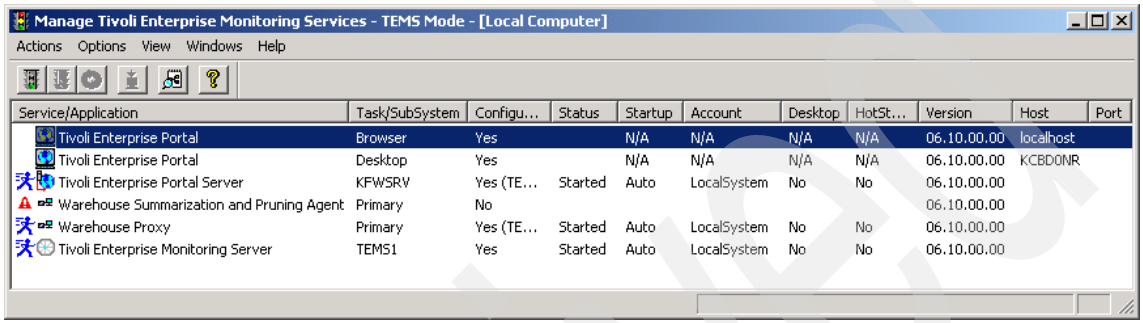

Figure 2-41 Manage Tivoli Enterprise Monitoring Services

> **Note:** Warehouse Summarization and Pruning Agent is not configured. See 2.2.3, “Configuring Warehouse Summarization and Pruning Agent” on page 81.

2.2.2 Launching Tivoli Enterprise Portal

To verify that the installation is running fine, use Tivoli Enterprise Portal Client, which you can launch Tivoli as either a desktop or Web-based application.

Launching Tivoli Enterprise Portal from Internet Explorer

To launch Tivoli Enterprise Portal using a browser:

1. Click **Start** → **Programs** → **Internet Explorer.**
2. Type `http://kcbd0nr:1920/client/client`

3. Click **Yes** to accept the Warning - Security message as shown in Figure 2-42.

Figure 2-42 The security certificate message

4. For the Logon window (Figure 2-43) User Credentials, enter `sysadmin` for the logon ID and leave the password blank. Click **OK**.

> **Note:** We do not have to enter the password because we do not have security enabled.

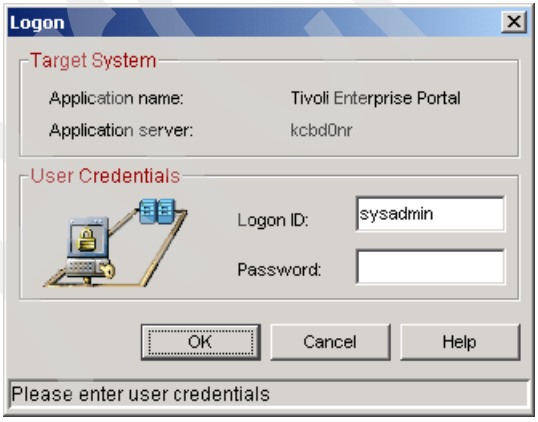

Figure 2-43 Logon window

5. In the Security Alert window (Figure 2-44), click **Always Accept** to accept the certificate.

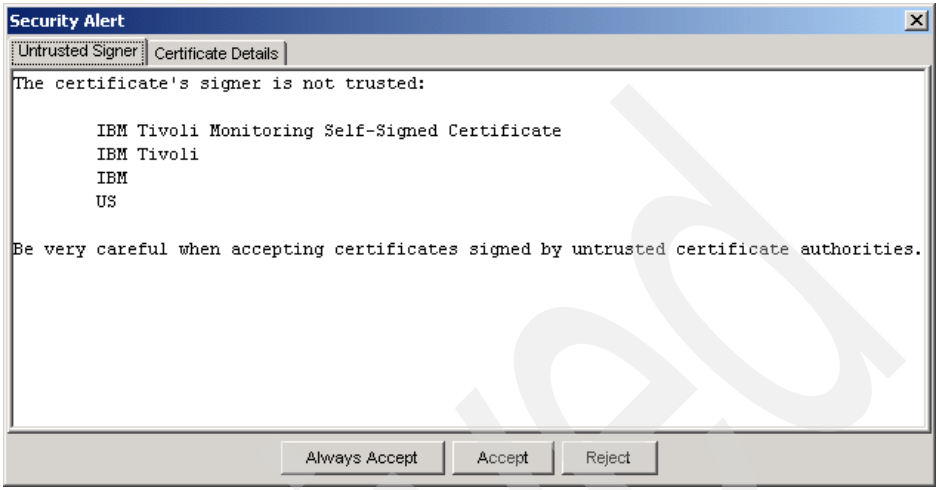

Figure 2-44 Security Alert

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

6. Click **Exit** to close the Welcome to IBM Tivoli Monitoring window, and select **File** → **Exit** and **Yes** to close Tivoli Enterprise Portal. You can also close Internet Explorer.

Launching Tivoli Enterprise Portal Client desktop application

When we install Tivoli Enterprise Portal Client, it creates a menu item and a desktop icon. We can launch Tivoli Enterprise Portal Client (Figure 2-45) by launching its icon or using **Start** → **Programs** → **IBM Tivoli Monitoring** → **Tivoli Enterprise Portal**.

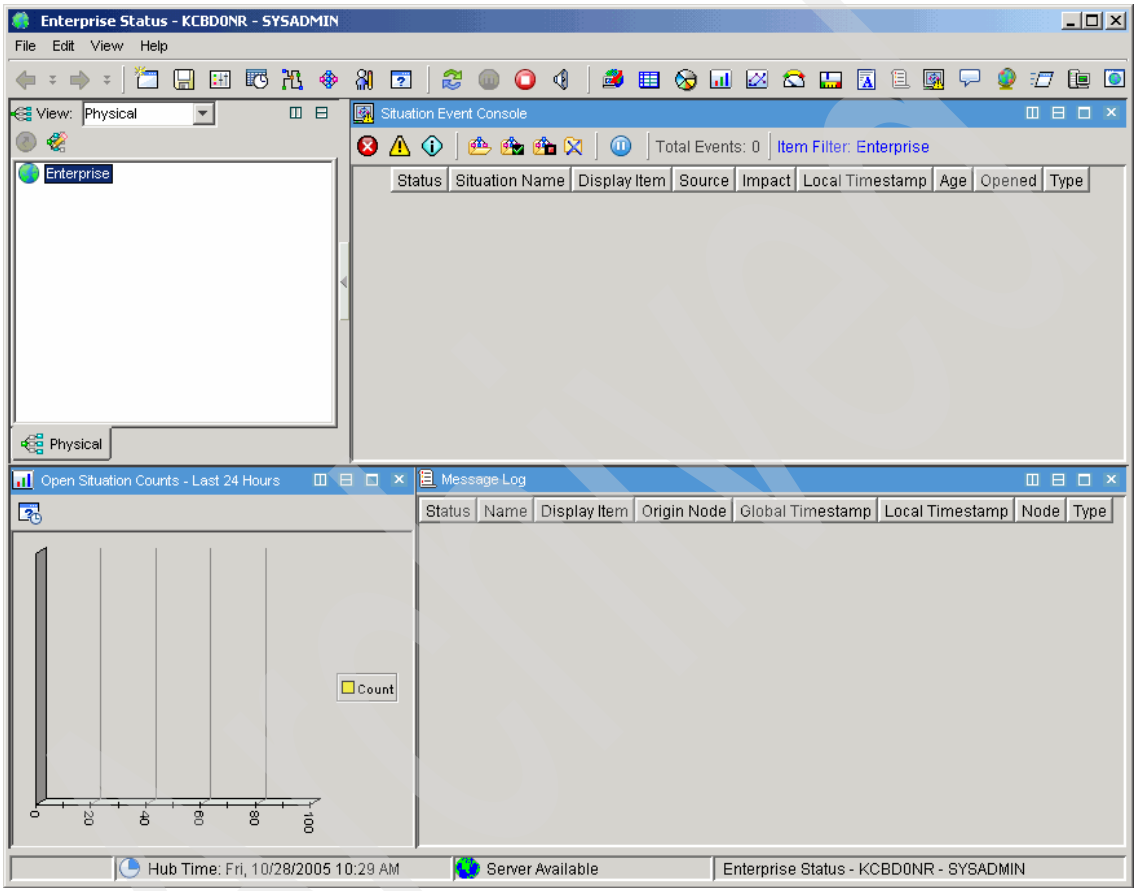

Figure 2-45 Tivoli Enterprise Portal Client Desktop

Note: Before you run the client version, you need to install its application from the IBM Tivoli Monitoring 6.1 image. In the browser version, we just need to have network access and a Web browser such as Internet Explorer.

2.2.3 Configuring Warehouse Summarization and Pruning Agent

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

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

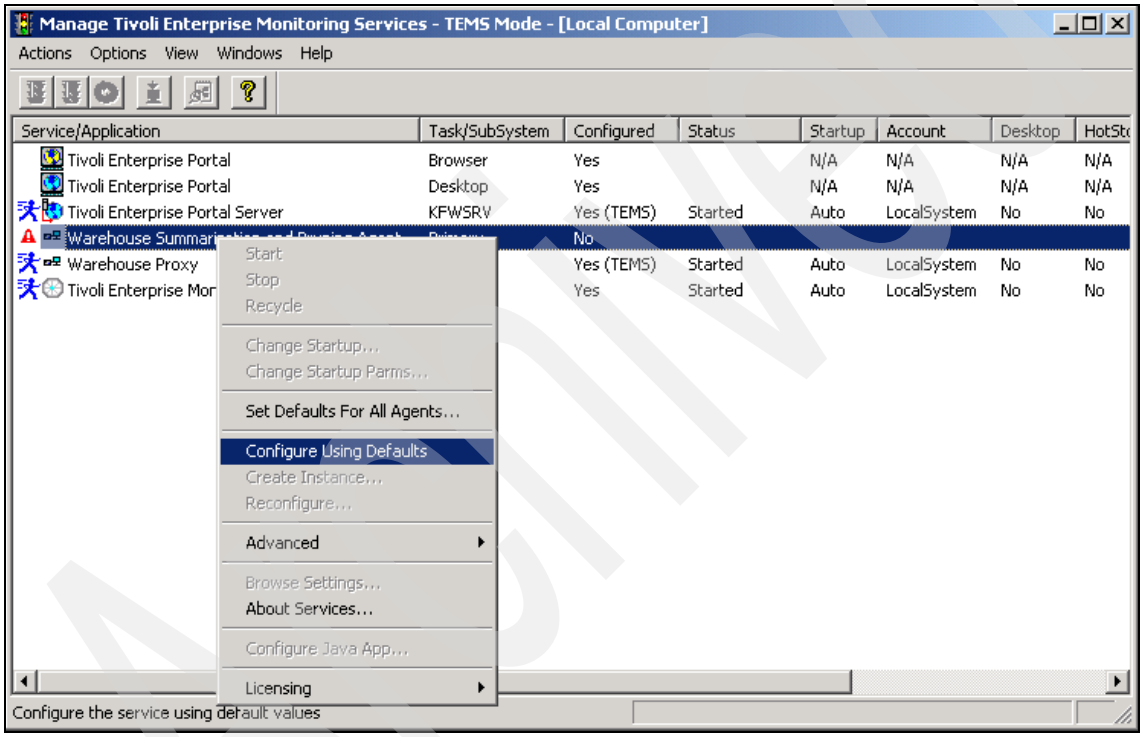

Figure 2-46 Warehouse Summarization and Pruning Agent configuration

3. Click **Yes** in the Would you like to configure this Summarization and Pruning Agent window.
4. In the Source tab of Configure Summarization and Pruning Agent Java application, you can leave the database settings as is.
5. Click the **Defaults** tab and select **Apply settings to default tables for all agents** check box.

6. Click the **Scheduling** tab, where you can specify how often and when the agent runs. Leave it as is.
7. Click **Work Days**. Here you can differ the working hours and non-working hours, and include vacation settings. Leave it as is.
8. Click the last tab, **Additional Parameters**, which you can use to configure other database parameters. You can leave it as is.
9. Click **Save** and **Close**.
10. Now, start Warehouse Summarization and Pruning Agent. Right-click **Warehouse Summarization and Pruning Agent.** Select **Start** (Figure 2-47).

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

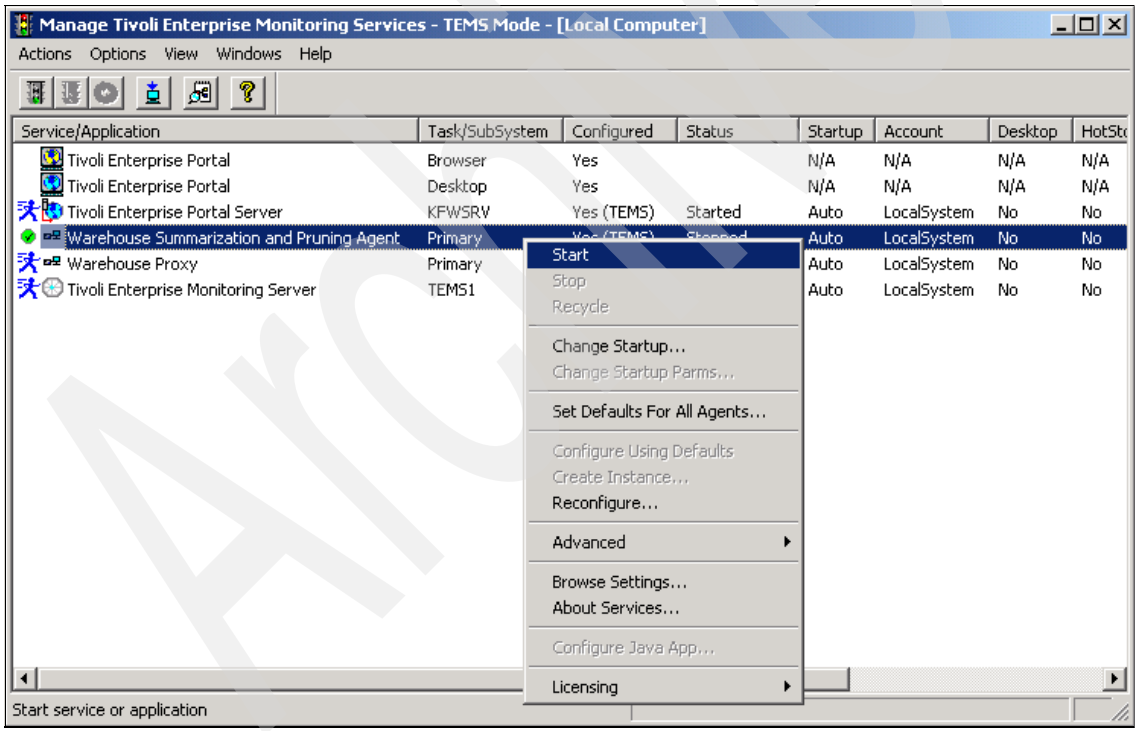

Figure 2-47 Starting Warehouse Summarization and Pruning Agent

This completes Warehouse Summarization and Pruning configuration. Next, we configure what components log data to Tivoli Data Warehouse.

2.2.4 Installing IBM Tivoli Monitoring Agents

Follow these steps to install IBM Tivoli Monitoring 6.1:

1. Log on to the system with the Administrator account.
2. Access the IBM Tivoli Monitoring 6.1 installation image. In our case, it was under C:\ITM61_image\itm61_image.
3. Open the **Windows** folder and launch **setup.exe**. This launches the IBM Tivoli Monitoring - InstallShield Wizard.
4. In the Welcome window (Figure 2-48), select **Modify** and click **Next**.

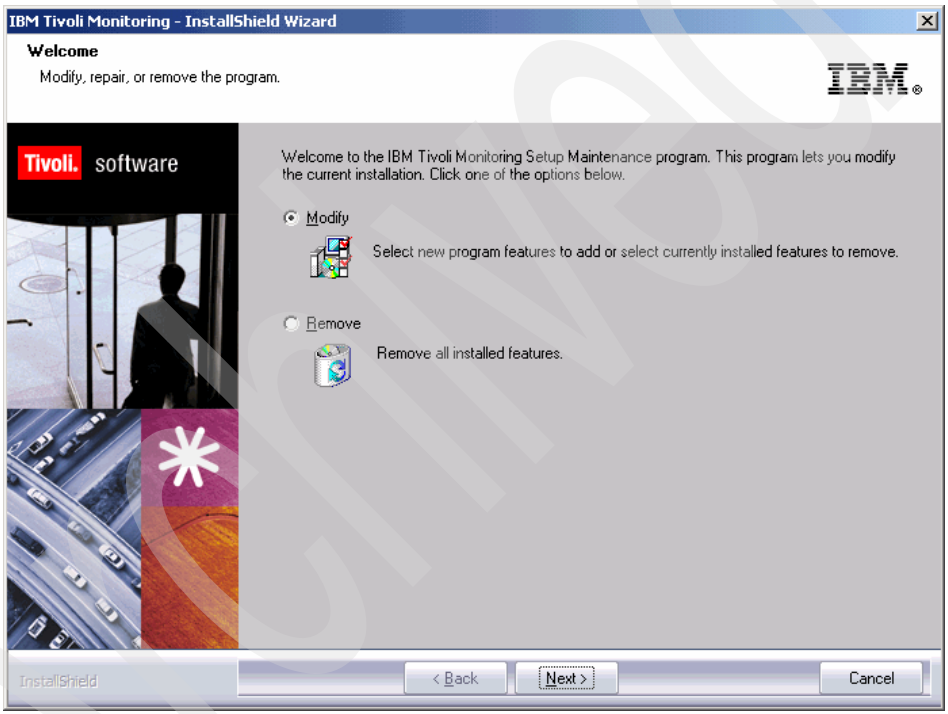

Figure 2-48 Welcome - Modify, repair, or remove program

5. Click **OK** in the information window shown in Figure 2-49.

Figure 2-49 Information window

6. Expand **Tivoli Enterprise Monitoring Agents** and check **Monitoring Agent for Windows OS** as shown in Figure 2-50.

Attention: Do not deselect anything that we installed so far. Deselecting any item uninstalls it.

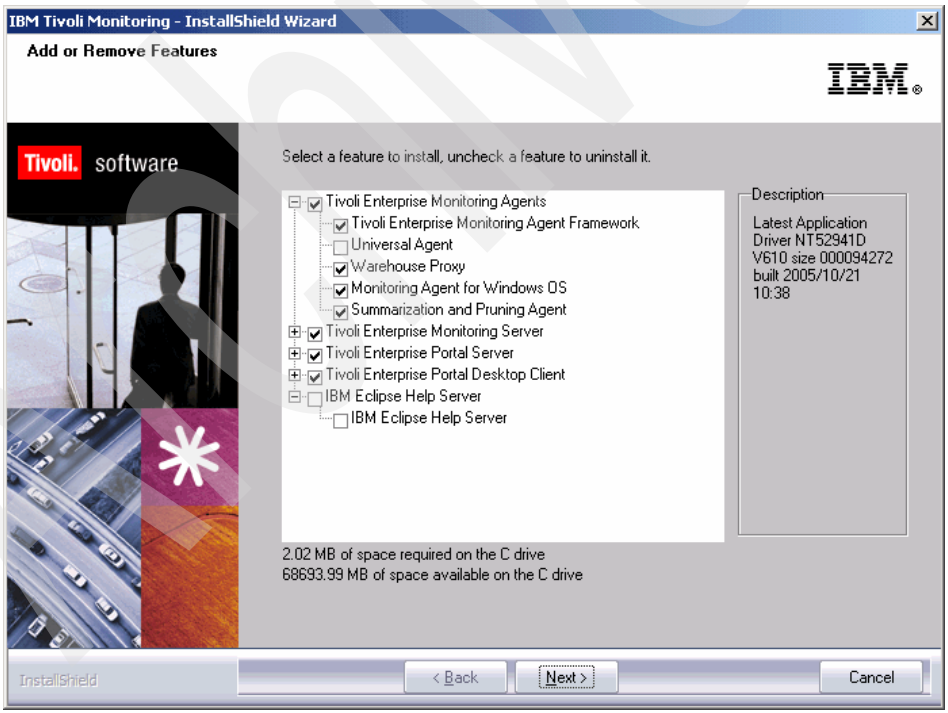

Figure 2-50 Selecting Monitoring Agent for Windows OS

7. Because Tivoli Enterprise Monitoring Server is installed on that computer, this next step (Figure 2-51) is to deploy. Leave **Universal Agent** and **Monitoring Agent for Windows OS** selected and click **Next**.

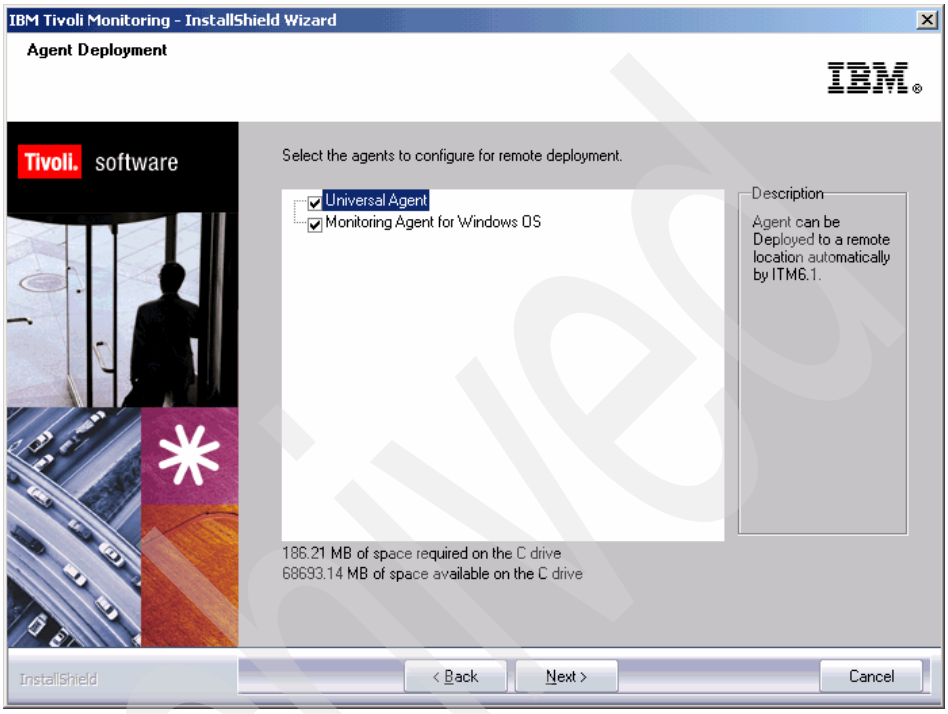

Figure 2-51 Selecting the Agents to deploy

8. Select **Next** in Start Copying Files.

9. Under Setup Type, we select only **Configure agents default connect to Tivoli Enterprise Monitoring Server**. Click **Next** as shown in Figure 2-52.

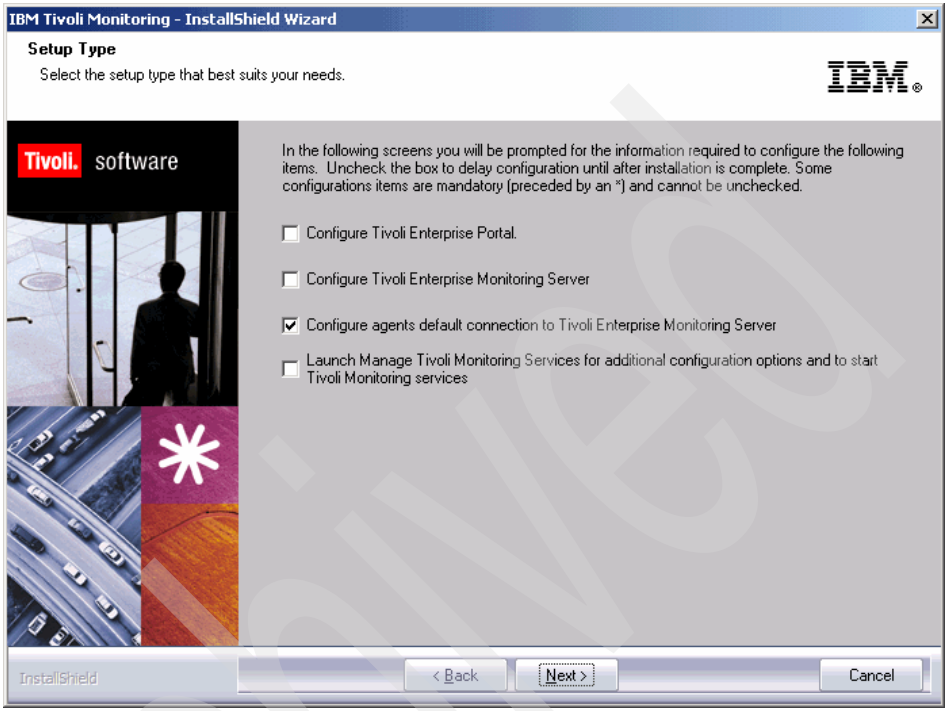

Figure 2-52 Configure agents' default connection to TEMS

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

Having finished Tivoli Monitoring Agent installation, we start Manage Tivoli Enterprise Monitoring Services to see its service status. Click **Start** → **Programs** → **IBM Tivoli Monitoring Manage** → **Tivoli Monitoring Services**. As shown in Figure 2-53 on page 87, Monitoring Agent for Windows is installed and started.

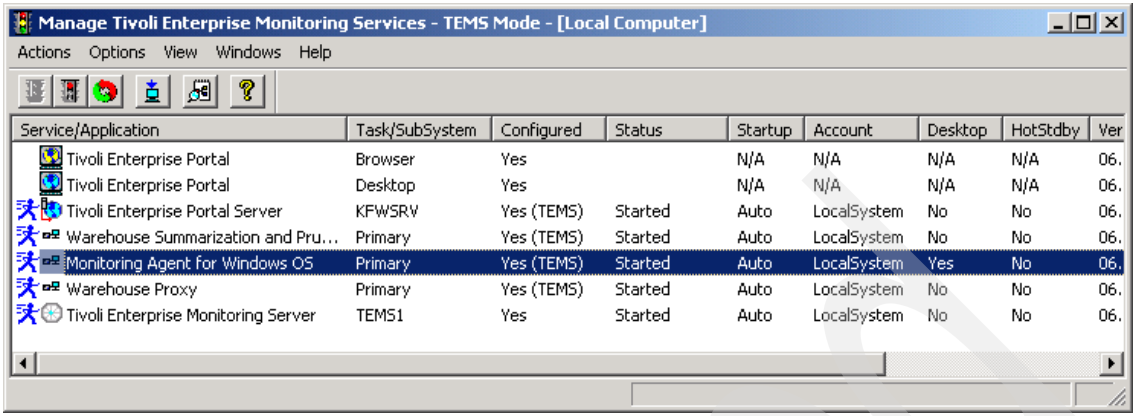

Figure 2-53 Monitoring Agent for Windows OS status

We can also launch (2.2.2, “Launching Tivoli Enterprise Portal” on page 77) Tivoli Enterprise Portal Client to see this Windows OS agent installed. You can navigate through the workspace to see that monitoring is already working.

3

Medium and large environment installation installation

In this chapter, we discuss detailed steps and best practices to implement IBM Tivoli Monitoring 6.1 using two different scenarios: Windows TEMS and UNIX TEMS. We offer best practices guidelines in terms of machine sizing and configurations.

This chapter discusses the following topics:

- Lab environment
- Installing IBM Tivoli Monitoring 6.1
- Uninstalling IBM Tivoli Monitoring 6.1

3.1 Lab environment

The following section describes the software and hardware components used during the implementation of IBM Tivoli Monitoring 6.1 in our lab environment. It also outlines the architecture used to build that environment.

To simulate real-time environments as much as possible, we set up two different scenarios: Windows-based TEMS and UNIX-based TEMS.

- 3.2.5, “Installing and configuring the scenario 1 environment” on page 102 covers a typical IBM Tivoli Monitoring 6.1 implementation with two Windows TEMS servers with second server used for Hot Standby.
- 3.2.16, “Installing and configuring the scenario 2 environment” on page 203 discusses an implementation with two UNIX TEMS servers, with a second server again used for Hot Standby.

Apart from the TEMS servers, all IBM Tivoli Monitoring 6.1 components remain the same in both scenarios. You can use one of these scenarios depending on the TEMS platform of your choice.

If you install your TEMS server on one platform (such as Windows), then decide to migrate it to another platform (such as UNIX), you can follow the instructions given in 3.2.17, “Replacing a Hub TEMS server with a new one” on page 210.

Notes:

- Both of these configurations can be achieved with one TEMS server instead of two, if you do not plan to use the Hot Standby functionality. For fault tolerance reasons, we recommend that you use the Hot Standby function.
- It is also possible to use one Windows and one UNIX TEMS server, as Hot Standby functionality also works between Windows and UNIX servers. We tested this scenario successfully for this book.

3.1.1 Hardware and software configuration

Table 3-1 shows the hardware and software configuration of our lab environment.

Table 3-1 Lab hardware and software configuration

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

3.1.2 Lab architecture

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

Lab architecture of scenario 1

Figure 3-1 shows the first scenario with two Windows Hub TEMS servers and two Remote TEMS servers, one UNIX server, and one Windows server™.

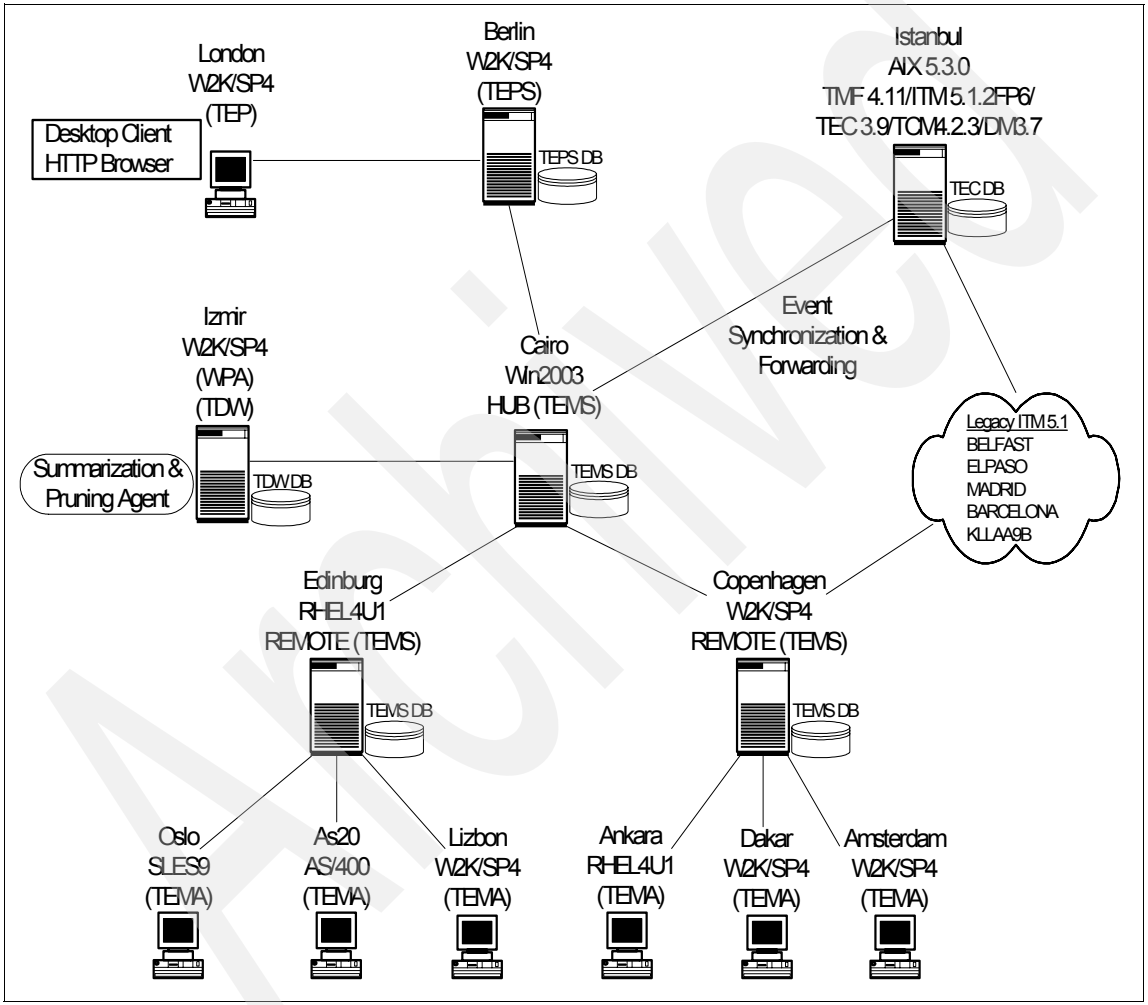

Figure 3-1 Lab architecture or a large-scale enterprise, scenario 1

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

Lab architecture scenario 2

Figure 3-2 shows the second scenario with two AIX Hub TEMS servers and the same configuration for the rest of the components as scenario 1.

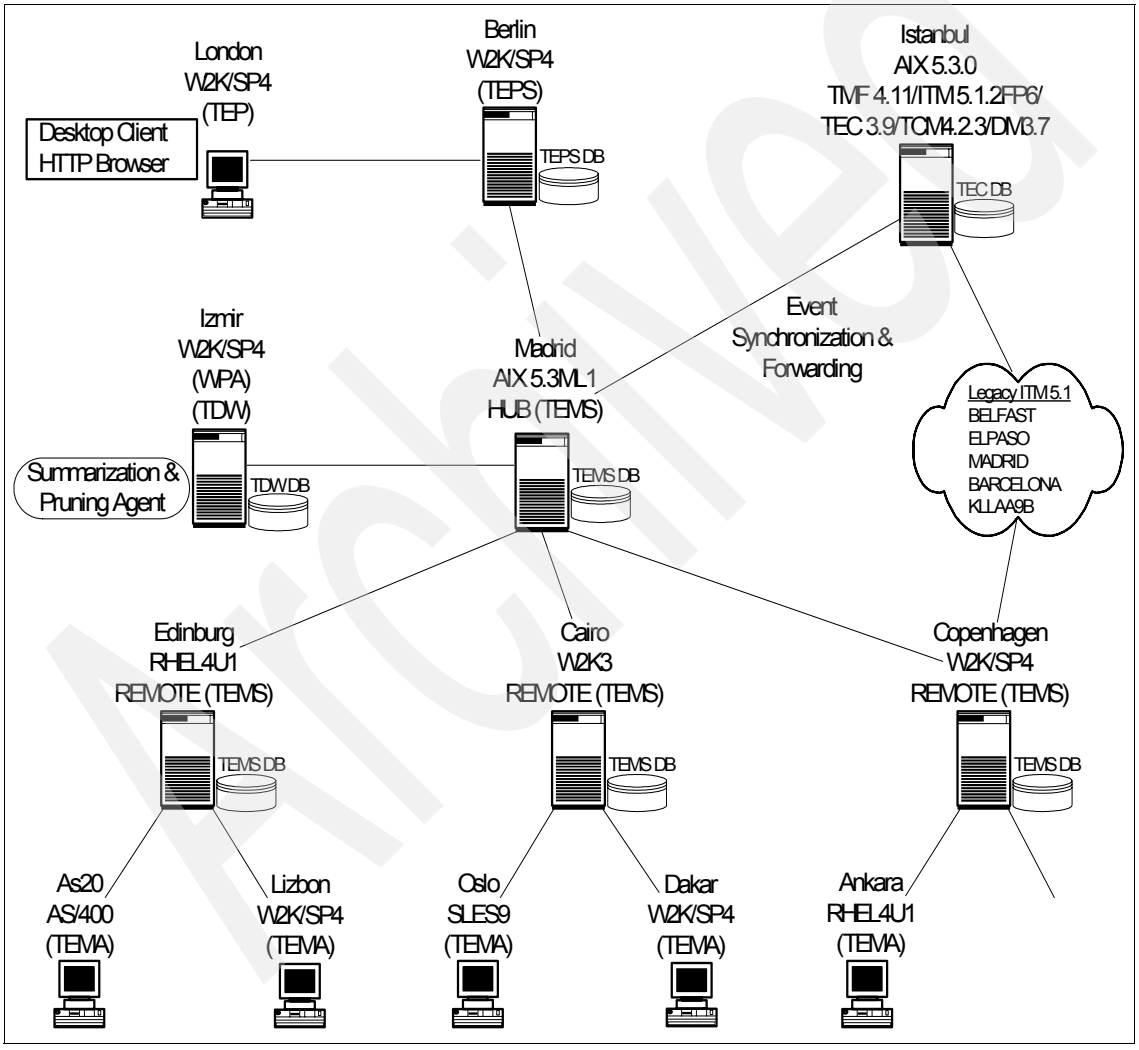

Figure 3-2 Lab architecture for a large-scale enterprise, scenario 2

This architecture is scalable and can be extended to contain more than 4000 agents. Refer to 1.2.4, “Huge installation (greater than 4000 agents)” on page 16 for more details about extending this architecture to handle more than 4000 agents.

To build the second scenario and reconfigure cairo as a Remote TEMS, we performed the steps described in 3.2.17, “Replacing a Hub TEMS server with a new one” on page 210.

3.2 Installing IBM Tivoli Monitoring 6.1

This section describes step-by-step the installation process of the different IBM Tivoli Monitoring 6.1 components, showing examples for both GUI and command line interface (CLI) installation.

Table 3-2 provides an overview of the steps required to fully install and deploy an IBM Tivoli Monitoring 6.1 environment.

Table 3-2 Installation steps

Steps	References
Planning the installation	“Planning the installation” on page 95
Install the Tivoli Enterprise Monitoring Server	“Installing and configuring a Hub TEMS on a Windows server” on page 102 and “Installing a Hub TEMS on a UNIX server” on page 203
Install the Tivoli Enterprise Remote Monitoring Server	“Installing a Remote TEMS on a Windows and UNIX server” on page 116
Install the Tivoli Enterprise Portal Server	“Tivoli Enterprise Portal Server - TEPS” on page 121
Install Tivoli Management Agent	“Tivoli Enterprise Monitoring Agent” on page 129
Install the portal desktop client on any system where you want to use it	“Tivoli Enterprise Portal (TEP)” on page 160
Install Warehouse Proxy	“Installing the Warehouse Proxy agent” on page 166
Install TEC event synchronization	“Event synchronization installation” on page 181

3.2.1 Planning the installation

This section outlines the information that you need to have ready before starting the installation.

We discuss the following topics:

- Expertise required
- Naming the monitoring server
- Creating an IBM Tivoli account on UNIX servers
- Import the images
- Host name for TCP/IP network services
- Use of fully qualified path names
- File descriptor (maxfiles) limit
- Hardware and software prerequisites

Expertise required

Installing IBM Tivoli Monitoring 6.1 requires expertise in several areas. In this section, we describe some of the general expertise required to perform the tasks listed above. We take each phase of the installation down to the operating system level. In most cases, it is not necessary for one person to have all of the expertise, but if the person designated as the Tivoli administrator possesses some knowledge of these different products, it will be easier to deploy and maintain the product.

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

Database administrator

The database administrator (DBA) must possess an understanding of how databases work. A DBA, if there is one in the organization, needs to know how to perform most of the work to be done with the chosen database. A thorough knowledge of the RDBMS is not needed in most instances, but will greatly enhance the IBM Tivoli Monitoring 6.1 experience.

Operating systems administrator

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

for growing processes, and any other assignments that a UNIX administrator would do in the normal course of business.

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

3.2.2 Define the architecture

Chapter 1, “Architecture and planning” on page 1 gives a complete and detailed description of the best practices to define an architecture that fits into your organization. We set up our lab architecture based on those best practices. The two scenarios resulting from those suggestions are described in Figure 3-1 on page 92 and Figure 3-2 on page 93.

Note: Although IBM Tivoli Monitoring 6.1 can be set up using two hubs with different platforms (Windows and UNIX, for example), if you are planning to implement the Hot Standby feature, it is advisable (but not mandatory) to have them on the same platform.

3.2.3 Creating a deployment plan

A deployment plan is essential for creating and installing an IBM Tivoli Monitoring 6.1 environment. The basic considerations for creating a deployment plan for a Tivoli environment are provided in Version 6.1.0 of *IBM Tivoli Monitoring Installation and Setup Guide*, GC32-9407.

You must gather at least the following information before installing any software:

- Base hardware and software requirements for IBM Tivoli Monitoring 6.1.
  - Whether the computer systems in your distributed network can support this new software, or these systems can be upgraded to meet your business needs, or whether new systems need to be obtained.
  - Which IBM Tivoli Monitoring 6.1 components to install on which computer systems in your distributed network to support your business needs and whether they have additional third-party software requirements. This information is provided in 1.1.1, “Platform support matrix for IBM Tivoli Monitoring 6.1” on page 7.

- For each system where you plan to install components of IBM Tivoli Monitoring 6.1, gather the following information:
  - Name of the monitoring server you are installing or that the agent will connect to
  - Operating system
  - Available memory and available disk space
  - Host name of the system where the product (a monitoring server or one instance of an agent) will execute.
  - Whether the monitoring server being installed will be configured as a hub or remote monitoring server
  - Hub host name
  - Port number

Naming the monitoring server

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

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

Table 3-3 and Table 3-4 on page 98 describe the various TEMS configuration on our two environments.

Table 3-3 Scenario 1 lab TEMS description

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

Table 3-4 Scenario 2 lab TEMS description

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

Creating an IBM Tivoli account on UNIX servers

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

- You can use any valid name. You can install the IBM Tivoli Monitoring software as the root user on UNIX, but you do not have to. If you do not install IBM Tivoli Monitoring 6.1 as root, you must use the following procedure to create the user and correctly set the permission. We created a user called *itmuser* in *itmusers* group. IBM recommends using the Korn shell for your IBM Tivoli account; however, you can use any shell that is shipped with the UNIX operating system.

  a. Create the itmusers group using the following procedures.

     For Linux, Solaris, and HP-UX computers, run the following command:

     ```
     groupadd itmusers
     ```

     For an AIX 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, Solaris and Linux computers run the following command to create the *itmuser* account:

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

- The same user should install all components.
- If you are using NFS or a local file system, you should establish your installation directory according to the guidelines used in your environment.

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

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

a. Set the CANDLEHOME directory. You must use the itmuser user profile.

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

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

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

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

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

```
cd $CANDLEHOME
```

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

```
pwd
```

e. Run the following commands:

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

Important: If you did this operation after the agent installation, run the following command to change the ownership of additional agent files:

```
bin/SetPerm
```

Select **All of the above** to set the proper permission on all installed agents.

Import the images

Import the IBM Tivoli Monitoring 6.1 images to the server where you will perform the installation.

You can create a separate file system where you will download the images and install IBM Tivoli Monitoring 6.1. To install on a Windows system, create a drive distinct from the C: drive (or whatever drive the operating system resides on).

Host name for TCP/IP network services

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

Execute the following command line from the TEMS:

```
nslookup hostname
```

In this example, `hostname` is host name of the servers in the IBM Tivoli Monitoring 6.1 environment (for example, the second Hub TEMS, the Remote TEMS, the TEPS, and so on.). After the command is performed successfully on those servers, proceed with the reverse lookup executing the following command:

```
nslookup -querytype=PTR
```

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

Use of fully qualified path names

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

File descriptor (maxfiles) limit

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

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

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

For AIX computers, run the following command:

```
ulimit -d
```

The `-d` option specifies the size of the data area in kilobytes. If the settings returned are less than 256 MB, increase the maxfiles limit to 256 MB.

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

Hardware and software prerequisites

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

3.2.4 Backup strategies

This section describes several of the backup strategies that should be deployed when using IBM Tivoli Monitoring 6.1. Without a good backup strategy, the enterprise can be vulnerable to outages of indeterminate lengths of time.

Tivoli backups

If the IBM Tivoli Monitoring 6.1 is being installed in an existing Tivoli server, we suggest that you back up the Tivoli database just in case, even though IBM Tivoli Monitoring 6.1 does not update the Tivoli Framework database. There are two ways to back up the Tivoli server and managed nodes. The **wbkupdb** command is available to back up the pertinent files in the $DBDIR directory. This does not back up custom scripts or anything outside of $DBDIR, but it is sufficient to restore a Tivoli server to running state if there is corruption in the database.

System-level backups

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

If you are installing IBM Tivoli Monitoring 6.1 in a TMR, make sure that you have a “clean” system before backing up. Use the **wchkdb** command with the appropriate parameters:

-ux For interconnected Tivoli regions
-u For all managed nodes
-ut For just the Tivoli server

A “clean” **wchkdb** command result allows for better backup and restore capabilities.

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

3.2.5 Installing and configuring the scenario 1 environment

This section describes the different IBM Tivoli Monitoring 6.1 components' installation and configuration on an Windows Hub TEMS environment.

Installing and configuring a Hub TEMS on a Windows server

The following sections provide detailed information about installing a Hub TEMS on a Windows server and performing the initial configuration.

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

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

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

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

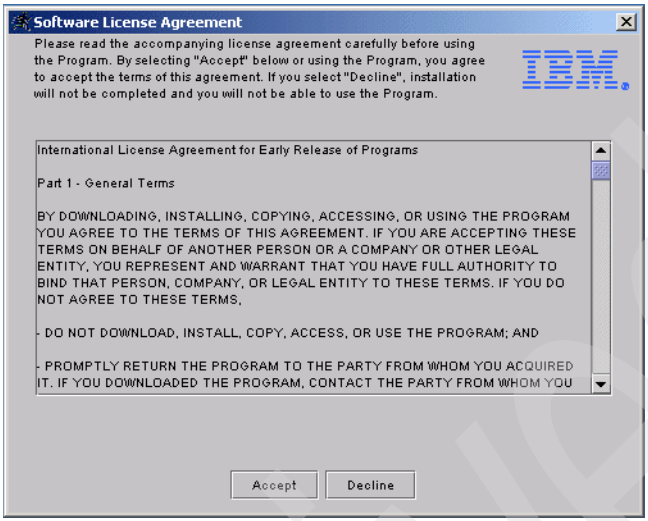

Figure 3-3 License agreement windows

4. Choose the directory where you want to install the product. The default directory is C:\IBM\ITM. You are strongly recommended to install IBM Tivoli Monitoring 6.1 in a different drive from one that holds the operating system. Click **Next**. Figure 3-4 shows the windows with the installation directory.

Figure 3-4 Installation windows

5. The next window asks you to type a 32-bit encryption key. You can use the default key.

Notes:

- This encryption key is used to established a secure connection (using SSL protocol) between the Hub TEMS and the other components of the IBM Tivoli Monitoring 6.1 environment as the Remote TEMS connected to the hub. Do not use any of the following characters in your key:

  =

  ,

  |

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

6. Click **Next**, then **OK** to confirm the encryption key.
7. Select the components that you want to install. Figure 3-5 shows the components we selected for our installation. Click **Next**.

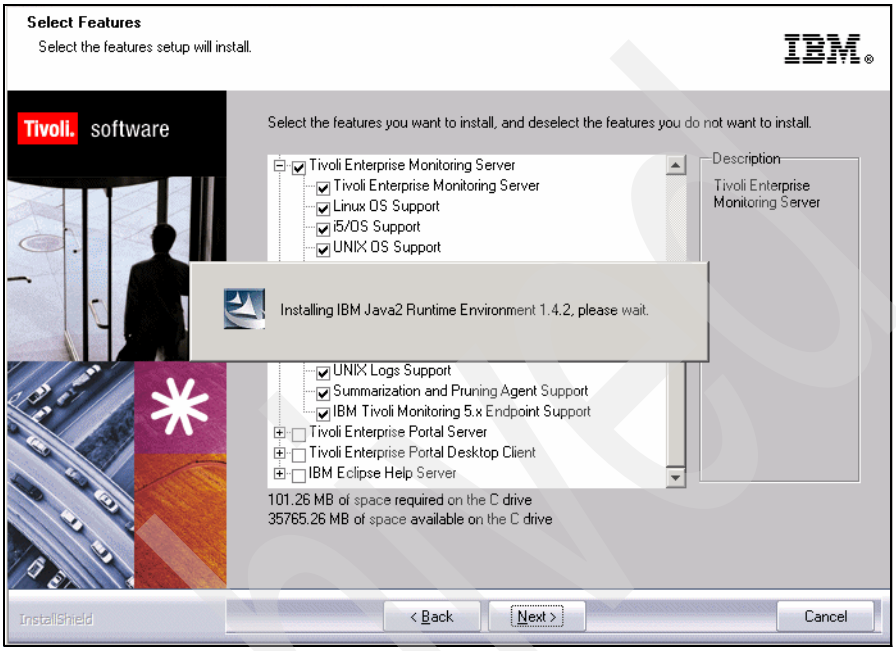

Figure 3-5 List of selected components to be installed

8. If you want to perform remote deployment of agent software, select the agents that you want to deploy (Figure 3-6). This step creates and populates the deployment depot, from which you can deploy agents at a later time.

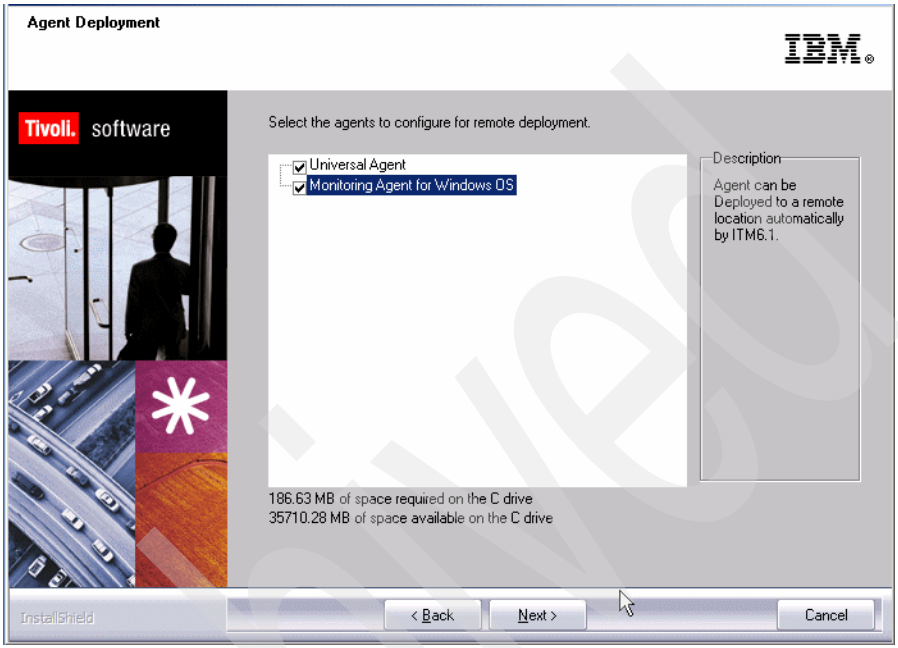

Figure 3-6 Agent list for remote deployment

9. Click **Next**.

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

10. Select a program folder as outlined in Figure 3-7 and click **Next**. The default program folder name is IBM Tivoli Monitoring.

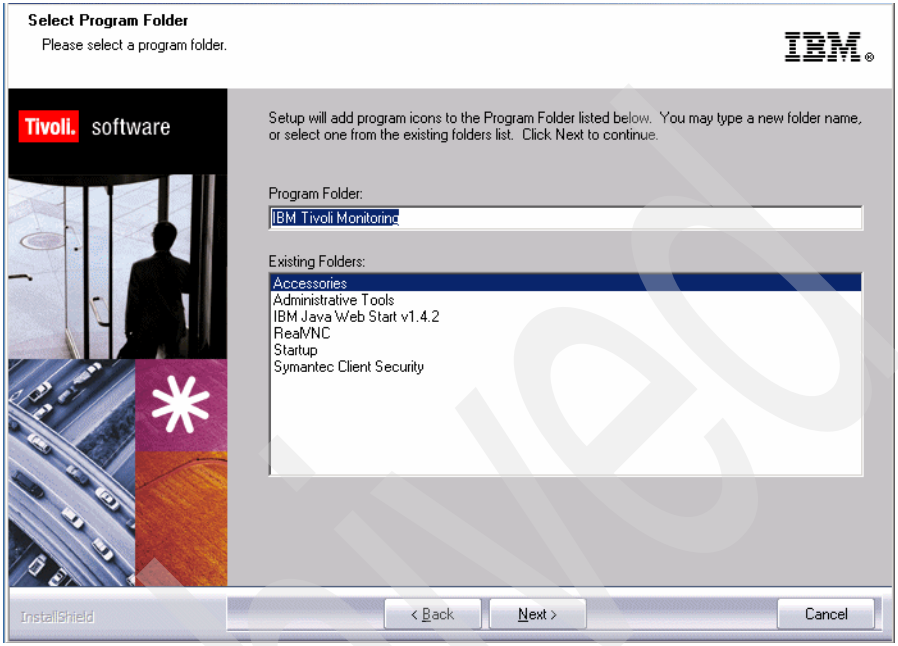

Figure 3-7 Program Folder for the IBM Tivoli Monitoring 6.1 installation

11. Review the installation summary details. This summary identifies what you are installing and where you have chosen to install. Click **Next** to begin the installation of components (Figure 3-8).

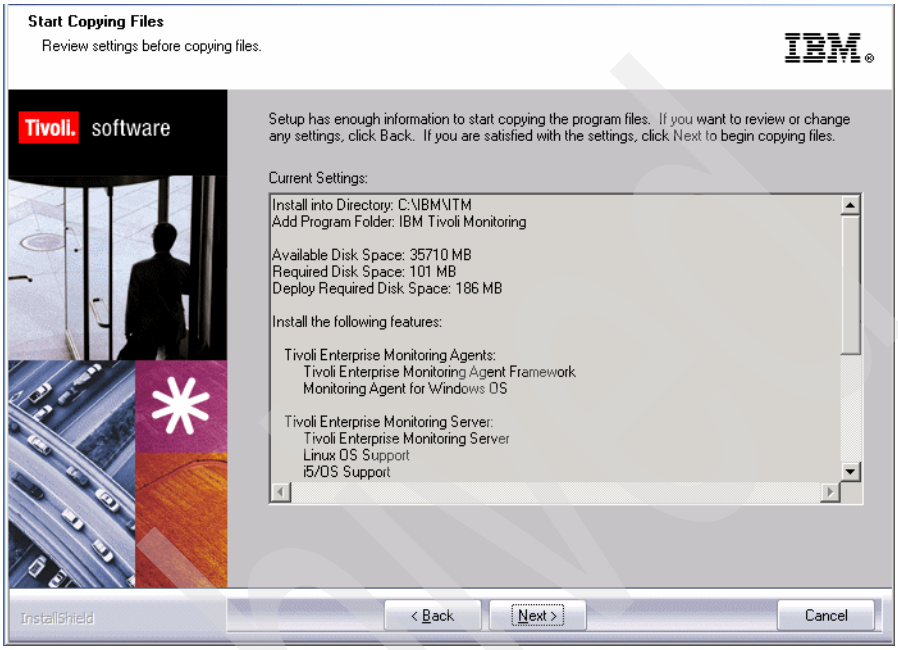

Figure 3-8 Installation summary details

12. After the components are installed, a configuration window (Figure 3-9) is displayed with the list of components that can be configured. Select those you want to configure and click **Next**. We selected all three components.

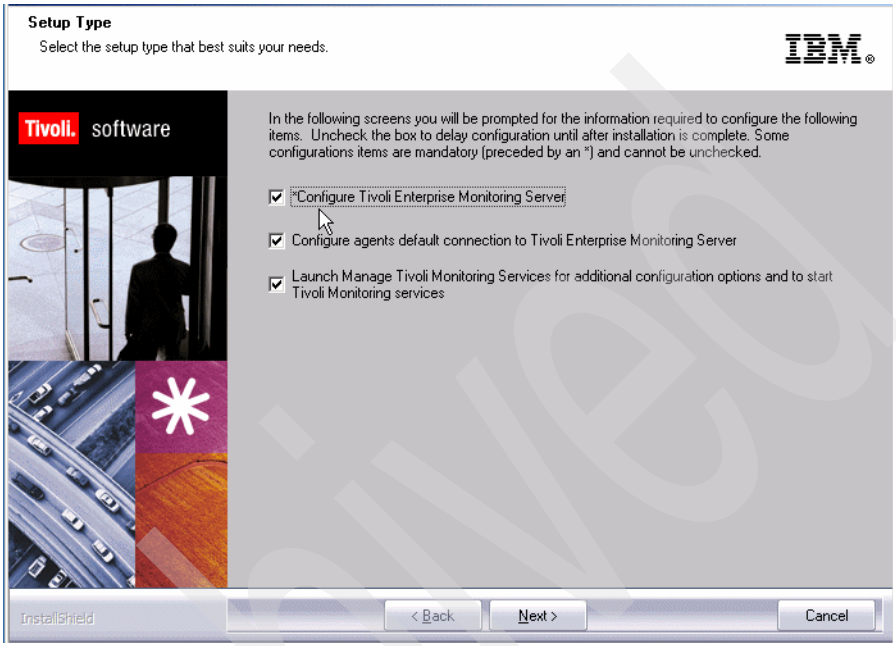

Figure 3-9 List of components that will be configured

13. Figure 3-10 shows the different options of monitoring the type of server that can be selected. Select **Hub**.

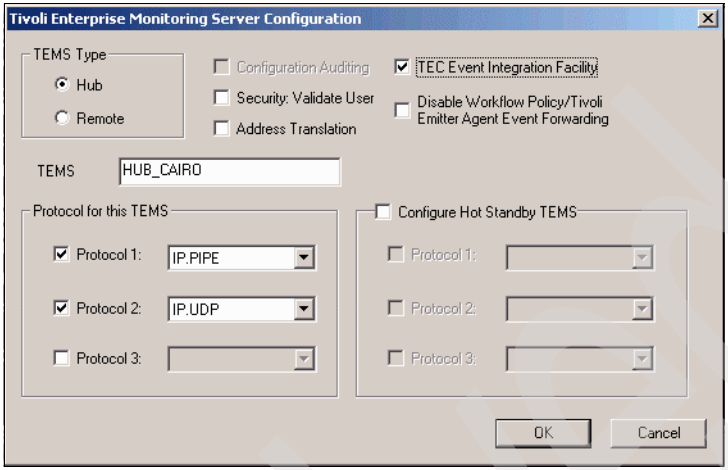

Figure 3-10 Monitoring server configuration window

14. Verify that the name of this monitoring server is correct in the TEMS field. If it is not, change it. The default name is hub_hostname. We chose HUB_CAIRO as our TEMS name.

15. Identify the communications protocol for the monitoring server. Your choices are: IP.UDP, IP.PIPE, IP.SPIPE, or SNA. You can specify three methods for communication, enabling you to set up backup communication methods. If the method you've identified as Protocol 1 fails, Protocol 2 is used. We selected IP.PIPE as our primary protocol and IP.UDP as secondary one.

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

If a firewall is between your TEMS and your agents, you cannot use IP.UDP.

Table 3-5 on page 111 describes the communication protocols that can be used. This information is valid for all components in the IBM Tivoli Monitoring 6.1 environment. We outline only Hub and Remote TEMS in this table.

Table 3-5 Communications protocol descriptions

Field	Description
IP.UDP settings: primary Hub TEMSIP.UDP settings: primary Hub TEMS	
Hostname or IP address	The host name or IP address for the hub monitoring server.
Port # and/or Port Pools	The listening port for the hub monitoring server.
IP.PIPE settings: primary Hub TEMS	
Host name or IP Address	The host name or IP address for the hub monitoring server.
Port Number	The listening port for the monitoring server. The default value is 1918.
IP.SPIPE settings: primary Hub TEMS	
Host name or IP Address	The host name or IP address for the hub monitoring server.
Port Number	The listening port for the monitoring server. The default value is 3660.
ESNA settings: remote TEMS	
Local LU Alias	The LU alias
TP Name	The transaction program name for this monitoring server.
SNA settings: primary Hub TEMS	
Network Name	The SNA network identifier for your location.
LU Name	The LU name for the monitoring server. This LU name corresponds to the Local LU Alias in your SNA communications software.
LU 6.2 LOGMODE	The name of the LU6.2 LOGMODE. The default value is .CANCTDCS.
TP Name	The transaction program name for the monitoring server.

16. If you want to forward situation events to IBM Tivoli Enterprise Console, select **TEC Event Integration Facility**.

We did not select the Configure Hot Standby TEMS option, because we will set it up when all TEMS are installed and properly configured. Neither did we select Disable Workflow Policy/TivoliEmitter Agent Event Forwarding. We suggest you do the same.

Click **OK**.

17. The next window displays the options to configure the hub server name or IP address and communication port the communication protocol will use. Complete the fields as shown in Figure 3-11.

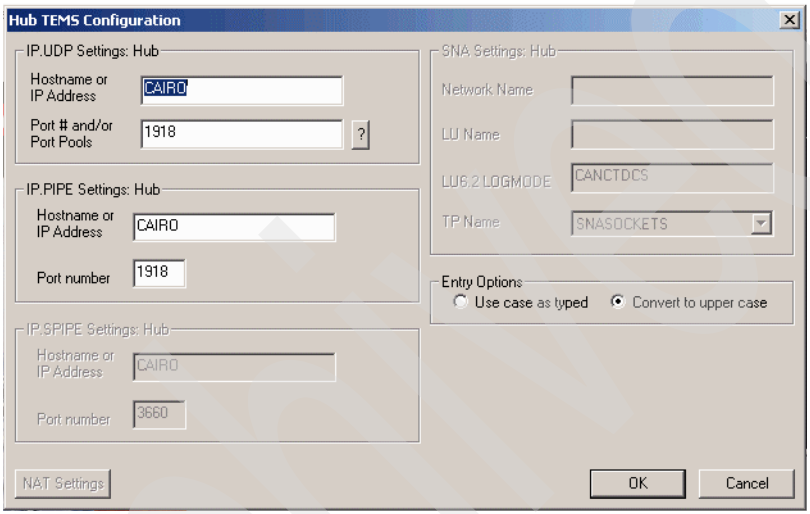

Figure 3-11 Host and communication protocol configuration window

18. If you are certain that you have typed in the values for all of these fields with exactly the correct cases (upper and lower cases), you can select **Use case as typed**. However, because IBM Tivoli Monitoring is case-sensitive, consider selecting **Convert to upper case** to reduce the chance of user error. Click **OK** to continue.

    The next configuration step is to add application support to the monitoring server, such as the workspaces and situations for agents.

19. After the configuration is complete you are prompted to seed the TEMS. Specify the location of the monitoring server. You have two options:

    a. On this computer

    b. On a different computer

    Chose the first option and click **OK**.

20. Because the monitoring server is not currently running, it will start automatically before the process begins. Click **OK** when you see Figure 3-12.

Figure 3-12 Monitoring server start confirmation windows

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

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

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

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

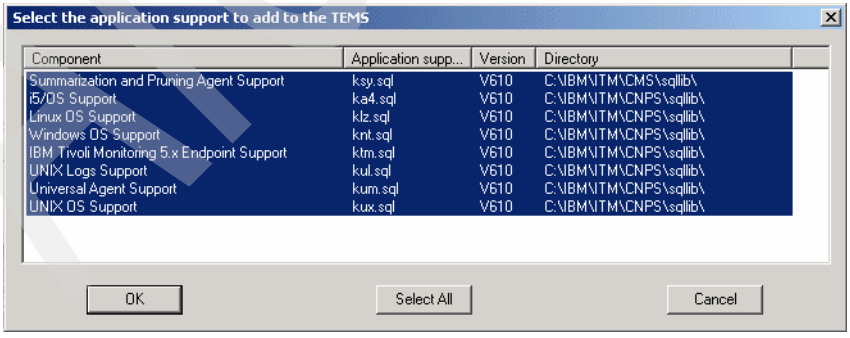

Figure 3-13 Application support to be added to TEMS

22. Verify that each application support added for the components has a return code (rc) equal to 0, as shown in Figure 3-14. Click **Next**.

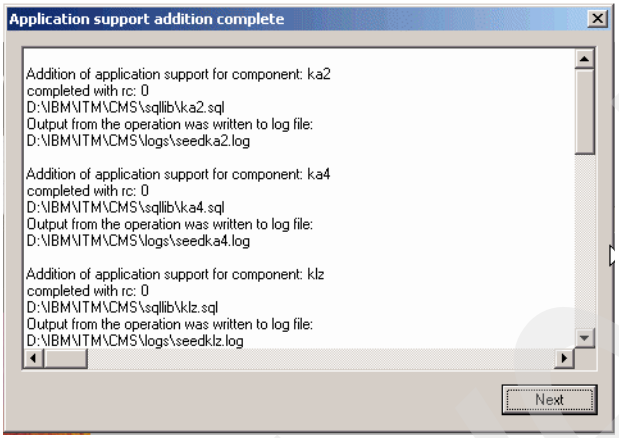

Figure 3-14 Application addition support window

The next configuration step (Figure 3-15 on page 115) configures the default communication between any IBM Tivoli Monitoring component and the hub monitoring server.

23. Specify the default values for IBM Tivoli Monitoring components to use when they communicate with the monitoring server.

    a. If agents must cross a firewall to access the monitoring server, select **Connection must pass through firewall**.

    b. Identify the type of protocol that the agents use to communicate with the hub monitoring server. Your choices are: IP.UDP, IP.PIPE, IP.SPIPE, or SNA as described in Table 3-5 on page 111. You can specify three methods for communication; this enables you to set up backup communication methods. If the method you identified as Protocol 1 fails, Protocol 2 is used. If using UDP will not break your security rules, we suggest using IP.UDP protocol.

    c. Click **OK**.

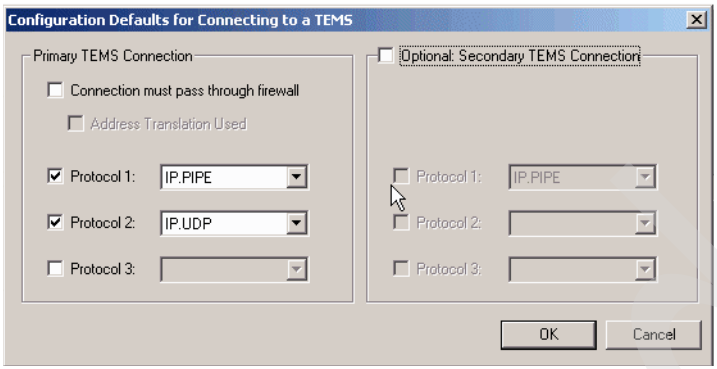

Figure 3-15 Communication protocol configuration to a TEMS

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

    The Manage Tivoli Enterprise Monitoring Services utility opens (Figure 3-16). You can start, stop, and configure IBM Tivoli Monitoring components with this utility.

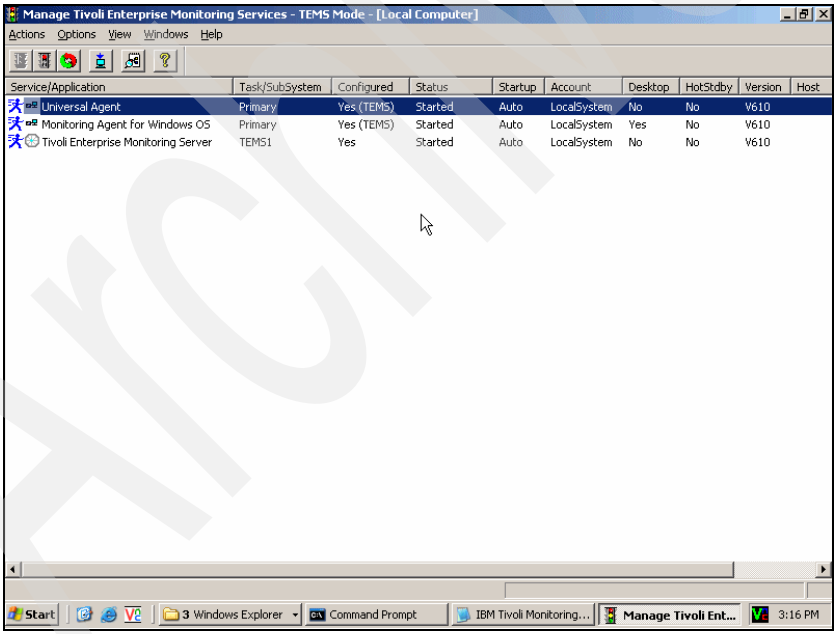

Figure 3-16 IBM Tivoli Monitoring 6.1 services window

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

3.2.6 Installing a Remote TEMS on a Windows and UNIX server

This section provides detailed information about installing and configuring the remote monitoring server. The following procedures are used in both scenarios.

Installing a Remote TEMS on a Windows server

The installation of a Remote TEMS is similar to the installation of a Hub TEMS. Unless they differ from the Hub TEMS installation, the figures for the Remote TEMS installation will not be shown.

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

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

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

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

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

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

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

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

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

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

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

    After the components are installed, a configuration window opens.
13. Select what you want to configure and click **Next**. The first step configures the monitoring server.
14. Select the type of monitoring server you are configuring: Hub or Remote. For this procedure, select **Remote** as shown in Figure 3-17.

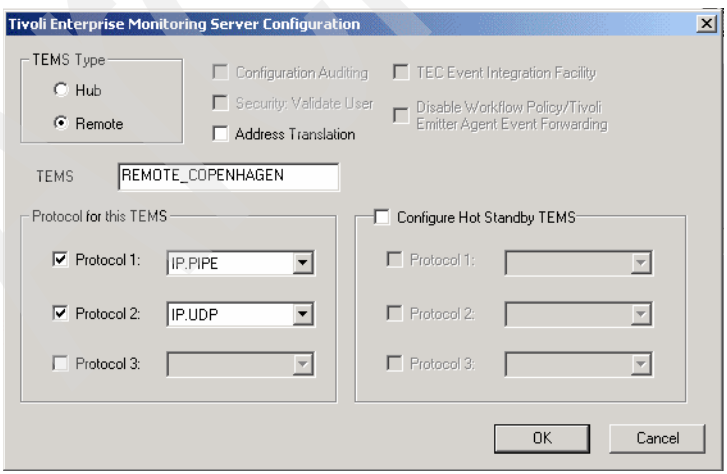

Figure 3-17 Remote TEMS configuration window

15. Verify that the name of this monitoring server is correct in the TEMS. If it is not, change it.
16. Identify the communications protocol for the monitoring server. Your choices are: IP.UDP, IP.PIPE, IP.SPIPE, or SNA. You can specify three methods for communication, which enables you to set backup communication methods. If the method you have identified as Protocol 1 fails, Protocol 2 will be used. Click **OK**.
17. Complete the following fields for the communications protocol for the monitoring server. Table 3-5 on page 111 shows descriptions for protocols that can be used.
18. If you are certain that you have typed the values for all of these fields with exactly the correct casing (upper and lower cases), you can select **Use case as typed**. However, because IBM Tivoli Monitoring is case-sensitive, consider selecting **Convert to upper case** to reduce the chance of user error.
19. Click **OK** to continue.

    The next configuration step is to seed the monitoring server.
20. Specify the location of the monitoring server. You have two options:
    a. This computer
    b. On a different computer

    Select **This computer** and click **OK**.
21. Because the monitoring server is not currently running, it is started automatically before the seeding process begins. Click **OK** when you get the the message that tells you this.
22. Select the data that you want to add to the monitoring server. By default, all available product data is selected. Click **OK**.
23. Click **Next** on the message that provides information about the seeding. The next configuration step configures the default communication between any IBM Tivoli Monitoring component and the hub monitoring server.
24. Specify the default values for any IBM Tivoli Monitoring component to use when they communicate with the monitoring server.
    a. If agents must cross a firewall to access the monitoring server, select **Connection must pass through firewall**.
    b. Identify the type of protocol that the agents use to communicate with the hub monitoring server. Your choices are: IP.UDP, IP.PIPE, IP.SPIPE, or SNA. You can specify three methods for communication, which enables you to set backup communication methods. If the method you have identified as Protocol 1 fails, Protocol 2 is used. Click **OK**.

25. Complete the communication protocol fields for the monitoring server. See Table 3-5 on page 111 for definitions of these fields.
26. Click **Finish** to complete the installation.

Installing Remote TEMS on a UNIX/Linux server

The Remote TEMS installation procedure is the same as the one for Hub TEMS. The difference occurs during the configuration. Table 3-6 shows the steps for installing, configuring, and seeding a Remote TEMS.

Table 3-6 Steps for installing a Remote TEMS

Steps	Where to find information
1. Install the Remote TEMS using the same instruction as installing the Hub TEMS.	Installing a Hub TEMS on a UNIX server
2. Configure the remote TEMS.	Configuring Remote TEMS on a UNIX/Linux server
3. Seed the Remote TEMS.	Installing agent support on (seeding) the hub monitoring server

Configuring Remote TEMS on a UNIX/Linux server

Use the following steps to configure the hub monitoring server:

1. At the command line, change to the `opt/IBM/ITM/bin` directory (or the directory where you installed IBM Tivoli Monitoring).
2. Run the following command:

   ```
   ./itmcmd config -S -t tems_name
   ```

   tems_name is the name of your monitoring server (for example, REMOTE_EDINBURG).
3. Type `remote` to indicate that this is a Remote TEMS.
4. Press Enter to accept the default host name for the monitoring server. This should be the host name for your computer. If it is not, type the correct host name and press Enter.
5. Enter the type of protocol to use for communication with the monitoring server. Your choices are: ip, ip.pipe, sna, or ip.spipe. Press Enter to use the default communications protocol (IP.PIPE).
6. If you want to set up a backup protocol, enter that protocol and press Enter. If you do not want to use backup protocol, press Enter without specifying a protocol.
7. Depending on the type of protocol you specified, provide the port number for each communication protocol and press Enter.

8. Press Enter to not specify the name of the KDC_PARTITION.
9. Press Enter when prompted for the path and name of the KDC_PARTITION.
10. If you want to use Configuration Auditing, type `y`; otherwise type `n` and press Enter.
11. Press Enter to accept the default setting for Hot Standby (NO). For best results, wait until after you have fully deployed your environment to configure Hot Standby for your monitoring server. See “Configuring Hot Standby” on page 197 for information about configuring Hot Standby.
12. Press Enter to accept the default for the Optional Primary Network Name (`none`).
13. Press Enter for the default security: `Validate User setting (no)`. If you need to use security validation in your environment, you can enable it after initial configuration is complete.
14. If you will use event synchronization to view situation events, type `y` and press Enter to enable TEC Event Integration. Complete the following additional steps:
    a. Type the name of the IBM Tivoli Enterprise Console event server and press Enter.
    b. Type the port number for the event server and press Enter.
15. Press Enter to not disable the Workflow Policy/Tivoli Emitter Agent.
16. Type `S` to save the default SOAP configuration and exit the configuration.

Notes:

- You can configure any SOAP information at a later time. The procedure is described in “Installing event synchronization on your event server” on page 183.
- A configuration file is generated in the install_dir/config directory with the format host_name_ms_tems_name.config (for example, edinburg_ms_REMOTE_EDINBURG.config).

3.2.7 Tivoli Enterprise Portal Server - TEPS

This section describes the steps for installing and configuring a TEPS in a Windows server using DB2 8.2 as RDBMS.

Note: Our choice for the Windows server was driven by a limitation of the IBM Tivoli Monitoring 6.1 beta version we were using. In the beta version of the code that we used for this project, it was not possible to connect to a Data Warehouse for long-term historical data views using a Linux portal server. This limitation is expected to go away in the general availability version. Refer the IBM Tivoli Monitoring 6.1 general availability documentation or contact IBM support to verify whether this issue has been resolved, if you are considering changing your platform because of that limitation.

Preinstallation steps

The Tivoli Enterprise Portal Server function requires a database to store information. Refer to *IBM Tivoli Monitoring Installation and Setup Guide*, GC32-9407, to install and set up your RDBMS.

Install the RDBMS

Prior to installing the TEPS, you have to install and set up the DB2 database in your environment.

ODBC connection for the TEPS

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

Create a user on the DB2 server

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

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

Installing the portal server on a Window server

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

1. Launch the installation wizard by double-clicking the **setup.exe** file in the WINDOWS subdirectory of the installation media.
2. Click **Next** on the Welcome window to start the installation.
3. Read and accept the software license agreement by clicking **Accept**.

4. If you do not have a database (DB2 or MS SQL) or the IBM Java SDK installed on this computer, a message regarding potentially missing required software is displayed. If you are missing a database, stop the installation, install the required database, and begin the installation again. If you are missing the IBM Java SDK, the installation program installs it automatically during a later step. Click **Next**.

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

5. Specify the directory where you want to install the portal software and accompanying files. The default location is C:\IBM\ITM. Click **Next**.
6. Type an encryption key to use. This key should be the same as what was used during the installation of the monitoring server to which this portal server will connect. Click **Next** and then **OK** to confirm the encryption key.
7. Select Tivoli Enterprise Portal Server from the list of components to install as shown in Figure 3-18.

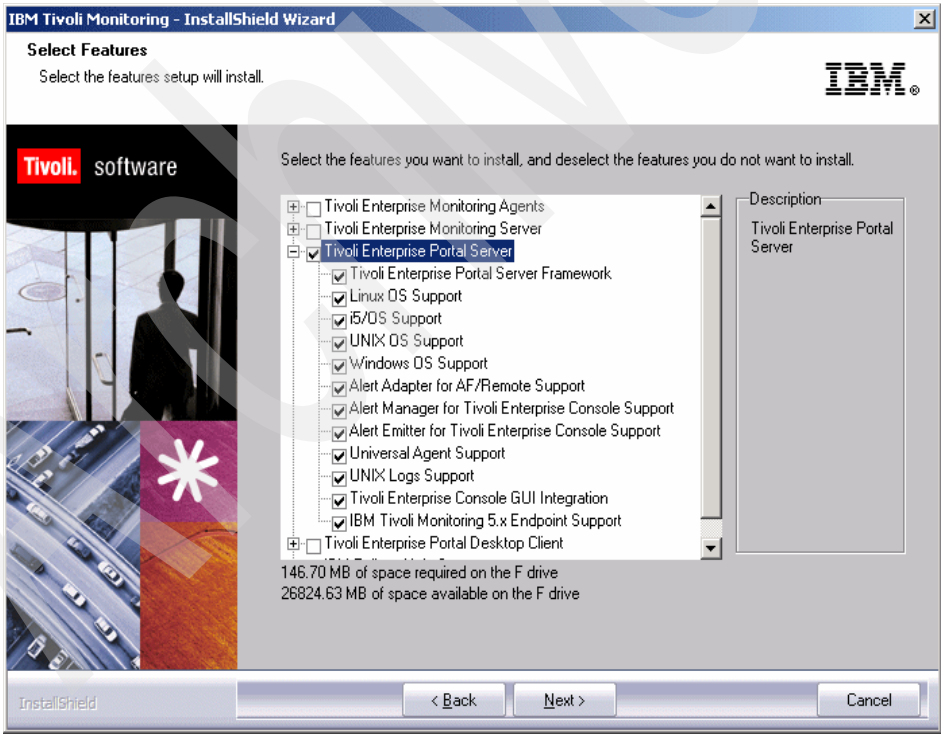

Figure 3-18 IBM Tivoli Monitoring 6.1 Components List

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

8. If you want to view events from the IBM Tivoli Enterprise Console event server through the Tivoli Enterprise Portal, expand the **Tivoli Enterprise Portal Server** selection and ensure that **Tivoli Enterprise Console GUI Integration** is selected. Click **Next**.
9. Do not select any agents on the Agent Deploy window. Click **Next**.
10. Type a name for the program folder. The default is IBM Tivoli Monitoring. Click **Next**.
11. Click **Next** to start the installation. After installation is complete, a configuration window (Table 3-19) is displayed.

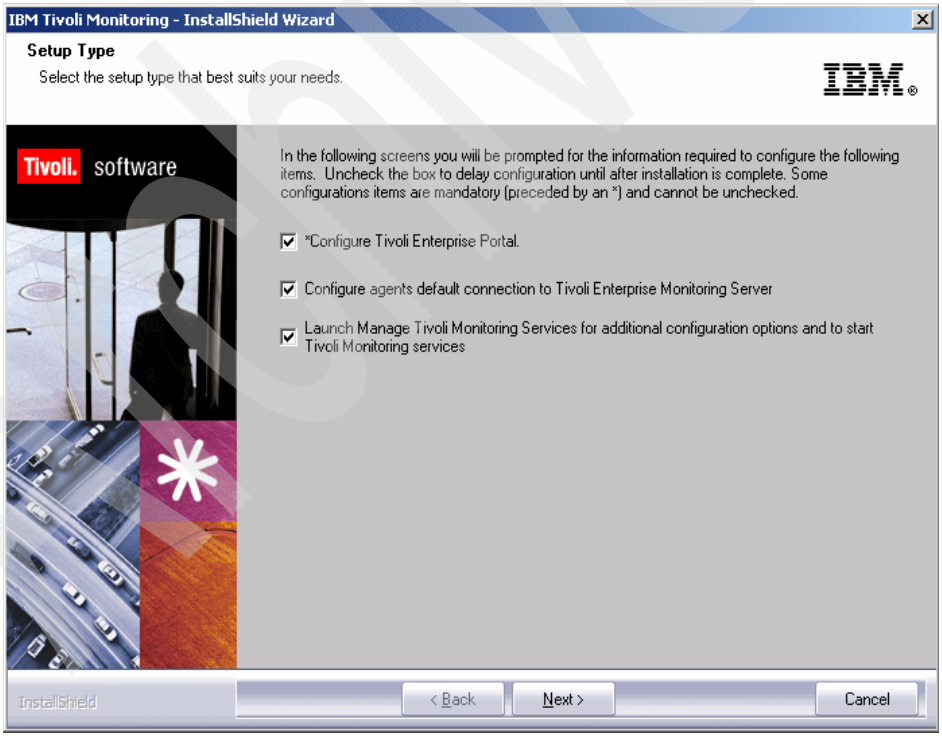

Figure 3-19 TEPS configuration option window

12. Click **Next** to begin configuring the portal server and the connection to the monitoring server, and to open Manage Tivoli Monitoring Services.

13. In the next window (Table 3-20) type the host name of the computer where you are installing the portal server and click **Next**.

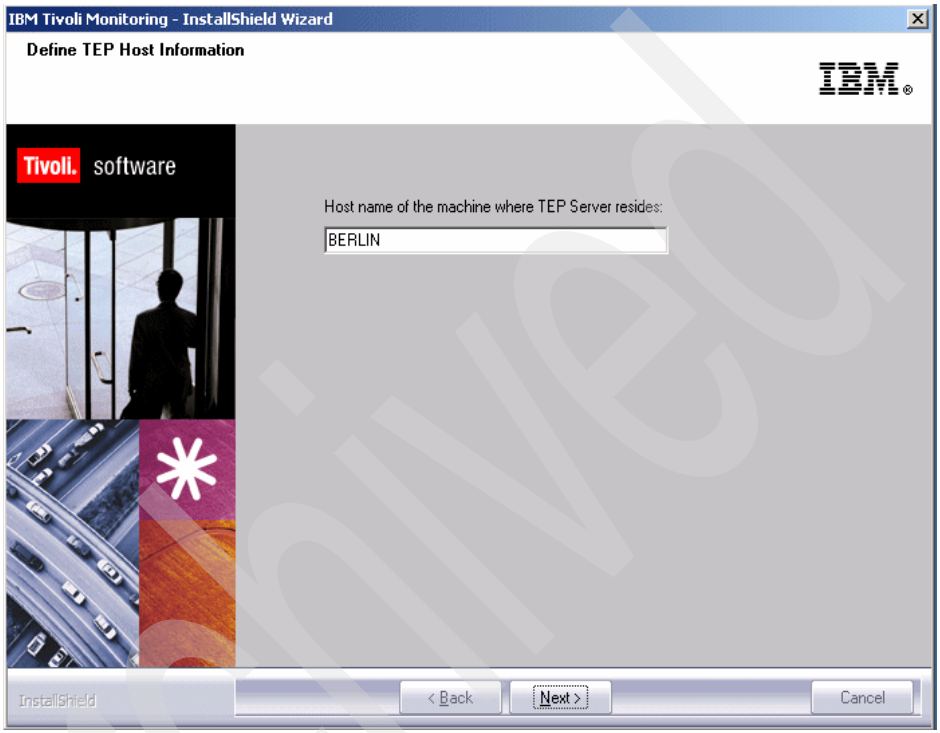

Figure 3-20 Hostname where TEPS will be installed

14. Configure the portal server's connection to the data source (such as your DB2 database). Type the password for the database administrator in the Admin Password field, as shown in Figure 3-21.

    Type a database user ID and password for your db2 Administrator account and click **OK**.

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

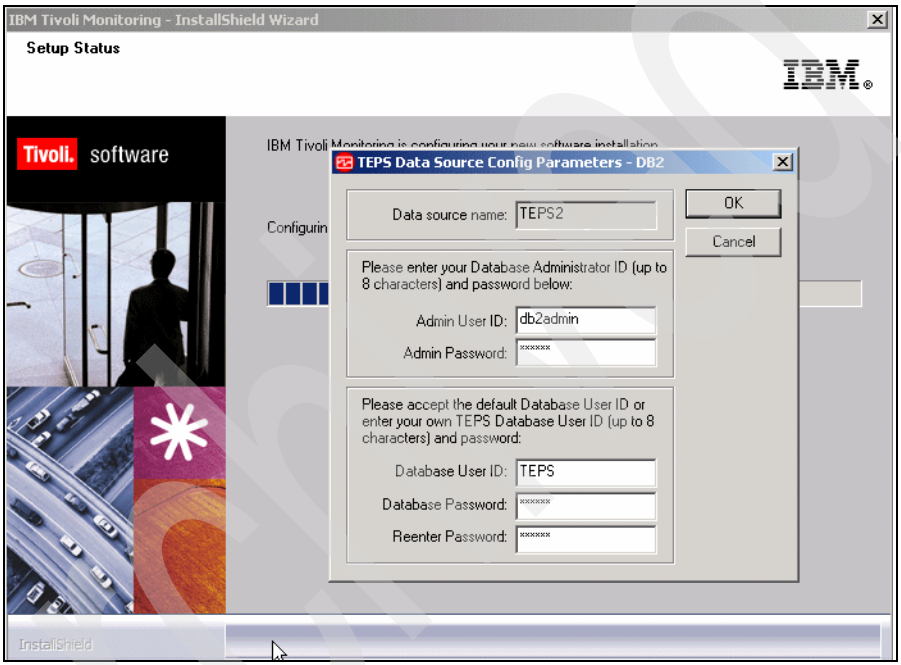

Figure 3-21 TEPS database configuration

15. Click **OK** on the message that tells you that the portal server configuration was successful (Figure 3-22).

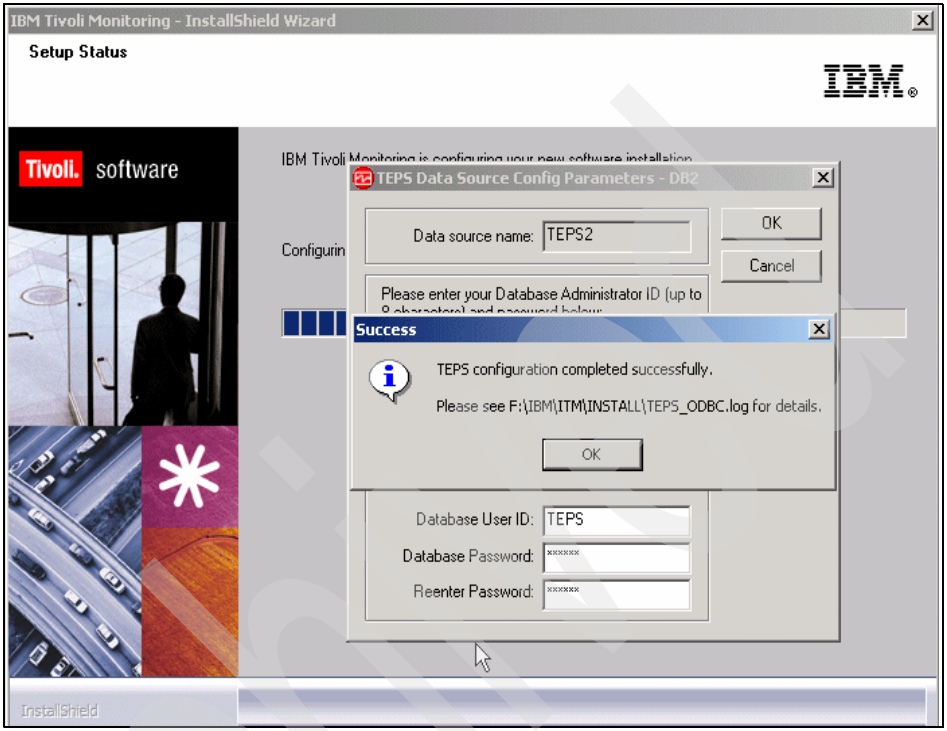

Figure 3-22 TEPS configuration completion window

16. When asked about the user credentials to access the Data Warehouse database, type a previously created user ID (such as `candle`) and a password. Click **Next (**Figure 3-23**)**.

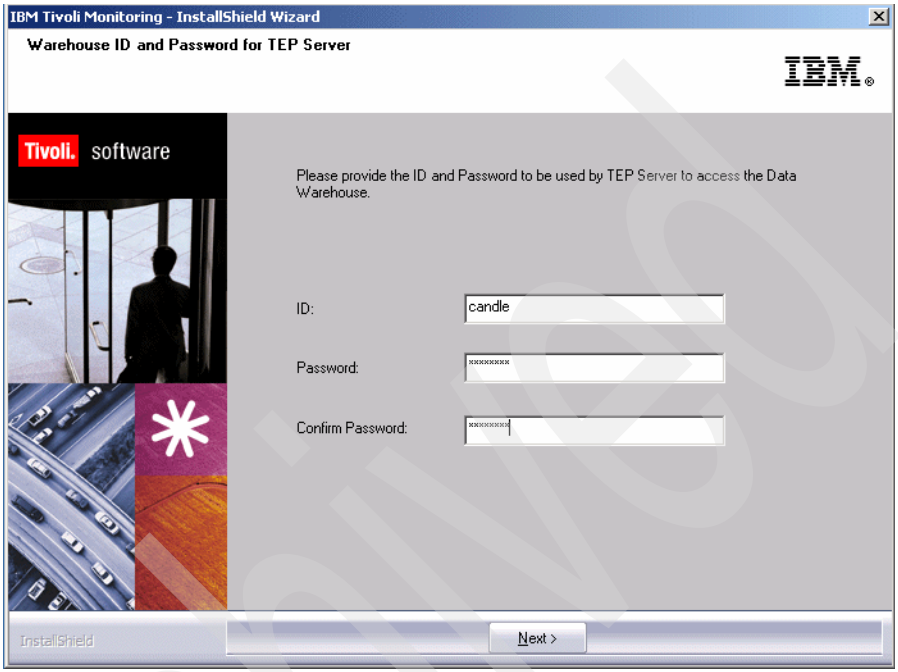

Figure 3-23 TEPS user configuration

17. Select the communication protocols as shown in Figure 3-24 and click **OK** (Figure 3-24). This defines the values for the connection between the portal server and the hub monitoring server.

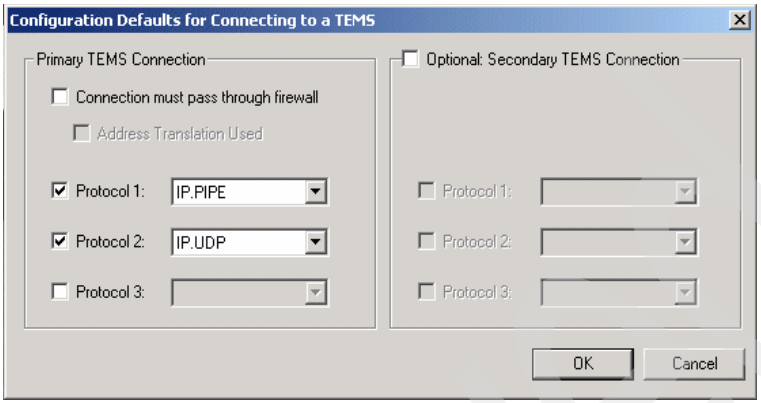

Figure 3-24 Communication protocol window configuration

18. Type the host name or IP address and the port number for the hub monitoring server as shown in Figure 3-25. Click **OK** when finished.

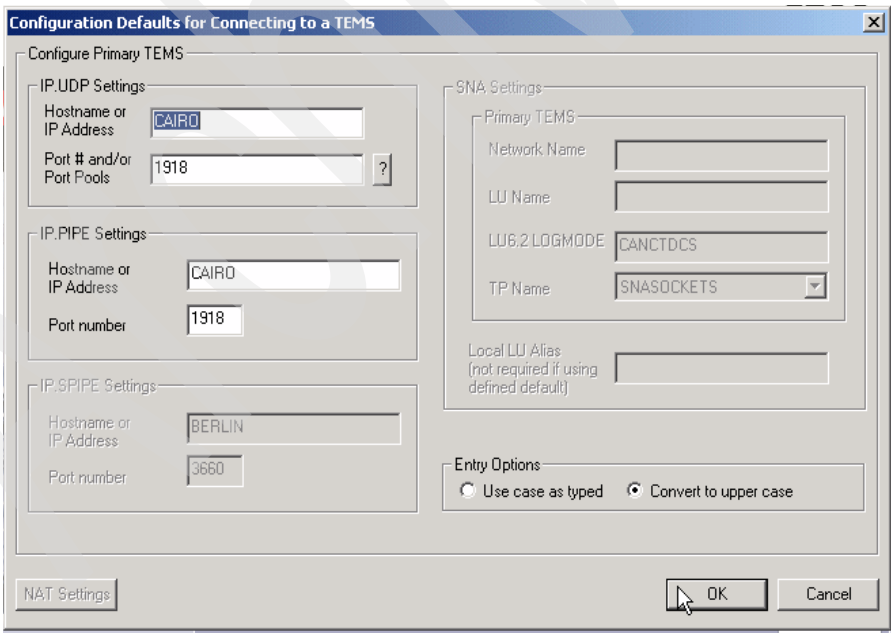

Figure 3-25 Configuration for connection to the TEMS

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

Now the Hub TEMS, Remote TEMS, and the TEPS are installed and configured. We will proceed with the installation of the TEMAs and the TEP, Warehouse Proxy agent, and event synchronization.

3.2.8 Tivoli Enterprise Monitoring Agent

In this section we cover the installation of Tivoli Enterprise Monitoring Agent (TEMA).

Deploying TEMA on a Linux server (using local images)

This section shows step by step how we deploy a TEMA on a Linux server using local downloaded IBM Tivoli Monitoring 6.1 images. Our server name is oslo and the user is itmuser.

Note: Whenever we did not enter or select an option, the Enter key was pressed to accept the default.

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

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

   Example 3-1 shows the output of the command with our selections in bold.

Example 3-1 Output of ./install.sh

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

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

Notes:

- If /opt/IBM/ITM does not exist, you will receive the following message:

```
"/opt/IBM/ITM" does not exist
try to create it [y or n; "y" is default]?
```

- You will notice small differences on the message between the following menu with the one you will be running because of the version differences. But the functions remains the same.

Example 3-2 Output of ./install.sh

```
install.sh        :  searching for product families; please wait.
Select one of the following:
1) Install products via command line.
2) Install products to depot via command line.
3) Exit install.
Please enter a valid number:  1
install.sh        :  OK to install.
install.sh        :  removing old JRE.
install.sh        :  old JRE has been removed.
install.sh        :  unloading JRE package(s).
install.sh        :  calculating available disk space.
install.sh        :  "33631276" kilobytes available.
install.sh        :  running li6243 jre.
Software Licensing Agreement
1. Czech
2. English
3. French
4. German
5. Italian
6. Polish
7. Portuguese
8. Spanish
9. Turkish
Please enter the number that corresponds to the language you prefer.
2
Software Licensing Agreement
Press Enter to display the license agreement on your
screen. Please read the agreement carefully before
installing the Program. After reading the agreement, you
will be given the opportunity to accept it or decline it.
If you choose to decline the agreement, installation will
not be completed and you will not be able to use the
Program.
```

2. Press the Enter key.

Example 3-3 Output of ./install.sh

```
International License Agreement for Early Release of Programs

Part 1 - General Terms

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

- DO NOT DOWNLOAD, INSTALL, COPY, ACCESS, OR USE THE
PROGRAM; AND
1
runGSkit        :  Preparing to install the Global Security Kit.
runGSkit warning:  the 'root' ID or password is required for this phase,
continuing ..
 Will enable automatic agent initiation after reboot.
Please enter root password or press Enter twice to skip.
Password:
Enter the root password

Preparing packages for installation...
gsk7bas-7.0-3.9
runGSkit        :  creating security files.
runGSkit        :  create keyfile.
runGSkit        :  create certificate.
runGSkit        :  setting encryption key.

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

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

Press Enter to continue viewing the license agreement, or,
Enter "1" to accept the agreement, "2" to decline it or
"99" to go back to the previous screen.
1
GSkit encryption key has been set.
Key File directory: /opt/IBM/ITM/keyfiles

 Product packages are available in /home/itmuser/unix
   Product packages are available for the following operating systems and
   component support categories:
```

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

Type the number for the OS or component support category you want, or type
"q" to quit selection
[ number "5" or "Linux Intel R2.6 (32 bit)" is default ]:
5

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

The following products are available for installation:

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

Type the numbers for the products you want to install, or type "q" to
quit selection.
If you enter more than one number, separate the numbers by a comma or
a space.

Type your selections here:  2

The following products will be installed:

  Monitoring Agent for Linux OS V610R115

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

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

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

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

... postprocessing; please wait.

 ... finished postprocessing.

 Installation step complete.

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

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

Post TEMA installation procedure

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

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

   Example 3-4 shows the output of the command.

Example 3-4 Post TEMA installation procedure

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

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

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

Example 3-5 Post TEMA installation procedure

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

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

```
     Now choose the next protocol from one of these:
     - ip
     - sna
     - ip.pipe
     - none
Network Protocol 2 (Default is: none): ip

     Now choose the next protocol from one of these:
     - ip
     - sna
     - none
Network Protocol 3 (Default is: none):none
IP Port Number (Default is: 1918):1918
IP.PIPE Port Number (Default is: 1918):1918
Enter name of KDC_PARTITION (Default is: null):null
IP.SPIPE Port Number (Default is: 3660)

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

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

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

     Now choose the next protocol from one of these:
     - ip
     - sna
     - ip.pipe
     - none
Secondary TEMS Protocol 2 (Default is: none): ip

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

Note: When installing on AIX, it asks:

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

2. When you are done, you can start the agent using this on the command line:

```
./itmcmd agent start lz
```

3. If you do not know the agent code, execute the **./cinfo** command from $CANGDELHOME/bin directory. You should see something like Example 3-6.

Example 3-6 Output ./cinfo command

```
[root@ankara bin]# ./cinfo

********** Fri Sep 23 15:31:15 EDT 2005 ******************
User      : root         Group: root bin daemon sys adm disk wheel
Host name : ankara.itsc.austin.ibm.com   Installer Lvl: 400 / 100
CandleHome: /opt/IBM/ITM
***********************************************************
-- CINFO Menu --
 1) Show products installed in this CandleHome
 2) Show which products are currently running
 3) Show configuration settings
 4) Show installed CD release versions
 X) Exit CINFO
```

4. Select option 1 for the type of result shown in Example 3-7.

Example 3-7 Post TEMA installation procedure

```
********** Fri Sep 23 15:33:37 EDT 2005 ******************
User      : root         Group: root bin daemon sys adm disk wheel
Host name : ankara.itsc.austin.ibm.com   Installer Lvl: 400 / 100
CandleHome: /opt/IBM/ITM
***********************************************************
...Product inventory
ax      IBM Tivoli Monitoring Shared Libraries
         li6243  Version: 610 Rel: 221
jr      Tivoli Enterprise-supplied JRE
         li6243  Version: 400 Rel: 100
lz      Monitoring Agent for Linux OS
         li6263  Version: 610 Rel: 115
uf      Universal Agent Framework
         li6243  Version: 610 Rel: 100
ui      Tivoli Enterprise Services User Interface
         li6243  Version: 610 Rel: 194
um      Universal Agent
         li6243  Version: 610 Rel: 229
-- CINFO Menu --
 1) Show products installed in this CandleHome
 2) Show which products are currently running
 3) Show configuration settings
 4) Show installed CD release versions
 X) Exit CINFO
```

Note: You can get the same result executing the following command:

```
./cinfo -i
```

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

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

Installing TEMA on a Windows server

Use the following steps to install a monitoring agent:

1. Launch the installation wizard by double-clicking the **setup.exe** file on the installation media.
2. Click **Next** on the welcome window (Figure 3-26).

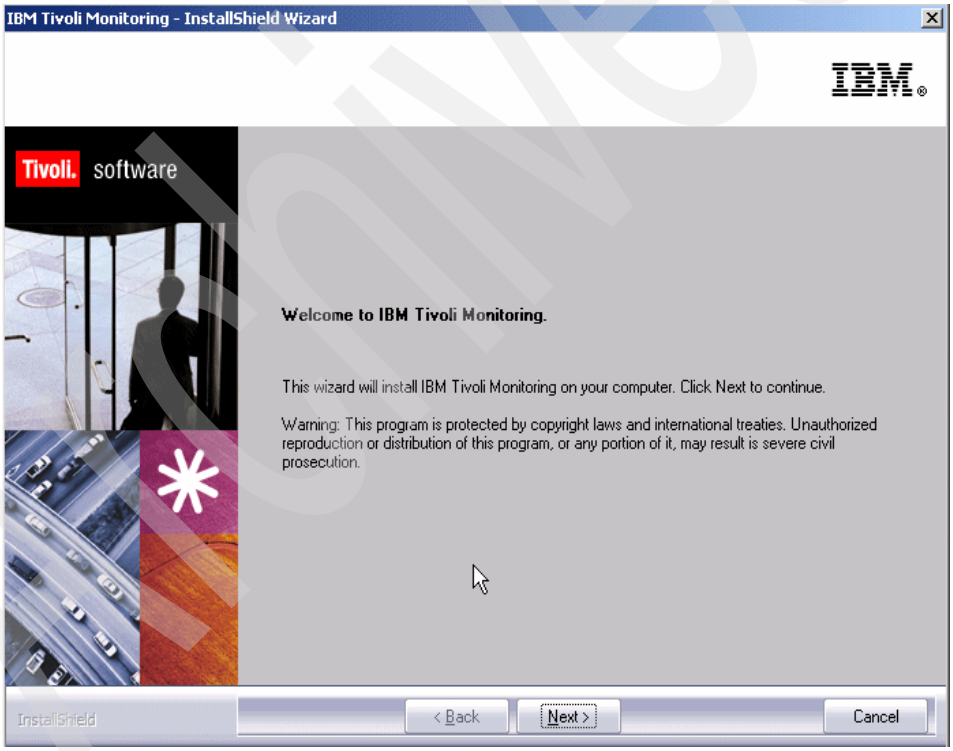

Figure 3-26 IBM Tivoli Monitoring 6.1 welcome installation window

3. Click **Accept** to accept the license agreement (Figure 3-27).

Figure 3-27 IBM Tivoli Monitoring 6.1 license agreements

4. If a database (DB2 or MS SQL) is not installed on this computer, a message regarding potentially missing software is displayed as shown in Figure 3-28. You do not need a database to install a management agent on this computer, so you can ignore this message and click **Next**.

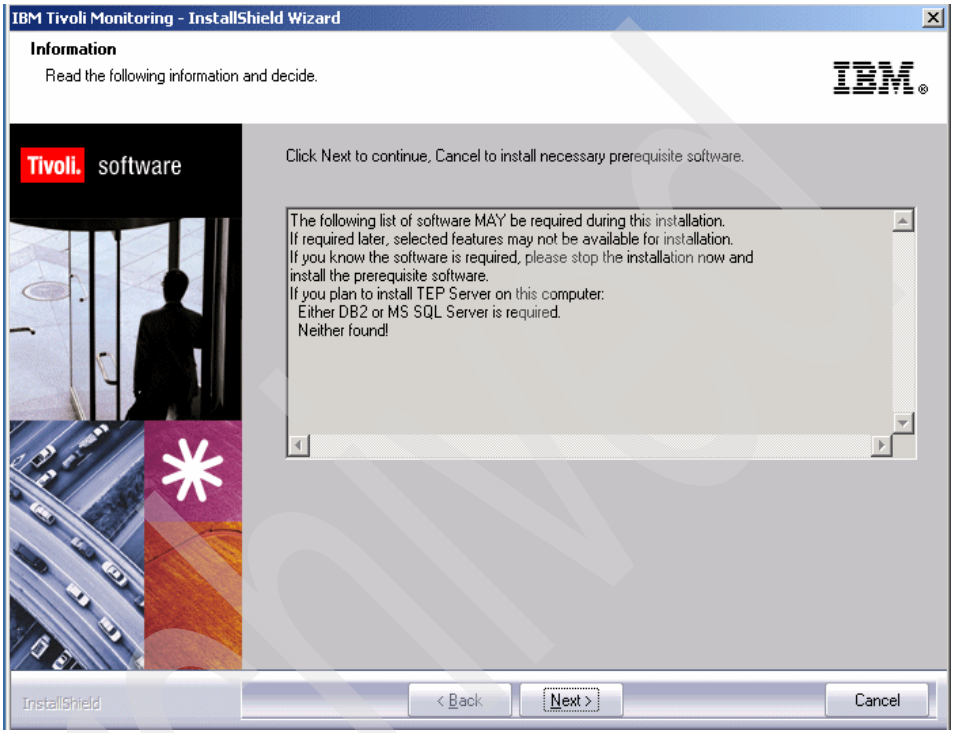

Figure 3-28 IBM Tivoli Monitoring 6.1 requisites information screen

5. Choose the directory where you want to install the product. The default is c:\IBM\ITM as shown in Figure 3-29. Click **Next**.

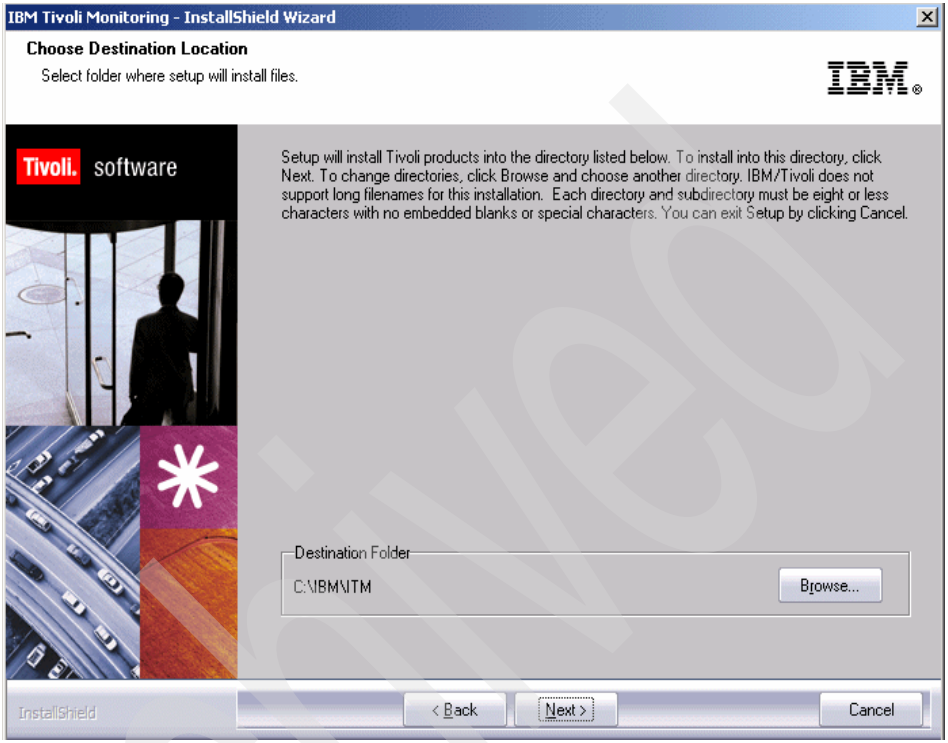

Figure 3-29 IBM Tivoli Monitoring 6.1 default destination installation directory

6. Type the 32-bit encryption key that was used during the installation of the monitoring server to which this monitoring agent connects. Click **Next** and **OK** to confirm the encryption key (Figure 3-30).

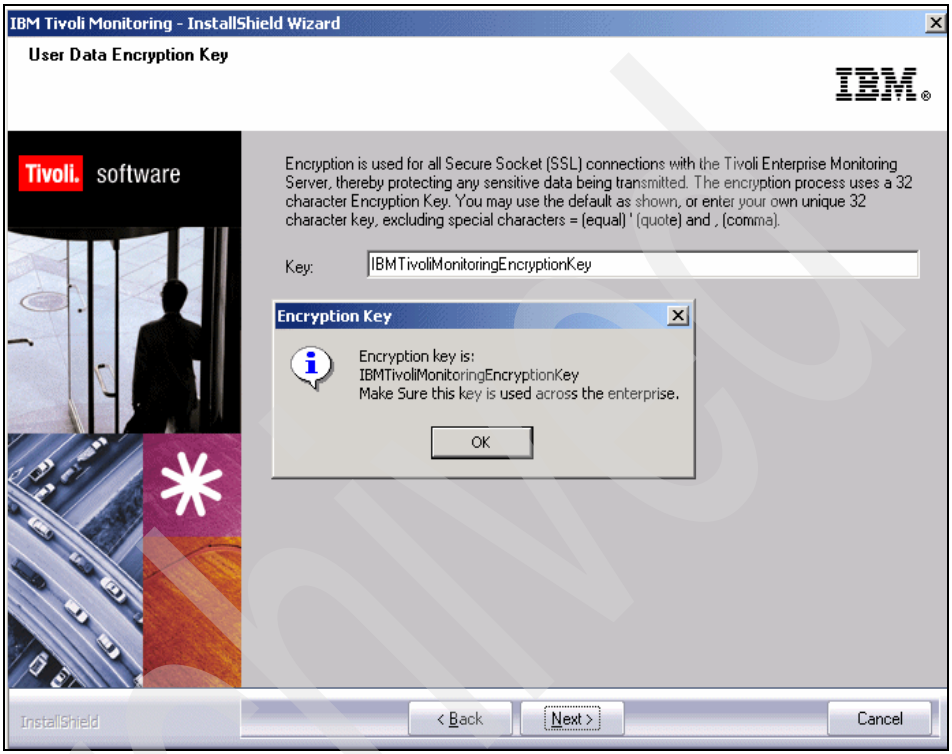

Figure 3-30 IBM Tivoli Monitoring 6.1 encryption key confirmation

7. Expand **Tivoli Enterprise Monitoring Agents** and select the name of the agent that you want to install. Click **Next** (Figure 3-31).

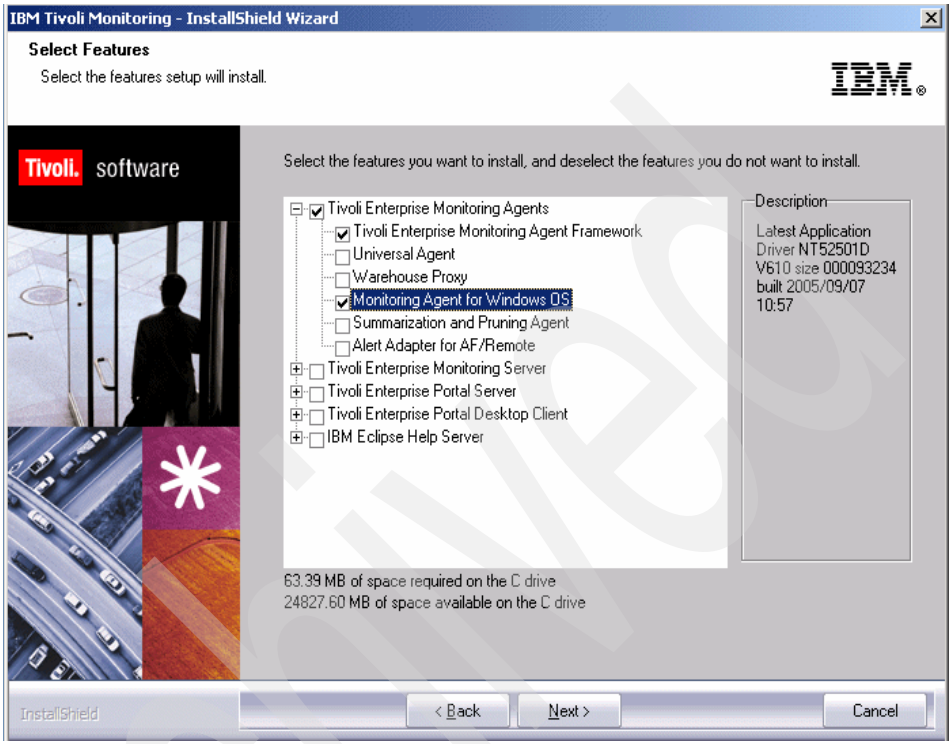

Figure 3-31 Monitoring agents to be installed

8. Click **Next** on the Agent Deploy window. Do not select any agents.

9. Type a program folder to use in your Start menu and click **Next**. The default folder is IBM Tivoli Monitoring, as shown in Figure 3-32.

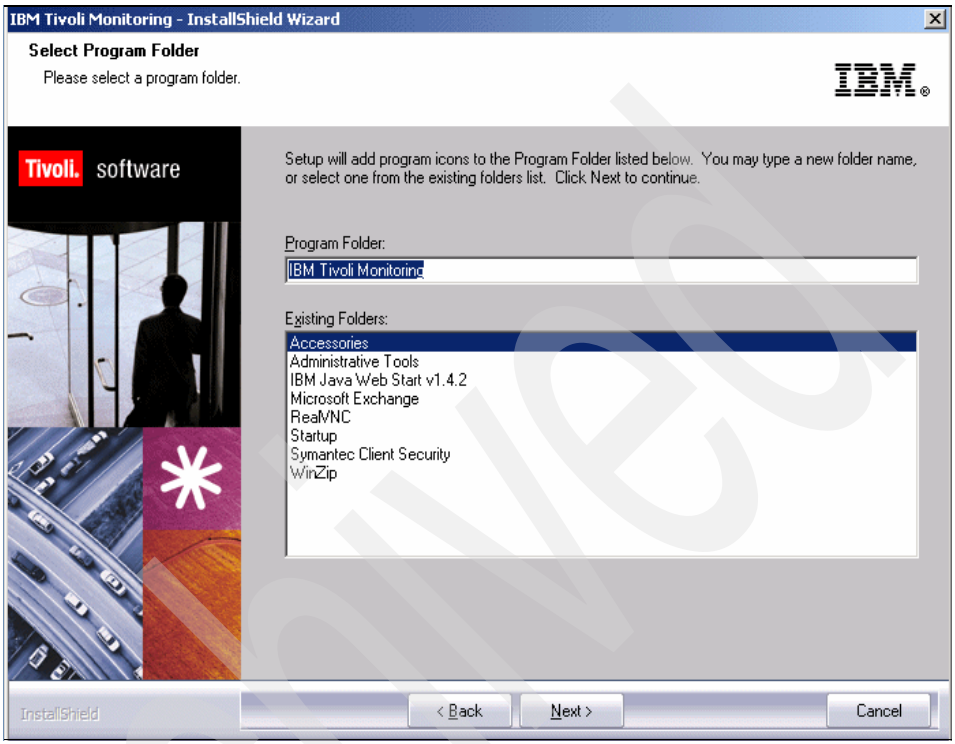

Figure 3-32 IBM Tivoli Monitoring 6.1 program folder

10. Review the installation summary details. This summary identifies what you are installing and where you have chosen to install (Figure 3-33). Click **Next** to begin the installation of components.

    After the components are installed and the configuration environment is initialized (indicated by a pop-up window), a configuration window is displayed. Click **Next**.

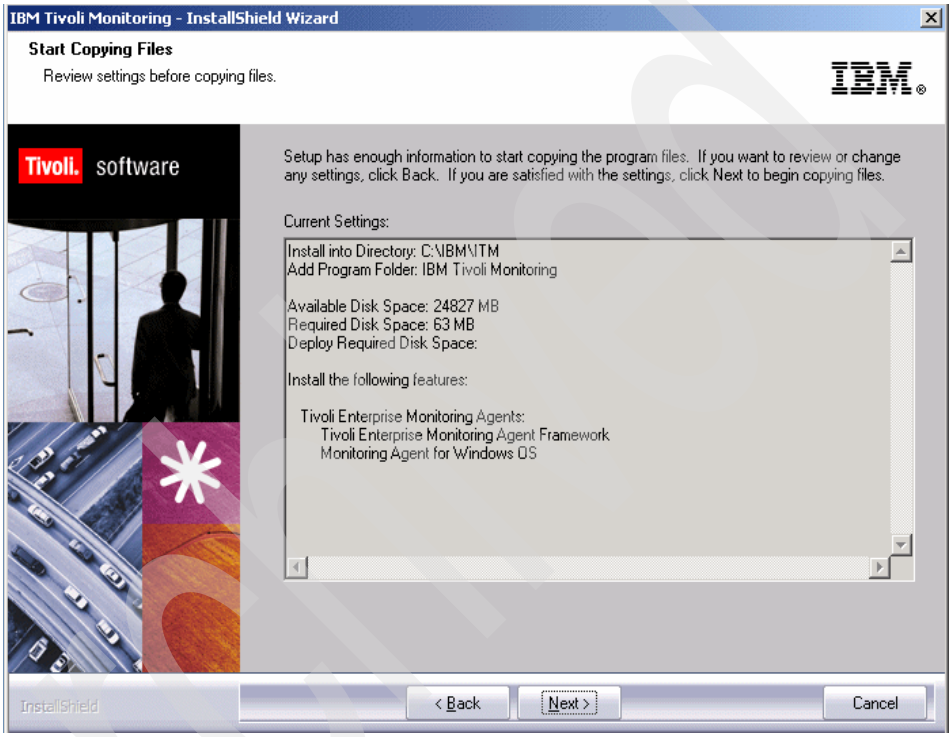

Figure 3-33 Installation summary details

11. Configure the default values for your agent (Figure 3-34). Click **Next**.

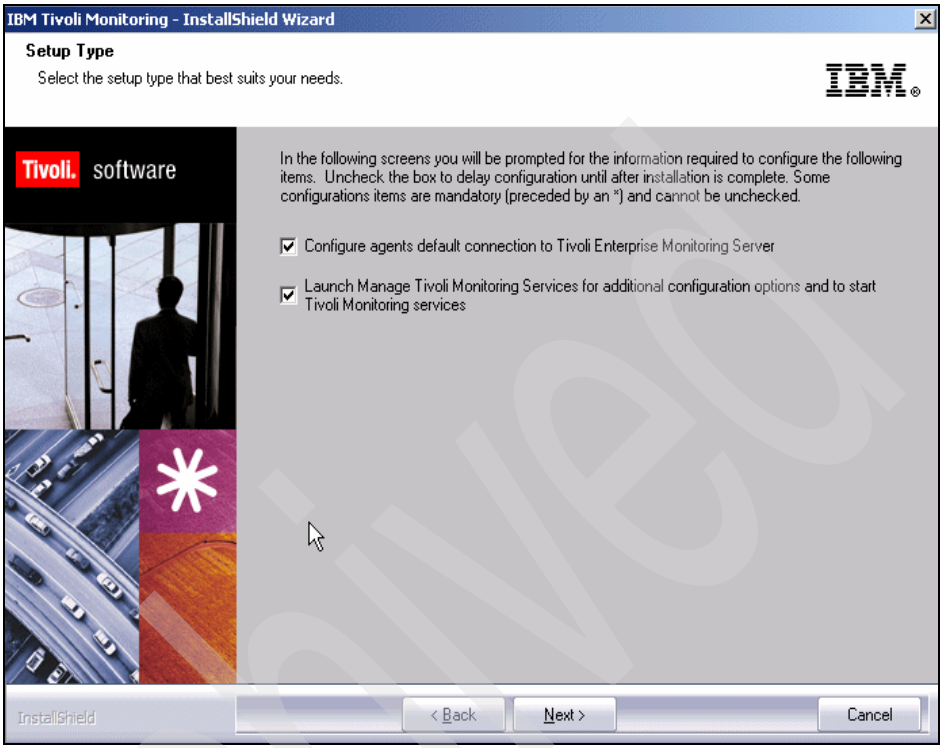

Figure 3-34 Configuration option choice

12. Specify the default values for any IBM Tivoli Monitoring agent to use when they communicate with the monitoring server.

    a. If the agent must cross a firewall to access the monitoring server, select **Connection must pass through firewall**.

    b. Identify the type of protocol that the agent uses to communicate with the monitoring server. Your choices are: 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 you have identified as Protocol 1 fails, Protocol 2 will be used. Click **OK**.

       Figure 3-34 on page 144 shows an example of the protocol communication to be used to communicate with TEMS.

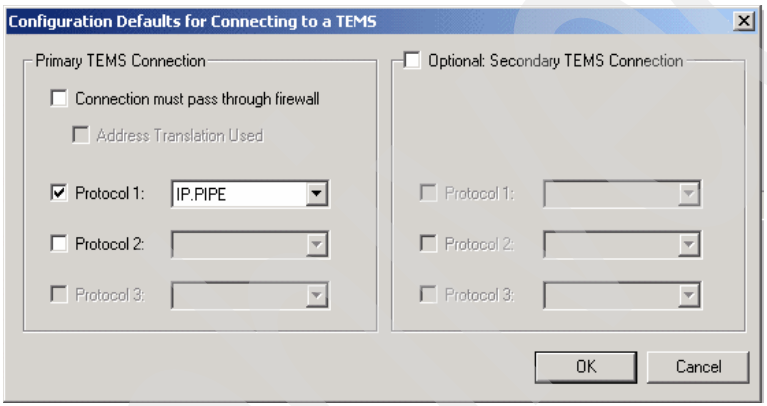

Figure 3-35 Agent communication protocols

13. Complete the fields to define the communications between agents and the monitoring server. Figure 3-36 shows the primary TEMS the agent will be connected to.

    If you have defined more than one TEMS, a second window will open requesting the configuration of the secondary TEMS host name.

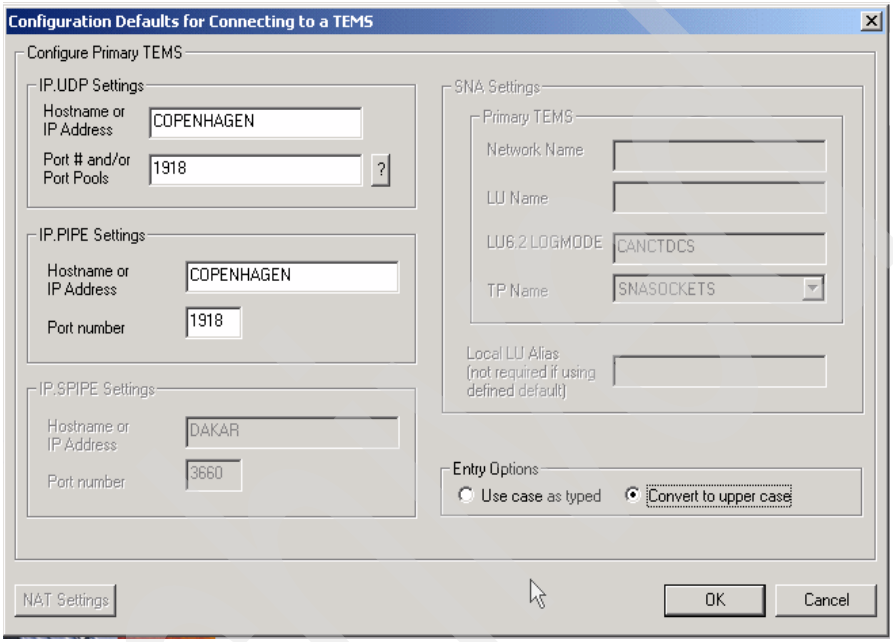

Figure 3-36 Agent's TEMS configuration

14. Click **Finish** to complete the installation.

15. Open the **Manage Tivoli Monitoring Services** utility to see whether the monitoring agent has been configured and started as shown in Figure 3-37. If you see `Yes` in the Configured column, the agent has been configured and started during the installation process.

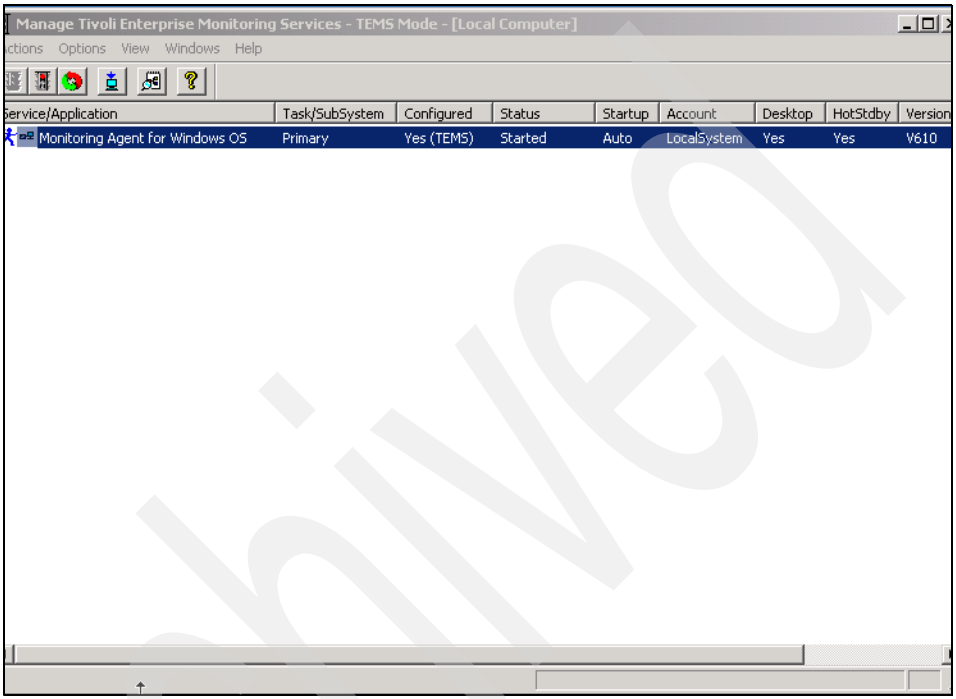

Figure 3-37 Tivoli monitoring services console

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

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

Installing TEMA on an OS/400 server

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

- During installation, you are required to know whether English is the primary language of your iSeries™ system. To determine this, complete the procedure in the next section, “Determining the primary language of your iSeries system.”
- If you are using TCP/IP for network communications, verify that your TCP/IP network services are configured to return the fully qualified host name of the computer where you will install the monitoring agent as described in “Verifying the TCP/IP configuration” on page 6.
- If you have a previous version of a Candle Monitoring Agent installed, delete it as in “Deleting previous versions of the monitoring agent” on page 7.

Determining the primary language of your iSeries system

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

1. Log on onto your system as user QSECOFR.
2. From an i5/OS command line, enter this command:

   ```
   GO LICPGM
   ```

   See Figure 3-38.

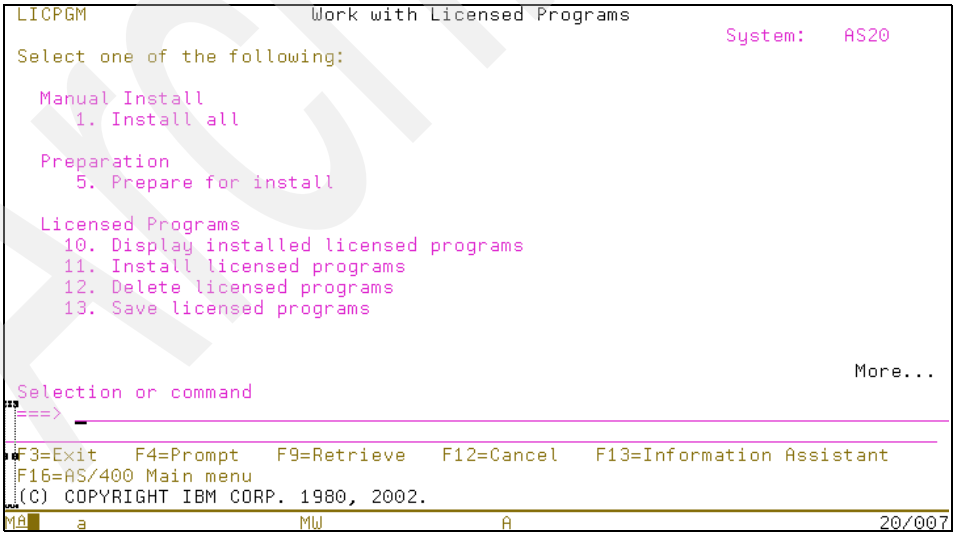

Figure 3-38 Main OS/400 Menu window

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

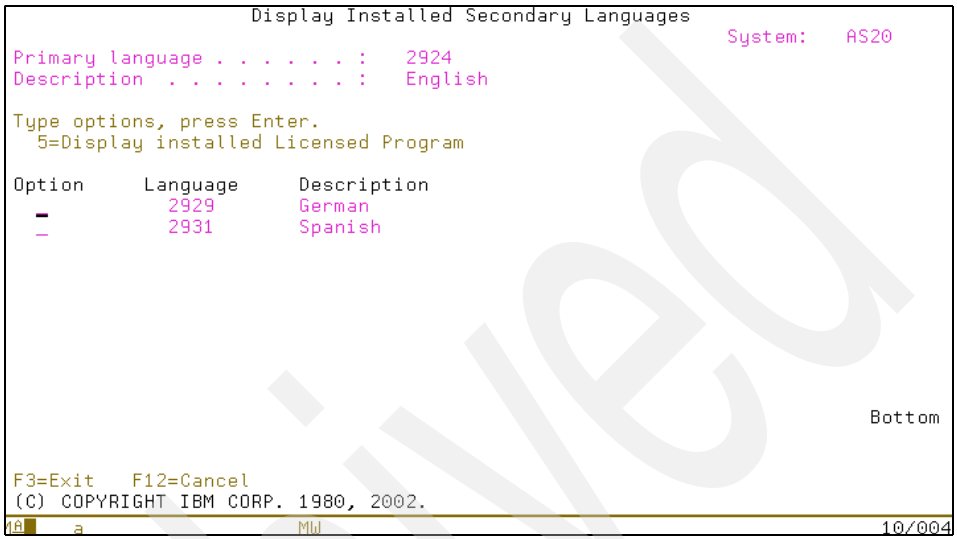

Figure 3-39 Primary language OS/400 definition window

Verifying the TCP/IP configuration

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

Required authorization role is *IOSYSCFG.

1. From an i5/OS command line, enter the following command:

   ```
   CFGTCP
   ```

2. Select **Work with TCP/IP host tables entries: option 10**.
3. Confirm that the first entry in the Host Name column is the fully qualified host name that is associated with the IP address of the iSeries computer where you plan to install the monitoring agent (Figure 3-40 on page 150). If it is not, change the entry to the fully qualified host name.

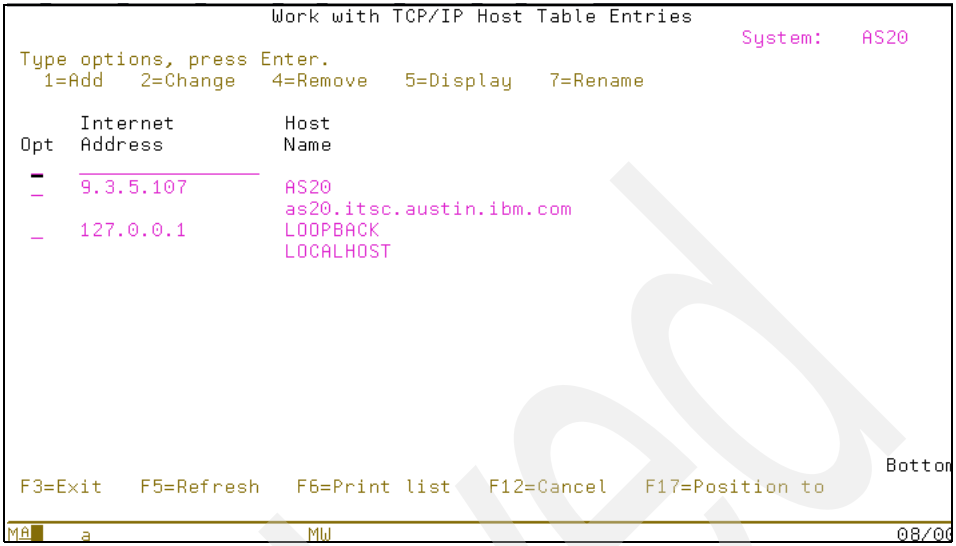

Figure 3-40 OS/400 TCP/IP configuration panel

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

Installing the monitoring agent

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

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

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

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

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

1. From an i5/OS command line, ensure that the QALWOBJRST system value is set to *ALL. To do this, follow these steps:
   a. Enter the following command:

      ```
      WRKSYSVAL QALWOBJRST
      ```

   b. Select **5** (Display) and verify that the value is set to *ALL.
   c. Press Enter to continue.
   d. If the value of QALWOBJRST is set to *ALL, skip to step 3.
      If the value of QALWOBJRST is not set to *ALL, make note of the values and go to step 2.
2. If the value of QALWOBJRST is not set to *ALL, follow these steps:
   a. On the Work with System Values window, enter 2 to change the values.
   b. On the Change System Value window, change the existing values to *ALL and press Enter.
   c. Press F3.
3. From an i5/OS command line, enter the following command to create an i5/OS CCCINST library for the Monitoring Agent for i5/OS installation if this library does not already exist:

   ```
   CRTLIB LIB(CCCINST)
   ```

4. Enter the following command to create a save file in the CCCINST library for the Monitoring Agent for i5/OS:

   ```
   CRTSAVF CCCINST/A4520CMA TEXT('ITM 61 i5/OS')
   ```

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

5. Transfer the software for the Monitoring Agent for i5/OS to the target iSeries computer.

   On a Windows PC, follow these steps:

   a. Insert the IBM Tivoli Monitoring 6.1 product CD into the PC CD-ROM drive.

b. Enter the following command to create a work folder:

```
WRKFLR
```

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

```
A4FLR
```

d. Enter the following command:

```
WRKLNK QOPT
```

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

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

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

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

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

where *volume_id* is the volume ID of the CD-ROM drive from step 5e.

h. Enter the following command to start an FTP session:

```
ftp computer_name
```

computer_name is the name of the target i5/OS computer.

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

```
binary
```

j. Enter the following command:

```
NAMEFMT 1
```

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

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

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

6. From an i5/OS command line, install the software for the Monitoring Agent for i5/OS:

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

```
RSTLICPGM LICPGM(0KA4610) DEV(*SAVF) SAVF(CCCINST/A4520CMA)
```

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

```
RSTLICPGM LICPGM(0KA4610) DEV(*SAVF) RSTOBJ(*PGM)
SAVF(CCCINST/A4520CMA)

RSTLICPGM LICPGM(0KA4610) DEV(*SAVF) RSTOBJ(*LNG) LNG(2924)
SAVF(CCCINST/A4520CMA) LNGLIB(QKA4LNG)
```

7. If you plan to install other monitoring agents, leave the value of QALWOBJRST set to *ALL until you are finished. If you do not plan to install other monitoring agents, change the value of QALWOBJRST to the values you recorded in 1d on page 151.
8. Optional: Enter the following command to delete the installation library, which is no longer needed:

   ```
   DLTLIB CCCINST
   ```

9. Optional for an iSeries computer: Delete the A4520CMA.SAV file from your folder. Follow these steps:
   a. Enter the following command:

      ```
      WRKDOC FLR(A4FLR)
      ```

   b. Enter 4 for the A4520CMA.SAV file.
   c. Press Enter to return to the command line.
   d. Enter the following command to delete the installation folder:

      ```
      WRKFLR
      ```

   e. Enter 4 for the A4FLR folder.
   f. Press F3 to return to the command line.

Configuring the Monitoring Agent for i5/OS

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

1. From an i5/OS command line, enter the following command:

   ```
   GO OMA
   ```

2. Enter **4** (Configure Tivoli Monitoring: i5/OS Agent). The Config i5/OS Monitoring Agent (CFGOMA) window appears.
3. Enter your site's values for the configuration parameters as shown in Figure 3-41 on page 154.

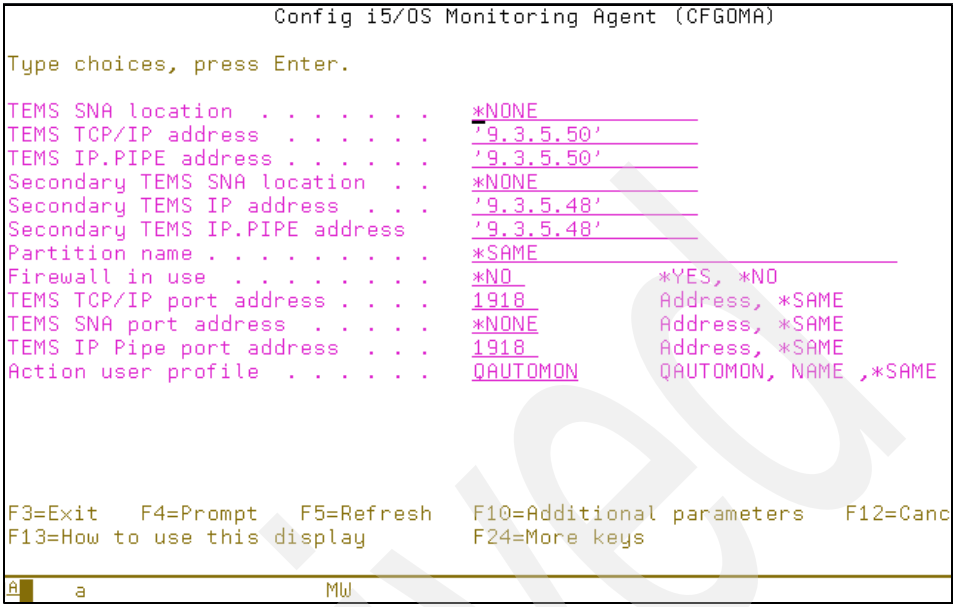

Figure 3-41 Configuring the monitoring agent

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

   – KA4_JOB_DATA_INTERVAL=15
   – KA4_IOP_DATA_INTERVAL=30
   – KA4_DISK_DATA_INTERVAL=30
   – KA4_POOL_DATA_INTERVAL=15
   – KA4_COMM_DATA_INTERVAL=60

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

   – Disk and IOP-related data require a minimum of 30 seconds between collection intervals.
   – Communication-related data requires a minimum of 60 seconds between collection intervals.
   – Collect job-related data as infrequently as possible to minimize the impact on system performance.
   – The i5/OS collection services performance data collector supports data collection at one-minute intervals, not at two-minute or four-minute intervals. Therefore, when using the API and requesting data at

two-minute or four-minute intervals, the data is collected at one-minute intervals, but reported back every two or four minutes.

5. Optional: Customize the time interval for custom situations by changing the value of the following configuration variable in the KMSPARM(KBBEV) file, which is listed with its default value:

```
KA4_COMM_SIT_INTERVAL=3600
```

Note: Custom situations created using APPN Topology or communication attributes use the time interval specified by the KA4_COMM_SIT_INTERVAL configuration variable. Change the value of this configuration variable if you want communication-related alerts to be raised at a different interval. The default interval is set to 3600 to prevent overloading the monitoring agent, because these custom situations are also created as a workaround for a known problem of agent failure when running consecutive APPN reports or running a situation after running an APPN report. These situations might be continuously running and based on events and can overload the monitoring agent when alerting for these conditions.

Starting the monitoring agent

The following steps show how to start the Monitoring Agent for i5/OS.

Background information

When the Monitoring Agent for i5/OS is started, you can use the associated CLI commands. Table 3-7 shows the group profiles that are authorized to these commands by default when the Monitoring Agent for i5/OS is first installed. A check mark in a column indicates that users associated with that group profile can use the command.

*Table 3-7 Commands owned by QSYS with *PUBLIC *CHANGE*

Command	QSRV	QSRVBAS	QSYSOPR	QPGMR
CFGOMA	√			
DSPOMALOG	√	√	√	√
ENDOMA	√		√	
STROMA	√		√	

To determine which group profile a user is associated with, use this command:

```
Display User Profile (DSPUSRPRF)
```

The group profile to which the user is associated is listed in the group profile field.

Required authorization role

*USER or, in some cases, *JOBCTL special authority if authorities for QAUTOMON were changed after installation.

Starting the agent

1. From an i5/OS, enter the following command:

   ```
   GO OMA
   ```

   This opens the window in Figure 3-42.

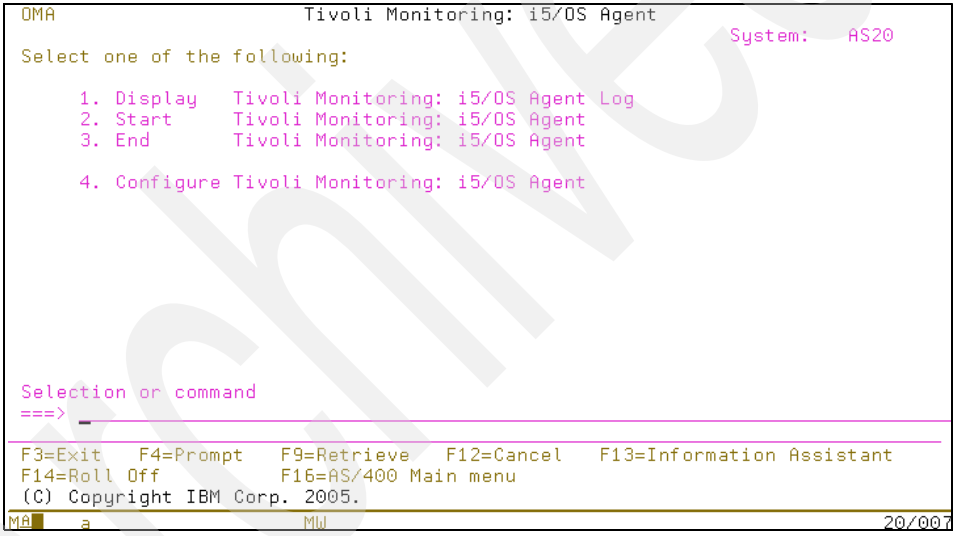

Figure 3-42 Monitoring agent configuration window

2. Enter 2 (Start Tivoli Monitoring: i5/OS Agent). The greater-than character (>) preceding option 2 indicates that the monitoring agent is not started. When the monitoring agent is started the greater-than character (>) is not displayed.

Important: If you did not seed the hub and Remote TEMS during their installation with this type of application (i5/OS), you must do it before the agent can be up and running properly. By default i5/OS is selected for seeding during TEMS installation. You can verify the supported application by using the **`cinfo`** command on the Hub and Remote TEMS.

Note: Use the same procedure to stop the monitoring agent, selecting the option 3.

Deploying TEMA from TEPS

To deploy a monitoring agent through the portal, you first have to deploy the OS monitoring agent on the system. Then you will be able to deploy any other agent from the TEP.

Note: You also must install the bundles on the server where the monitoring agent is being deployed.

Use the following steps to deploy an agent through the portal GUI:

1. Open the Tivoli Enterprise Portal.
2. In the Navigation tree, navigate to the computer where you want to deploy the agent.
3. Right-click the computer and click **Add Managed System**.
4. Select the agent that you want to deploy and click **OK**.
5. Select the configuration fields required for the agent. For information about these fields, see the configuration documentation for the agent that you are deploying.
6. Click **Finish**.
7. If the computer where you are deploying the agent already has a version of that agent installed, you can either stop the deployment or, if the existing version is older than the version you are deploying, specify to replace the existing agent with this new agent. To replace the existing agent, click **Yes**.
8. Click **Finish** on the message that tells you that deployment was successful.

3.2.9 Deploying TEMA from the command line interface

In many cases you must create a node (install an OS agent) from the command line. Before beginning the procedure, be sure that the packages are already in the depot server where you will execute the commands.

Deploying a Windows OS agent from a Remote TEMS using command line

1. Check whether the target platform bundles are already installed in the server. Execute the following command:

   ```
   tacmd login -s tems_hostname -u tems_user -p tems_password
   ```

   In this command:

   – *tems_hostame* is the host name where you want to initiate the installation.

   – *tems_user* is the user ID on the tems_hostname.

   – *tems_password* is the tems_hostname password.

2. Execute the following command:

   ```
   tacmd listBundles
   ```

3. If the bundles are not present, execute the following commands to add them on the server:

   ```
   cd image_dir
   ```

   image_dir is the directory where you untar the IBM Tivoli Monitoring 6.1 codes.

   ```
   tacmd addBundles -i bundles_path
   ```

4. Deploy the agent on the targeted server executing the following command:

   ```
   tacmd createNode -h server -u user -w password -d target_directory
   ```

   Table 3-8 on page 182 installs the Window agent on london from copenhagen using the -p option to set the agent properties.

Example 3-8 Deploying the agent on the targeted server

```
C:\>tacmd createNode  -h london -u Administrator -w **** -d c:/IBM/ITM -p
KEY=IBMTivoliMonitoringEncryptionKey PROTOCOL1=IP.PIPE PROTOCOL2=IP.UDP
PORT=1918 SERVER=COPENHAGEN BSERVER=EDINBURG BPROTOCOL1=IP.UDP
PROTOCOL2=IP.PIPE PORT=1918
KUICCN001I Initializing required services...
KUICCN039I Attempting to connect to host london ...
KUICCN050I Distributing file 203 of 203 (85.9 MB / 85.9 MB)...
```

```
KUICCN002I Beginning the installation and configuration process...

KUICCN057I The node creation on host london was successful.

KUICCN065I The node creation operation was a success.
```

Deploying an application agent from a Remote TEMS using command line

The same procedure can be used to install a monitored agent using the addSystem option instead of createNode. The following command performs this operation:

```
tacmd addSystem -t type -n node_name -p SECTION.NAME=value ....
```

Example 3-9 shows how to deploy a Microsoft SQL Server agent on a nice server to monitor the wproxy database instance.

Example 3-9 Deploying an application agent

```
tacmd addSystem -t OQ -n Primary:nice:NT -p DBSETTINGS.db_sid=MyServer
DBSETTINGS.db_login=sa DBSETTINGS.db_password=sapwd
"DBSETTINGS.db_home=c:\Program Files\Microsoft SQL Server\MSSQL"
"DBSETTINGS.db_errorlog=C:\Program Files\Microsoft SQL
Server\MSSQL\LOG\ERRORLOG" INSTANCE=wproxy
```

Starting the TEMA from the Remote TEMS

After the agent is installed, start it by executing the following procedure:

1. Log on to the agent Remote TEMS by executing the following command:

   ```
   tacmd login -s remote_tems -u user -p password
   ```

2. When you are logged in, execute the command to start the agent:

   ```
   tacmd startAgent -n hostname -t pc
   ```

   pc is the product code (*lz* for Linux, *nt* for Windows, *um* for Universal Agent).

3.2.10 Installing a new managed system: Microsoft Exchange example

We use the Microsoft Exchange Server deployment as an example of deploying a new managed system on a TEMS environment.

Installing the OS Agent

First, install the OS Agent on the Microsoft Exchange Server. (Refer to “Tivoli Enterprise Monitoring Agent” on page 129.) You can install the OS Agent either locally or remotely using **`tacmd createNode`** on the command line.

Installing the application agent

After you install the OS Agent, install the Microsoft Exchange Server Agent. Refer to the procedure in “Installing TEMA on a Windows server” on page 136 if you want to install the agent locally, or “Deploying TEMA from TEPS” on page 157 if you want to deploy the agent from the TEPS. If you want to deploy the agent from a TEMS command line interface, refer to “Deploying an application agent from a Remote TEMS using command line” on page 159.

Installing support for the agent being deployed

Install the support on the Hub TEMS, the Remote TEMS, and the TEPS.

Note: If you fail to install the support (seed) for the agent, you will be able to see the agent on the TEP, but you will not see any data when you click on the attribute group, only a message saying that the request has failed.

3.2.11 Tivoli Enterprise Portal (TEP)

There are two ways to access the Tivoli Enterprise Portal: browser and desktop client. The browser-based client has two main advantages: There is no need to install an updated client if a newer version is available; the browser client will always be at the latest level available from the server. Also, you can store links to some of your favorite workspaces as you would store any other link in a browser. The only downside to the browser-based client is the fact that you lose desktop real estate taken up by the browser’s headers. From a functional point of view, there are no differences between the two.

Tip: IBM Tivoli Monitoring 6.1 requires IBM Java V 1.4.2 to be installed on all systems where the TEP browser client will be initiated. One likely error that signifies this is: `KFWITM215E - unable to process login request.`

Installing Tivoli desktop client on a Windows machine

Use the following steps to install the desktop client for Tivoli Enterprise Portal:

1. On the computer where you want to install the desktop client, start the installation wizard by launching the **setup.exe** file from the installation media.
2. Click **Next** on the welcome window.
3. Accept the software license by clicking **Accept**.
4. Read the information regarding potentially missing prerequisites and click **Next**.
5. Specify the directory where you want to install the portal software and accompanying files. The default location is C:\IBM\ITM. Click **Next**.
6. Type an encryption key to use. This key should be the same as the one that was used during the installation of the portal server to which the client will connect. Click **Next** then **OK** to confirm the encryption key.
7. Select **Tivoli Enterprise Portal client**.
8. If you want to view IBM Tivoli Enterprise Console events through the Tivoli Enterprise Portal, expand **Tivoli Enterprise Portal client** and ensure that **Tivoli Enterprise Console GUI Integration** is selected.
9. Click **Next**.
10. Click **Next** without selecting any agents to deploy.
11. Specify the program folder name and click **Next**.
12. Confirm the installation details and click **Next** to start the installation. After the installation is complete, a configuration window is displayed.
13. Click **Next** to configure the connection to the portal server, the connection to the monitoring server, and to launch Manage Tivoli Monitoring Services.
14. Type the host name of the portal server and click **OK**.
15. Configure the default connection to the monitoring server:
    a. If the agent must cross a firewall to access the monitoring server, select **Connection must pass through firewall**.
    b. Identify the type of protocol that the agent uses to communicate with the hub monitoring server. Click **OK**.
16. Complete the rest of the fields (refer to Table 3-5 on page 111) for the monitoring server, and click **Finish** to complete your installation.

Installing the desktop client on a Linux machine

Use the following steps to install and configure the portal desktop client on a Linux computer.

Installing the desktop client

Use the following steps to install the portal server and desktop client:

1. In the directory where you extracted the installation files, run the following command:

   ```
   ./install.sh
   ```

2. When prompted for the IBM Tivoli Monitoring home directory, press Enter to accept the default (opt/IBM/ITM) or change the directory as per your needs.

3. Type `y` to create this directory when prompted. If the directory already exists, you will receive the following type of message:

   ```
   CANDLEHOME directory "/opt/IBM/ITM" already exists.
   OK to use it [ y or n; "y" is default ]?  y
   ```

   Select option `1` when the message in Example 3-10 is displayed.

Example 3-10 Selecting install options

```
Select one of the following:
1) Install products via command line.
2) Install products to depot via command line.
3) Exit install.
Please enter a valid number:
```

4. Type 1.

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

6. Press Enter to display the agreement.

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

8. Type the encryption key that was used during the installation of the portal server to which the client will connect, and press Enter. This displays a numbered list of available operating systems. If you have already installed other IBM Tivoli Monitoring 6.1 components on that machine, the key should already be defined and you will receive the following message

   ```
   runGSkit       :  Keyfile.kdb already exists, skipping keyfile and
   certificate creation.
   ```

9. Press Enter to accept the OS type; the default value is your current operating system. If not, type the number for the operating system that you are installing on.

10. Type `y` to confirm the operating system and press Enter. This displays a numbered list of available components.
11. A list of products are presented as shown in Example 3-11. Type the number corresponding to the TEP Desktop client: `6`.

Example 3-11 List of products

```
The following products are available for installation:

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

12. Type `y` to confirm the installation. The installation begins.
13. After all of the components are installed, you are asked whether you want to install components for a different operating system. Type `n` and press Enter. Installation is complete. You will see the message in Example 3-12.

Example 3-12 Installation complete message

```
Installation step complete.

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

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

The next step is to configure the TEP desktop client on the server.

Configuring the portal desktop client on Linux

Use the following steps to configure the desktop client on Linux:

1. At the command line change to the opt/IBM/ITM/bin directory.
2. Run the following command:

   ```
   ./CandleConfig -A cj
   ```

3. Type your TEP instance and press Enter, or just press Enter to use the default instance name. We use `tep_ankara`, ankara being the server name where we are installing TEP.

4. Type the host name for the portal server and press Enter.
5. Type your browser path directory and press Enter.
6. Press Enter when you are asked whether you want to use HTTP Proxy support. The default value is no. The desktop client is now configured. The next step is to start the portal server and portal desktop client.

   Example 3-13 shows the TEP desktop configuration on server ankara.

Example 3-13 TEP desktop configuration

```
[root@ankara bin]# ./CandleConfig -A cj
CandleConfig        :  installer level  400 / 100.
CandleConfig        :  running li6243 jre.
Agent configuration started...
Enter TEP Instance Name(Default is: none): tep_ankara
TEP Server Hostname(Default is: none): berlin
Browser Path(Default is: /usr/bin/mozilla):
HTTP Proxy Support? [YES or NO] (Default is: no):
Agent configuration completed...
```

7. Seed the TEMS with the following command line:

   ```
   ./CandleSeed -t tems_name pc
   ```

   where pc = cj
8. Start the agent executing the following command:

   ```
   ./itmcmd agent start cj
   ```

3.2.12 Warehouse Proxy installation and configuration

This section describes the steps for installing and configuring a Warehouse Proxy agent. The Tivoli Data Warehouse needs a relational database to store the historical data. DB2 UDB is the preferred database, but MS SQL and Oracle are also supported. The product ships with a copy of DB2 UDB.

Preinstallation configuration

Before initiating the Warehouse Proxy agent installation and configuration, you must create a Windows user.

Note: ITMUser is default user used in the Warehouse Proxy agent.

Creating a Windows user

Use the following steps to create a Windows user called ITMUser; remember that the database used for this book is DB2 so if you use another database, the configuration can be different:

1. Open the Computer Management window.
2. In the navigation pane of the Computer Management window, expand **Local Users** and **Groups**.
3. Right-click the **Users** folder and click **New User**.
4. Type `ITMUser` in the User Name field.
5. Type `marathOn` in the Password field. Type the password again in the Confirm password field to confirm it.

   Note: You can set a different user and password if you prefer.

6. Clear the **User must change password at next logon** check box.
7. Click **Create** to create the user.
8. Click **Close** to close the window.
9. Click the **Groups** folder.
10. Double-click **DB2ADMNS** in the right pane of the window.

    Note: DB2ADMNS group is created with the DB2 database installation.

11. Perform the following step if you are using Windows 2003:
    a. Click **Add**.
    b. Type `ITMUser` in the Enter the names to select (examples) field and click **Check Names**.
    c. Click **OK** and then click **OK** again.
12. Perform the following step if you are using Windows 2000:
    a. Click **Add** in the Administrator Properties window.
    b. Locate **ITMUser**, the new user you created, and select it.
    c. Click **Add**.
13. Click **OK** twice to close the Administrator Properties window.
14. Close the Computer Management window.

Important:

1. You must create a database for the IBM Tivoli Monitoring Warehouse proxy if you are using a non-DB2 database or you are using DB2 database on a UNIX server. You also must create an ODBC that points to the database you created to store the data in the datawarehouse proxy.

   Execute the following command to create the wproxy database in your DB2 RDBMS:

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

2. When creating an Oracle or DB2 database the code set must also be utf-8.

Installing the Warehouse Proxy agent

The Warehouse Proxy is used to upload historical data from agents into the Tivoli Enterprise Data Warehouse for historical reporting. As with any other IBM Tivoli Monitoring 6.1 agent, the Warehouse Proxy agent installation follows the same procedure as the one described in “Installing TEMA on a Windows server” on page 136. Warehouse Proxy agent runs only on the Windows platform.

Database configuration and installation prerequisites

Use the following recommendation when installing RDBMS on DB2 or Oracle.

- DB2

  You must be using at least DB2 V8.2 FP10. You need also to set the environment variable DB2CODEPAGE=1208 as a system environment on the Windows box where the Warehouse Proxy is installed.

  You can find the DB2 fix packs at the following address:

  http://www.ibm.com/software/data/db2/udb/support/downloadv8.html

- Oracle

  If you have Oracle 9.2, you must upgrade the ODBC Driver to Version 9.2.0.4. Set the environment variable NLS_LANG=AMERICAN_AMERICA.AL32UTF8 as a system environment on the Windows box where the Warehouse Proxy is installed.

  Site for Oracle ODBC drivers:

  http://www.oracle.com/technology/software/tech/windows/odbc/htdocs/utilsoft.html

Note: IBM plans to provide Warehouse Proxy agent on UNIX and Linux platforms as well, but at GA time only Windows will be supported.

Configuring the Warehouse Proxy agent

The next step after installing the Warehouse Proxy is to configure it to connect to the database in order to insert and retrieve data from the database. The following steps show 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** when you see the message shown in Figure 3-43.

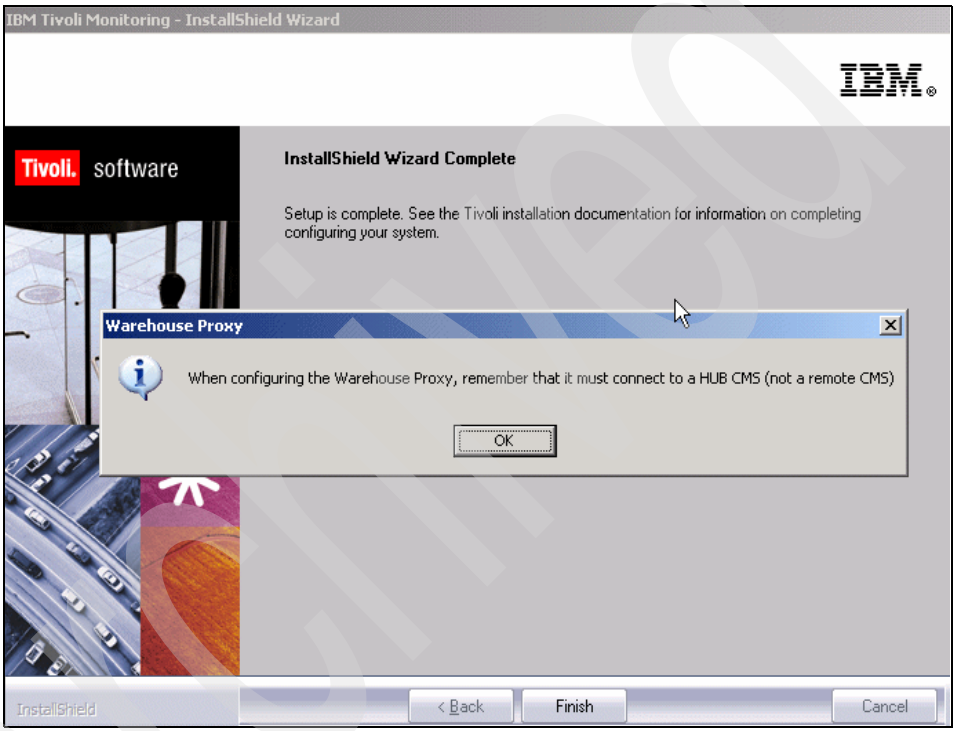

Figure 3-43 Informational window display

3. Configure the protocol communication between the TEMS and the Warehouse Proxy as shown in Figure 3-44 and click **OK**.

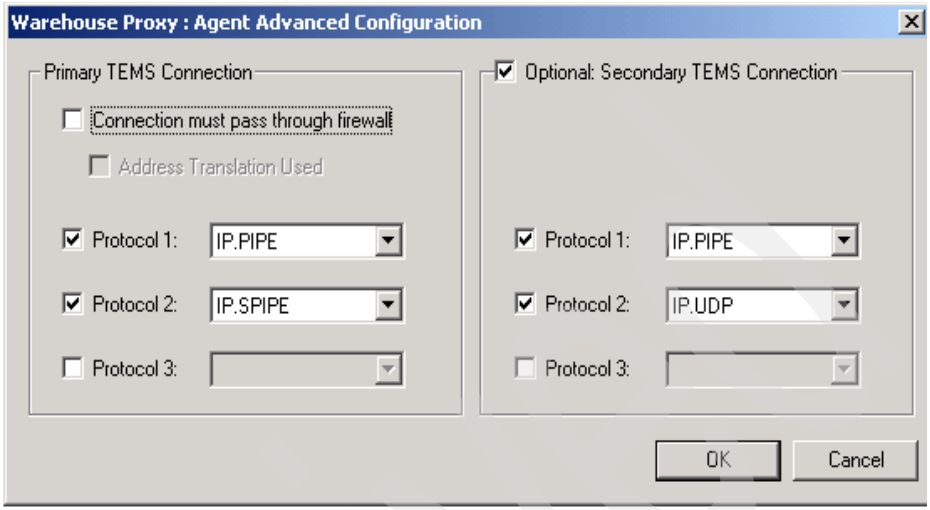

Figure 3-44 Warehouse Proxy agent communication protocol configuration

4. Configure the Hub TEMS host name and the ports where the Warehouse Proxy will connect and click **OK**.

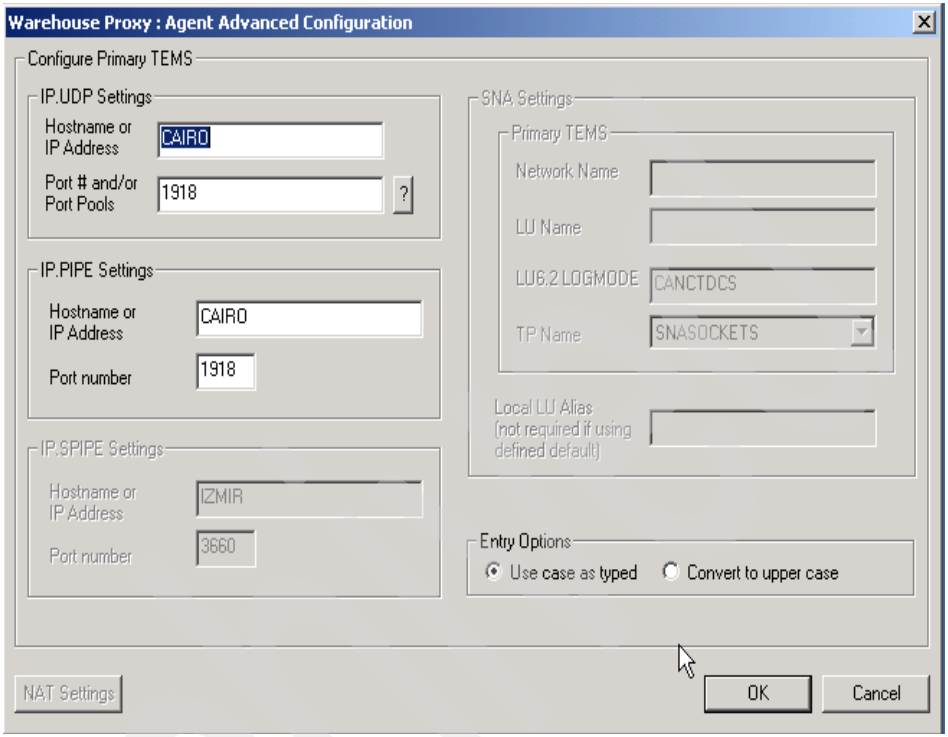

Figure 3-45 Warehouse Proxy agent Hub TEMS and port configuration

5. Click **OK** when you see the window shown in Figure 3-46.

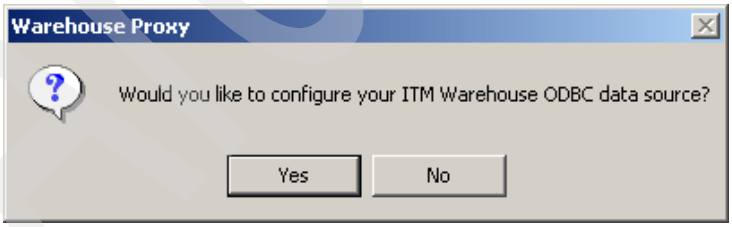

Figure 3-46 ITM Warehouse ODBC configuration confirmation window

6. Select the database the Warehouse Proxy agent you will use (Figure 3-47).

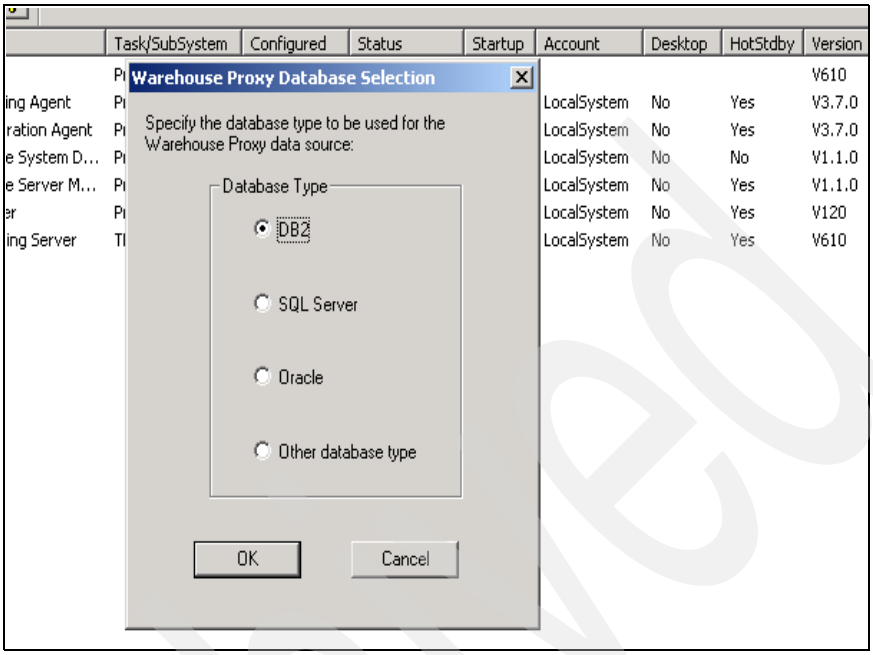

Figure 3-47 Database selection for Warehouse Proxy configuration

7. Fill in the following fields (Figure 3-50 on page 172) then click **OK**:

Data Source Name	Leave as ITM Warehouse.
Database Name	The name of the database the Warehouse Proxy agent will use to store the data.
Admin User ID	The database user administrator created during database installation (default is db2admin for DB2).
Admin Password	The user database administrator password.
Database User ID	The user ID that will own the table made to store warehouse data. This user must be created on the OS first; refer to “Creating a Windows user” on page 165. The default user is ITMUser.
Database Password	The password of the Database user ID.

Note: After this step completed, the database and the associated tables will be created on your database.

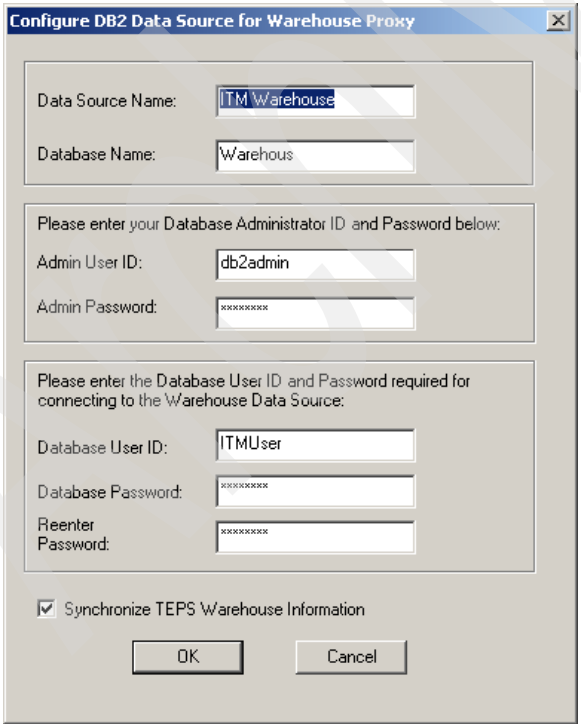

Figure 3-48 Data source configuration window for the Warehouse Proxy

8. Click **OK** on the next pop-up window stating that the Data Warehouse was successfully completed, as shown on Figure 3-49.

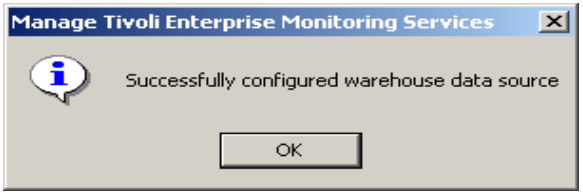

Figure 3-49 Warehouse configuration status message

9. Click **Yes** on the next window (Figure 3-50) to complete the configuration.

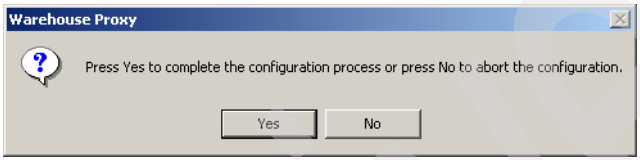

Figure 3-50 Warehouse Proxy database configuration completion

10. Restart the Warehouse Proxy agent by double-clicking on it.

Important:

You can change the default ODBC data source name using the following procedure:

1. Edit the Windows registry:

   ```
   regedit
   ```

2. Find this registry key:

   ```
   HKEY_LOCAL_MACHINE\SOFTWARE\CANDLE\KHD\Ver610\Primary\Environment
   ```

3. Double-click the string **ODBCDATASOURCE** and enter the ODBC data source name of your choice.

3.2.13 Summarization and Pruning agent installation and configuration

The Summarization and Pruning agent is responsible for aggregating historical data and for pruning to the size of the database according to the desired guidelines. This installation is identical to the other agent installation. This section focuses on how to configure your Summarization and Pruning agent.

Installing the Summarization and Pruning agent

Summarization and Pruning agent is similar to any other common agent. To install it, follow the procedure described in “Installing TEMA on a Windows server” on page 136 and use the next section, “Configuring the Summarization and Pruning agent” to make the appropriate configurations.

Configuring the Summarization and Pruning agent

After the Summarization and Pruning agent is installed, configure when and how data will be collected, aggregated, and pruned:

1. From your Windows desktop, click **Start** → **Programs** → **IBM Tivoli Monitoring** → **Manage Tivoli Enterprise Monitoring Services**.

   On a Linux or UNIX system, **cd** to install_dir/bin. Type:

   ```
   ./itmcmd manage
   ```

   Note: For more details about this command, execute this phrase:

   ```
   itmcmd manage ?
   ```

   Or see the *IBM Tivoli Monitoring Installation and Setup Guide*, GC32-9407.

2. Right-click **Summarization and Pruning agent**.

3. Click **Reconfigure** as shown in Figure 3-51.

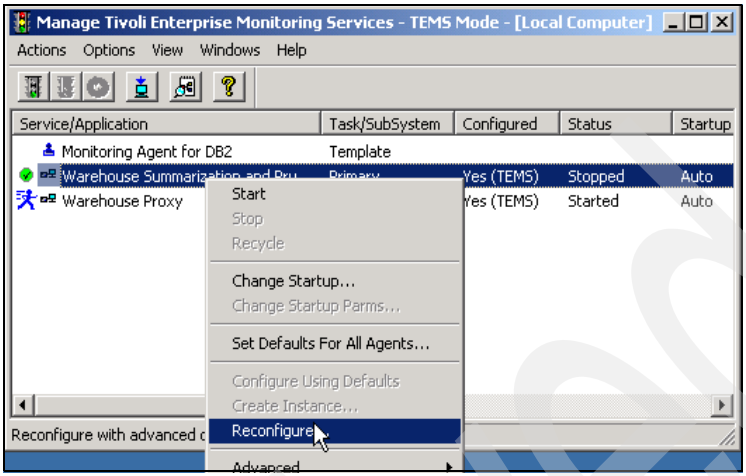

Figure 3-51 Configuring through monitoring console

4. Click **OK** in the Advanced Configuration window (Figure 3-52).

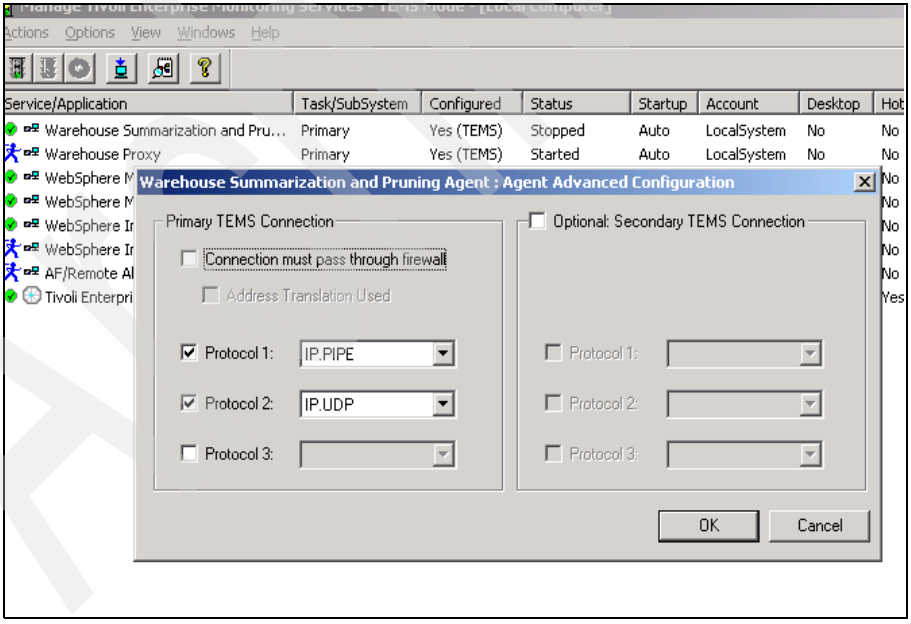

Figure 3-52 Configuring Summarization and Pruning agent connection protocol

5. Click **OK** in the next window.

6. Click **Yes** in the Warehouse Summarization and Pruning agent window to configure the Summarization and Pruning agent.
7. On the Sources tab, enter the Tivoli Data Warehouse database and Tivoli Enterprise Portal server information. Before performing any update, confirm that the default configuration is accurate. If it is not, use the following procedure to update the information:
   a. In the JDBC™ drivers field:
      i. Click **Add** to invoke the file browser window to select your JDBC driver. The default is:

         ```
         DB2: C:\Program Files\IBM\SQLLIB\java\db2java.zip
         ```

         Click **OK** to close the browser and add the JDBC drivers to the list.
      ii. To delete a driver, highlight its entry in the JDBC drivers list and click **Delete**.

      This gives you the ability to collect JDBC drivers to communicate with your Tivoli Data Warehouse database. JDBC drivers are installed separately and each database provides a set of these JDBC drivers.

      Notes:

      - If your Tivoli Data Warehouse database is on UNIX, find the directory where your database is installed and in the jdbc drivers directory, select only the db2jcc.jar and db2java.zip files. For example: <db2installdir>/java/db2jcc.jar and db2java.zip.
      - If your Tivoli Data Warehouse database is on MS SQL Server, install the JDBC drivers from the Microsoft SQL Server Web site. These are the three files that you need:
        - c:\Program Files\Microsoft SQL Server 2000 Driver for JDBC\lib\msbase.jar
        - c:\Program Files\Microsoft SQL Server 2000 Driver for JDBC\lib\mssqlserver.jar
        - c:\Program Files\Microsoft SQL Server 2000 Driver for JDBC\lib\msutil.jarv. In the pull-down list, select the type of database for your Tivoli Data Warehouse.

   b. Enter the Warehouse URL, Driver, Schema, user ID and password.

Important: During the configuration of the Warehouse Proxy, a database user (called ITMUser by default) is created. The user ID that you enter here must match that database user.

c. Click **Test database connection** to ensure you can communicate with your Tivoli Data Warehouse database.

d. Enter the Tivoli Enterprise Portal Server host and port if you do not want to use the defaults.

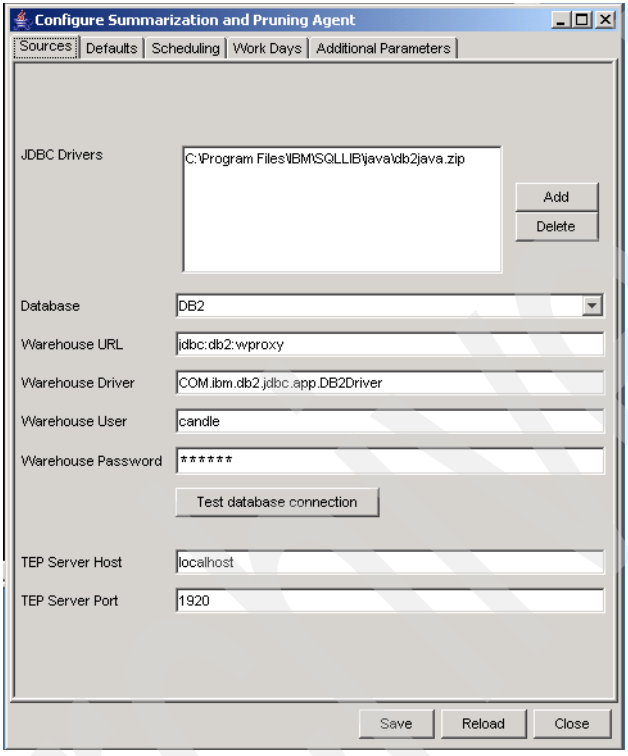

Figure 3-53 Configuring agent TEPS and database connection

8. Click the **Defaults** tab and select the settings for your summarization and pruning information (Figure 3-53 on page 176).

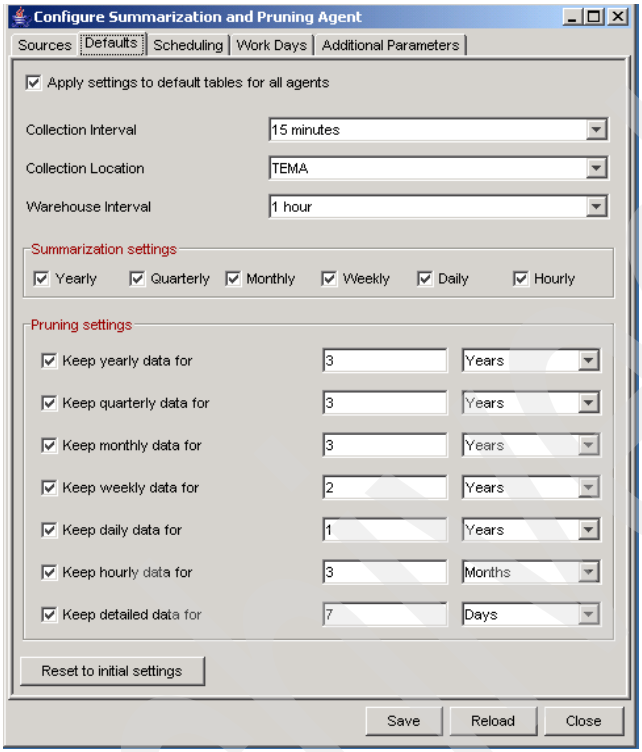

Figure 3-54 Configuring how data will be collected and pruned

- Clicking **Reset** returns all settings in this window to the default settings.
- If you do not want to use the defaults, select the appropriate time periods you want in the Summarization section to change your summarization values.
- To change your Pruning settings:
  i. Select the time periods for the pruning of your data: **Keep yearly data for**, **Keep quarterly data for**, and so on.
  ii. Enter the number of time periods you wish in the next field.
  iii. Select the time period you wish. For example, if you want to prune hourly data when it becomes 30 days old, select Hourly, keep 30 and choose Days as the time period from the drop down list.
- Select **Apply settings to default tables for all agents** to keep the changes you have made.

9. Click the **Scheduling** tab and select the scheduling information (Figure 3-55).
   - Schedule the agent to run every x days.
   - Select the hour of the day that you want the summarization to run. The default is to run every day at 2 a.m.

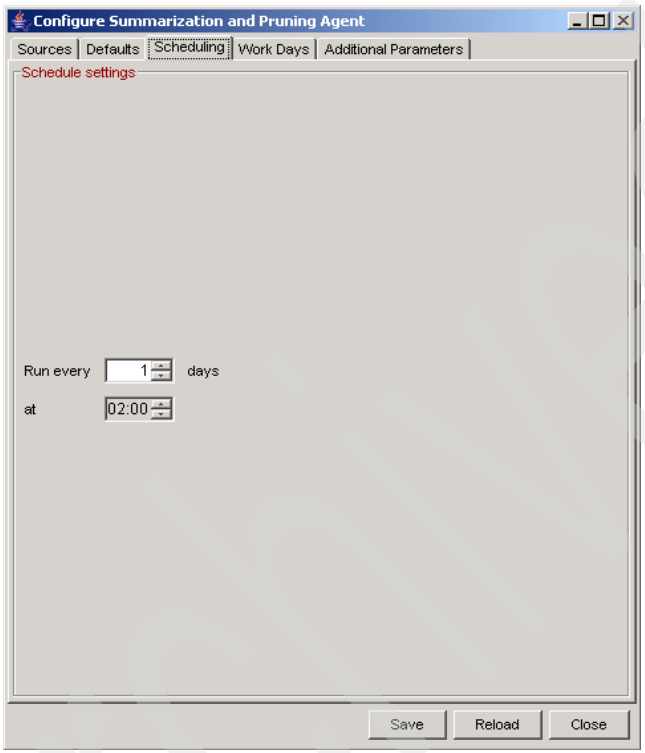

Figure 3-55 Scheduling the data collection and pruning

10. Click the **Work Days** tab (Figure 3-56 on page 179) and specify shift information and vacation settings:
    - Select day the week starts on.
    - If you want to specify shifts, select **Specify shifts**. The default settings for this field are listed in the Peak Shift Hours box on the right side of the window. You can change these settings by selecting the hours you want in the Off Peak Shift Hours box and clicking the right arrow button to add them to the Peak Shift Hours box.

> **Note:** Changing the shift information after data has been summarized can create an inconsistency in the data. Data that has been collected and summarized cannot be recalculated with the new shift values.

– To change your vacation settings, select **Specify vacation days**. If you do not want to set your vacation days, do not select this check box.

  i. Click **Yes** or **No** to count weekends as vacation days.

  ii. Click **Add** to add vacation days, and select the vacation days you want to add from the calendar.

> **Note:** On UNIX or Linux, right-click to select the month and year.

  iii. The days you select appear in the box below the Select vacation days field. If you want to delete any days you have previously chosen, select them and click **Delete** (Figure 3-56**)**.

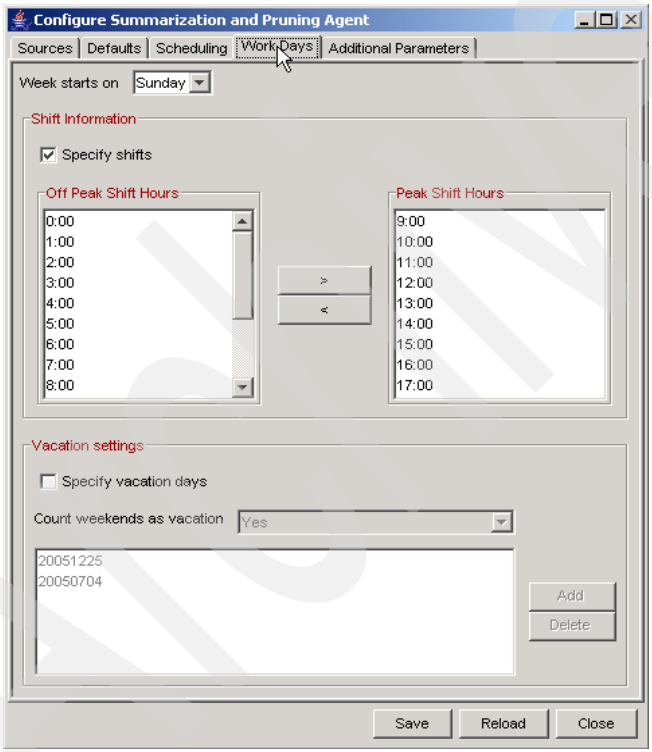

Figure 3-56 Defining shift periods and vacation settings

11. Click the **Additional Parameters** tab (Figure 3-57):

    a. Specify the maximum number of rows that can be deleted in a single database transaction. The values are 1 through n. The default is 1000.

    b. Specify the age of the hourly and daily data you want summarized. Values are 0 through n. The default is 1 for hourly data and 0 for daily data.

    c. Choose the time zone you want to use from the pull-down list. If the Tivoli Data Warehouse and agents that are collecting data are all not in the same time zone, and all the data is stored in the same database, use this option to identify the time zone you want to use.

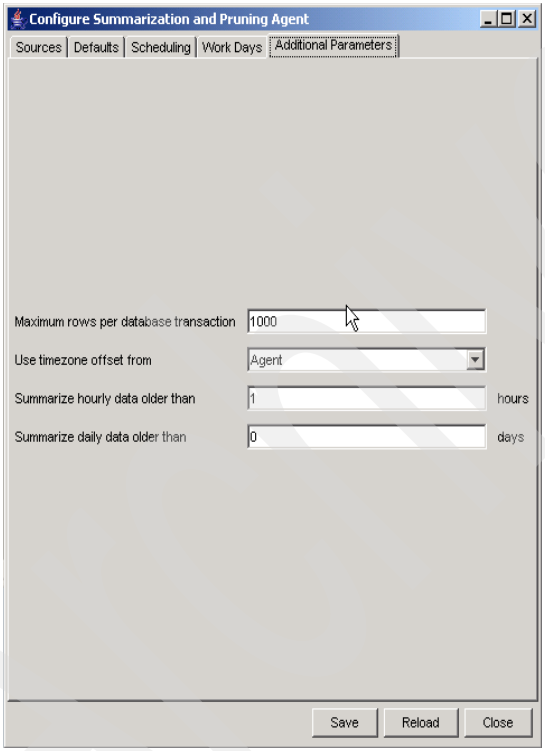

Figure 3-57 Configuring additional parameters

12.Click **Yes** on the next window to save your configuration (Figure 3-58).

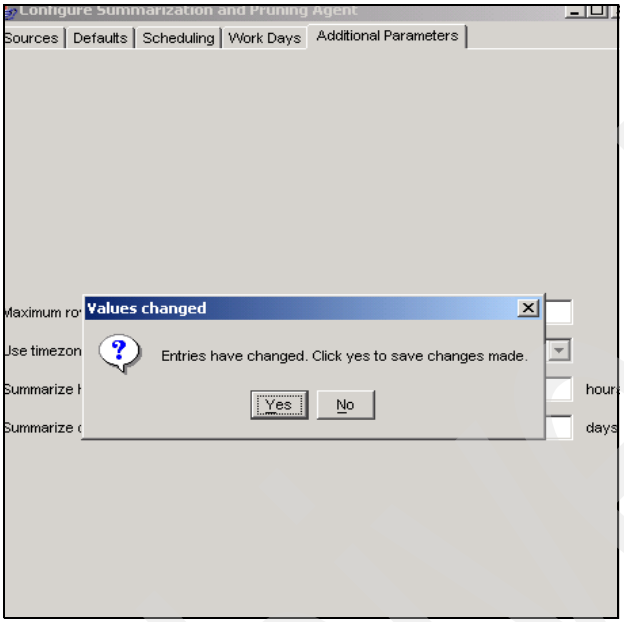

Figure 3-58 Saving the Pruning and Summarization agent configuration

12. The following buttons are visible only on a UNIX or Linux system:

- Click **Save** after you have all your settings correct.
- Click **Reload** to reload the original values.
- Click **Cancel**, at any time, to cancel out of the ConfigureSummarization and Pruning agent window. You are prompted to save any data you have changed.

Changing configuration settings using the History Collection Configuration window in the Tivoli Enterprise Portal

To change the default data summarization, pruning configurations, or both after installing the Summarization and Pruning agent, use the History Collection Configuration window in the Tivoli Enterprise Portal.

3.2.14 Event synchronization installation

Event synchronization components enable IBM Tivoli Monitoring 6.1 to send events to IBM Tivoli Enterprise Console server, as well as IBM Tivoli Monitoring 6.1 users to view events from IBM Tivoli Enterprise Console in the Tivoli Enterprise Portal. Install the IBM Tivoli Enterprise Console on the event server

and configure the TEMS to send events to the IBM Tivoli Enterprise Console server to have those features available. Table 3-8 provides an overview of the steps required to install and configure the IBM Tivoli Enterprise Console.

Table 3-8 TEC event synchronization installation and configuration steps

Step	Reference
1. Gather information required during the installation and configuration processes.	"Information to gather before you begin" on page 182
2. Install the IBM Tivoli Enterprise Console on your event server.	"Installing event synchronization on your event server" on page 183
3. Configure your monitoring server to forward events to IBM Tivoli Enterprise Console.	"Configuring the monitoring server to forward events" on page 194
4. Start and stop IBM Tivoli Enterprise Console on the monitoring server.	"Starting and stopping the process that sends updates to a monitoring server" on page 195

Information to gather before you begin

You need the following information to successfully install and configure event synchronization between IBM Tivoli Monitoring and IBM Tivoli Enterprise Console:

- Host names (or IP addresses), user IDs, and passwords for the monitoring servers that you want to receive events from.
- Simple Object Access Protocol (SOAP) information to send events to a monitoring server (the URL, the rate to send requests to the server).
- Event rule base information (either the name of a new rule base to create or the name of an existing rule base to use).

Notes:

- If your IBM Tivoli Enterprise Console event server is running on Windows 2003 and you are planning to install the IBM Tivoli Enterprise Console remotely (using a program such as Terminal Services to connect to that Windows 2003 computer), run the **`change user /install`** command before you run the installation. This puts the computer into the required "install" mode. After the installation, run the **`change user /execute`** command to return the computer to its previous mode.
- On a UNIX computer, you must configure your TCP/IP network services in the /etc/hosts file to return the fully qualified host name.

Installing event synchronization on your event server

You can install the event synchronization either through an installation wizard or from the command line.

Note: The IBM Tivoli Enterprise Console event server must be recycled during this installation process.

Configuring SOAP on the Hub TEMS

Simple Object Access Protocol (SOAP) is a communications XML-based protocol that enables applications to exchange information through the Internet. SOAP is platform independent and language independent. SOAP uses XML to specify a request and reply structure. It uses HTTP as the transport mechanism to drive the request and to receive a reply.

By default, all monitoring servers are enabled for Web Services. Use the following sections to configure IBM Tivoli Monitoring Web Services (SOAP server) on Windows XP Professional Edition or Windows 2000 computers.

The instructions in this section assume that you have a basic understanding of SOAP, XML and XML Namespaces, and the Web Services Description Language (WSDL).

For complete information about customizing the SOAP interface for your site, refer to *IBM Tivoli Monitoring Administrator's Guide,* SC32-9408.

Table 3-9 outlines the steps required to configure SOAP.

Table 3-9 SOAP configuration steps

Steps	References
1. Define the hubs with which your SOAP server communicates.	"Defining the Hub TEMS that communicate with SOAP" on page 183
2. Create users and grant them access.	"Adding users" on page 184
3. Verify that you have successfully configured SOAP.	"Verifying the SOAP configuration" on page 185

Defining the Hub TEMS that communicate with SOAP

In this step you use Manage Tivoli Monitoring Services to activate the SOAP server and define hubs with which the SOAP server communicates.

To define the SOAP hubs:

1. Open **Manage Tivoli Monitoring Services**.

2. Right-click **Tivoli Enterprise Monitoring Server**.
3. Click **Advanced** → **Configure SOAP Server Hubs**.
4. Click **Add Hub**. The Hub Specification window opens.
5. Select the communications protocol from the Protocol menu.
6. Specify an alias name in the Alias field (for example: SOAP).
7. If you are using TCP/IP or TCP/IP Pipe communications, complete the following fields:
   - Hostname/ip address: Corresponds to the host name or IP address of your Hub TEMS.
   - Port: Default is 1920 (as the one to connect to TEPS).

   Note: If you are connecting to a remote monitoring server, the protocol information must be identical to that used for the hub monitoring server.

8. Click **OK**.

Adding users

In this step you define users on each Hub and specify the access rights for each user (query or update).

Use the following steps:

1. Select the server (click anywhere within the server tree displayed), if necessary.
2. Under Add User Data, type the user name. User IDs must be identical to those specified for monitoring server logon validation. Access is restricted to only that monitoring server to which a user has access.

   Attention: If you do not supply a user ID, all users are given permission to update data.

3. Click the type of user access: **Query** or **Update**.
4. Click **Add User**. The server tree is updated, showing the user and type of access.

   To delete a user, select the user name from the tree and click **Delete Item**.

   To delete a hub, click anywhere in the hub's tree and click **Clear Tree**.

When done you should see a window similar to Figure 3-59.

Figure 3-59 SOAP server hub configuration

Verifying the SOAP configuration

In this step you verify that SOAP has been configured properly by starting the SOAP client and making a request using the Internet Explorer Web browser:

1. From your Hub TEMS type the following address in your Internet browser and press Enter.

   ```
   http://localhost:1920///cms/soap/kshhsoap.htm
   ```

2. In the window that opens, enter the type of SOAP request and the endpoint where you want to retrieve the data (Figure 3-60). Click **Make SOAP Request**.

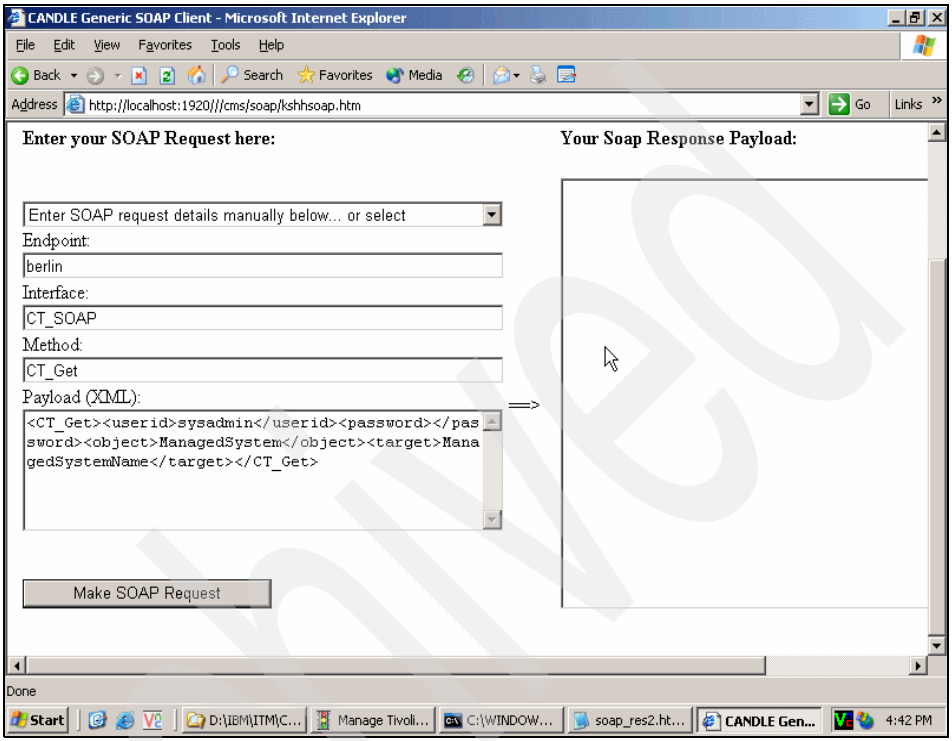

Figure 3-60 SOAP Web interface configuration test

3. This displays the page shown in Figure 3-61.

Figure 3-61 SOAP Response

Installing event synchronization from a wizard

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

> **Note:** If your IBM Tivoli Enterprise Console Server is a UNIX machine, execute the following procedure using a local GUI or an X-Terminal.

1. On the event server, launch the IBM Tivoli Enterprise Console installation by executing the following command:

```
cd $install_dir/unix/tec/
./setupAIX.bin
```

2. Click **Next** on the Welcome window.

3. Select **Accept** in the license agreement window (Figure 3-62).

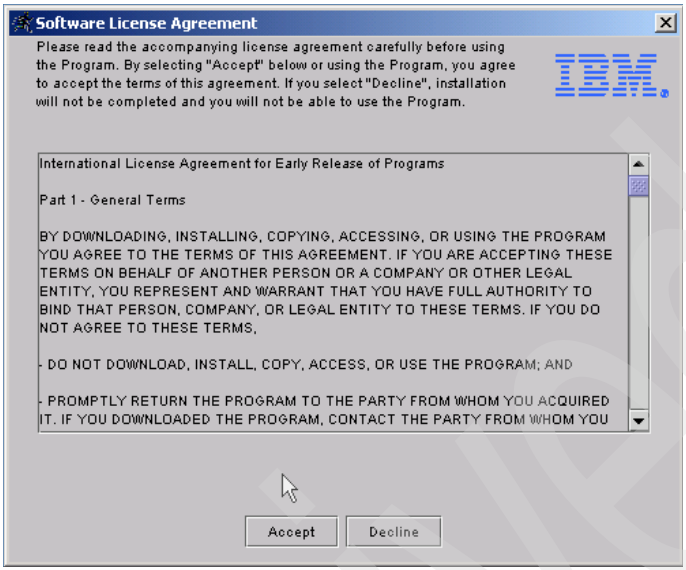

Figure 3-62 Event synchronization Software License Agreement window

4. Click **Next**.

Figure 3-63 Event synchronization configuration fields

5. Complete the fields and click **Next**.

   Table 3-10 shows each configuration field and its respective description.

Table 3-10 Tivoli Enterprise Console event synchronization configuration fields

Fields	Description
Name of the configuration file	The name of the file where event synchronization configuration information is stored. The default name is situpdate.conf.
Number of seconds to sleep when no situation updates	The polling interval, in seconds. The minimum (and default) value is 1. If there are no situation events, the process that forwards events to IBM Tivoli Enterprise Console will rest for 1 second.

Fields	Description
Number of bytes to use to save last events	Number of bytes that the long-running process will use when it saves the location of the last event it processes. This value must be an integer. The minimum (and default) is 50.
URL of the monitoring server SOAP server	The URL for the SOAP server configured on the computer where the monitoring server is running. The default value is cms/soap. This value is used to create the URL to which IBM Tivoli Enterprise Console sends event information. For example, `http://hostname:port///cms/soap`, where `hostname` is the host name of the monitoring server and `port` is the port used by that server.
Rate for sending events from IBM Tivoli Enterprise Console to TEMS via Web services	The maximum number of events sent to the monitoring server at one time. The minimum (and default) value is 10 events.
Level of debug detail for log	The level of information for event synchronization that will be logged. You have the following options: ► Low (default) ► Medium ► Verbose

6. Complete the information about the files where events will be written as described in Table 3-11 when the window in Figure 3-64 pops up, and click **Next**.

Figure 3-64 Event synchronization cache file configuration window

Table 3-11 TEC event synchronization caches file config fields description

Fields	Description
Maximum size of any single cache file, in bytes	The maximum permitted size, in bytes, for any one event cache file. The minimum (and default) value is 50000. Do not use commas (as in 50,000) when specifying this value.
Maximum number of cache files	The maximum number of event caches files at any given time. The minimum (and default) value is 10. When this value is reached, the oldest file is deleted to make room for a new file.

Fields	Description
Directory for cache files to reside	The location where event cache files are located. The default locations are as follows: ► On Windows: C:\tmp\TME\TEC\OM_TEC\persistence ► On UNIX: /var/TME/TEC/OM_TEC/persistence

7. Provide the host name, user ID, and password for each monitoring server with which you want to synchronize events and click **Add**. You must specify information for at least one monitoring server. Figure 3-65 shows an example of TEMS information during the event synchronization configuration.

Host name The fully qualified host name for the computer where the monitoring server is running. This should match the information that will be in events coming from this monitoring server.

User ID The user ID to access the computer where the monitoring server is running.

Password The password to access the computer.

Confirmation The password confirmation.

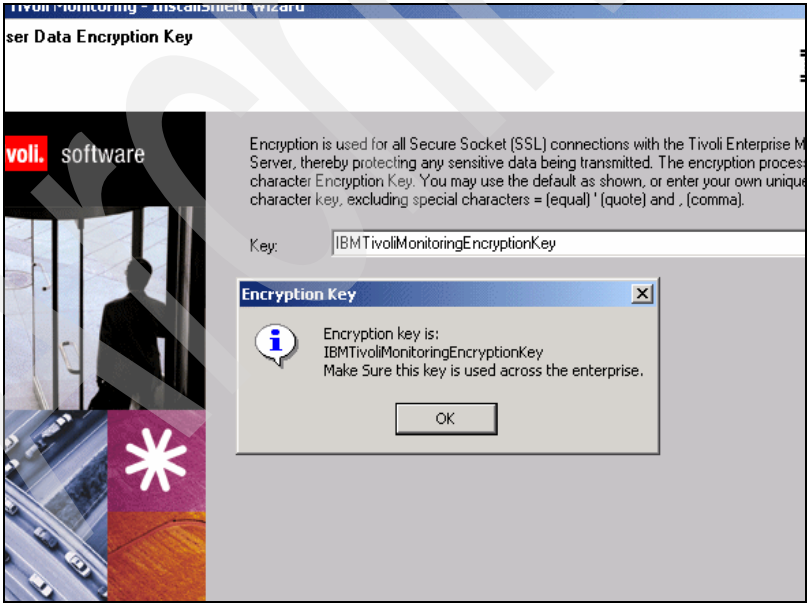

Figure 3-65 Event synchronization Tivoli Enterprise Monitoring Server information

8. When you have provided information about all of the monitoring servers, click **Next**.
9. Specify the rule base that you want to use to synchronize events (Figure 3-66). You can either:
   - Create a new rule base.
   - Use an existing rule base. If you select to use an existing rulebase, the IBM Tivoli Enterprise Console BAROC class files (omegamon.baroc and Sentry.baroc [if not present]) and the omegamon.rls ruleset file are imported into your existing rulebase.

   We used the second option as we already have IBM Tivoli Enterprise Console set up and running properly.

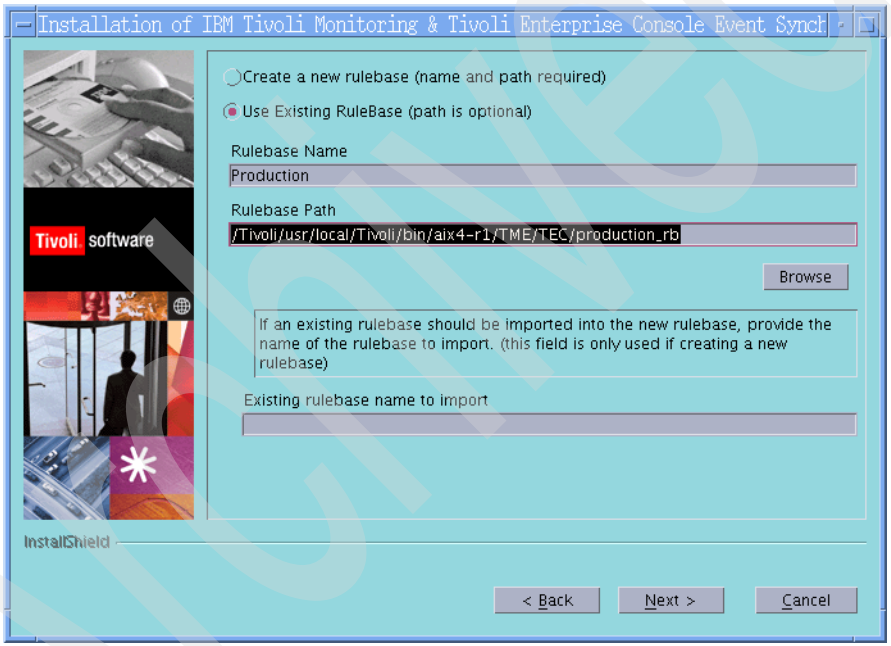

Figure 3-66 IBM Tivoli Enterprise Console rule base configuration

Notes:

- If you are creating a new rule base, type the name for the rule base you want to create and the path to the new rule base location. You must specify a location as there is no default.
- If you are using an existing rule base, type the name of the rule base.
- If you want to import an existing rule base into a new rule base, type the name of the existing rule base in the Existing rulebase to import field. This step is available only if you are creating a new rule base.

10. Click **Next**.
11. Click **Next** on the preinstallation summary panel. The installation begins.
12. When the installation and configuration steps have completed, click **Finish** on the Summary Information window.

Note: If any configuration errors occurred during installation and configuration, you are directed to a log file that contains additional troubleshooting information.

If you did not configure the event forwarding during the Hub TEMS installation and configuration, refer to “Configuring the monitoring server to forward events” on page 194.

Configuring the monitoring server to forward events

Before the monitoring server forwards any situation events to IBM Tivoli Enterprise Console, you have to enable that forwarding and the filtering of events.

Enabling event forwarding

Use the following steps to enable event forwarding on your monitoring server:

1. From your Hub TEMS, in Manage Tivoli Monitoring Services, right-click the monitoring server and click **Reconfigure** (Windows) or **Configure** (UNIX).
2. On the configuration options window, select **TEC Event Integration Facility**. For UNIX, click the **TEC** tab to view this configuration option.
3. Click **OK** and then **OK** again.

4. Complete the following fields on the IBM Tivoli Enterprise Console Server: Location and Port Number window and click **OK**:

   TEC Server Location

   The host name or IP address (in dotted format, such as 0.0.0.0) for the computer where the IBM Tivoli Enterprise Console event server is installed.

   TEC Port Number

   The port number for the event server. Set this value to 0 (when your event server is a UNIX server) unless the portmapper is not available on the event server (as when the event server is running on a Windows server). When you specify 0, the port number is retrieved by the portmapper.

   If you want to use the default port (5529), edit the tec_installdir/TME/TEC/.tec_config file on the event server and remove the semicolon (;) from the following line: tec_recv_agent_port=5529. Port 5529 is often used when the event server is a Windows platform.

   After you have done this, any error during the installation can be found in the error log file, /tmp/tec_sync_install.log.

5. Click **Finish.**

Enabling event filtering

By default, all situation events are filtered out, meaning that they are never forwarded to IBM Tivoli Enterprise Console. Use the following steps to change the filtering on the TEMS servers that forward events to IBM Tivoli Enterprise Console:

1. Open the om_tec.config file (located in <install_dir>\cms\TECLIB\ on Windows and <install_dir>/tables/<tems_name>/TECLIB on UNIX).
2. Comment out the following line by adding a pound sign (#) in front of it:

   ```
   Filter:Class=ITM_Generic;master_reset_flag='';
   ```

3. Save and close the file.

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

To send event updates to a monitoring server, you must start a long-running process called Situation Update Forwarder. This process is started automatically when the event server starts. To stop the process manually, change to the

$BINDIR/TME/TEC/OM_TEC/bin directory (where $BINDIR is the location of the IBM Tivoli Enterprise Console installation) and run the following command:

On Windows:

```
stopSUF.cmd
```

On UNIX:

```
stopSUF.sh
```

On Windows, you can also 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. Refer to Figure 3-63 on page 189 and Table 3-10 on page 189 for more details.

3.2.15 Configuring the Hot Standby

The optional Hot Standby function enables you to maintain continuous availability by defining a standby monitoring server to provide backup for your hub monitoring server. If the hub monitoring server fails, hub functions automatically switch to the standby monitoring server. IBM Tivoli Monitoring automatically connects all remote monitoring servers and agents to the standby monitoring server. There is no automatic switch that returns control to the hub monitoring server when it is available. If you want to switch back to the hub monitoring server, you must manually stop the standby monitoring server.

Configuring Hot Standby involves the following steps:

1. Install the monitoring server software on the systems you want to use as Hot Standby (refer to “Installing the backup hub monitoring server” on page 197). We assume that the primary Hub TEMS is already up and running.

2. Configure Hot Standby on the hub monitoring server, the backup monitoring server, and any remote monitoring servers associated with the hub monitoring server; refer to “Configuring Hot Standby” on page 197.
3. Configure Hot Standby on any agents that are associated with the hub monitoring server like the TEPS and the Warehouse Proxy agent; refer to “Configuring the Warehouse Proxy” on page 199.

Note: TEMS Hot Standby is not supported on z/OS.

Installing the backup hub monitoring server

See “Installing and configuring a Hub TEMS on a Windows server” on page 14 or “Installing a Hub TEMS on a UNIX server” on page 116 for information about installing a hub monitoring server. When you are installing the backup hub monitoring server, use identical values to those you used when installing the primary hub monitoring server.

Configuring Hot Standby

Configure the hub server, the standby hub server, and any remote servers associated with the hub server.

Note: The hub and standby monitoring servers should be configured as mirrors of each other.

Configuring Hot Standby on a Windows TEMS

Use the following procedure to configure Hot Standby on a Windows TEMS:

1. In Manage Tivoli Monitoring Services, right-click the name of the hub monitoring server and click **Reconfigure** (or **Configure** on UNIX).
2. Select **Configure Standby CMS** and specify the protocols used by the standby server. These protocols should match those specified for the hub server.
3. Click **OK**, then **OK** again on the message that is displayed.
4. Click **OK** on the window that displays the communication settings for this server.
5. Type the host name or IP address for the standby monitoring server in the Hostname or IP Address field and click **OK**.
6. Configure the Tivoli Enterprise Console server name and port in the next window. The default will be the one you configure on your Hub TEMS.
7. Restart the monitoring server.

8. Repeat these steps for the standby monitoring server and any remote monitoring servers.

Configuring Hot Standby on a UNIX TEMS

Use the following procedure to configure Hot Standby on a UNIX TEMS:

1. From the $CANDLEHOME/bin execute the following command:

   ```
   ./itmcmd config -S -t tems_name
   ```

   tems_name is the name of the TEMS hosted by the UNIX server. In Example 3-14, server MADRID is being configured with server cairo as its Hot Standby server.

Example 3-14 ./itmcmd config -S -t HUB_MADRID output

```
[root@madrid][/opt/IBM/ITM/bin]-> ./itmcmd config -S -t HUB_MADRID
CandleConfig        :  installer level  400 / 100.
CandleConfig        :  running aix516 jre.
Configuring CMS...
```

2. Press Enter if *LOCAL is the default. If not, type *LOCAL.

   ```
   Hub or Remote [*LOCAL or *REMOTE] (Default is: *LOCAL): *LOCAL
   TEMS Host Name (Default is: madrid):
   ```

3. Select your primary communication protocol.

   ```
   Network Protocol 1 [ip, sna, or ip.pipe] (Default is: ip.pipe):
   ```

4. Select a secondary communication protocol.

   ```
     Now choose the next protocol from one of these:
     - ip
     - sna
     - none
   Network Protocol 2 (Default is: ip):
   ```

5. Select a third communication protocol.

   ```
     Now choose the next protocol from one of these:
     - sna
     - none
   Network Protocol 3 (Default is: none):
   ```

6. Choose the port used by the server being configured.

   ```
   IP Port Number (Default is: 1918):
   IP.PIPE Port Number (Default is: 1918):
   ```

7. Accept the default for the next option or enter the correct file name.

   ```
   Enter name of KDC_PARTITION (Default is: null):
   Enter path and name of KDC_PARTITIONFILE (Default is:
   /opt/IBM/ITM/tables/HUB_MADIRD/partition.txt):
   ```

8. Press Enter to accept the default.

```
Configuration Auditing? [YES or NO] (Default is: YES):
Now enter with the server host name used as hot standby (backup)
Hot Standby TEMS Host Name (Default is: milan):
```

9. Enter the communication protocol and the port (Example 3-15).

Example 3-15 Entering communication protocol and the port

```
Hot Standby Protocol 1 [ip, sna,ip.pipe or ip.spipe] (Default is: ip.pipe):

     Now choose the next protocol from one of these:
     - ip
- sna
     - ip.spipe
     - none
Hot Standby Protocol 2 (Default is: ip):

     Now choose the next protocol from one of these:
     - sna
- ip.spipe
     - none
Hot Standby Protocol 3 (Default is: none):
Hot Standby IP Port Number (Default is: 1918):
Hot Standby IP.PIPE Port Number (Default is: 1918):
```

The next steps are similar to those in “Configuring the UNIX monitoring server” on page 206.

Configuring the Warehouse Proxy

The Warehouse Proxy must be configured to point to a Secondary TEMS in case the primary Hub TEMS fails and the Hot Standby takes place. Use the following procedure to configure the Warehouse Proxy:

1. Open the Manage Tivoli Monitoring Services console from the Warehouse proxy server, right-click on the **Warehouse Proxy** server, and click **Reconfigure**.

2. Click **OK** on the pop-up window.

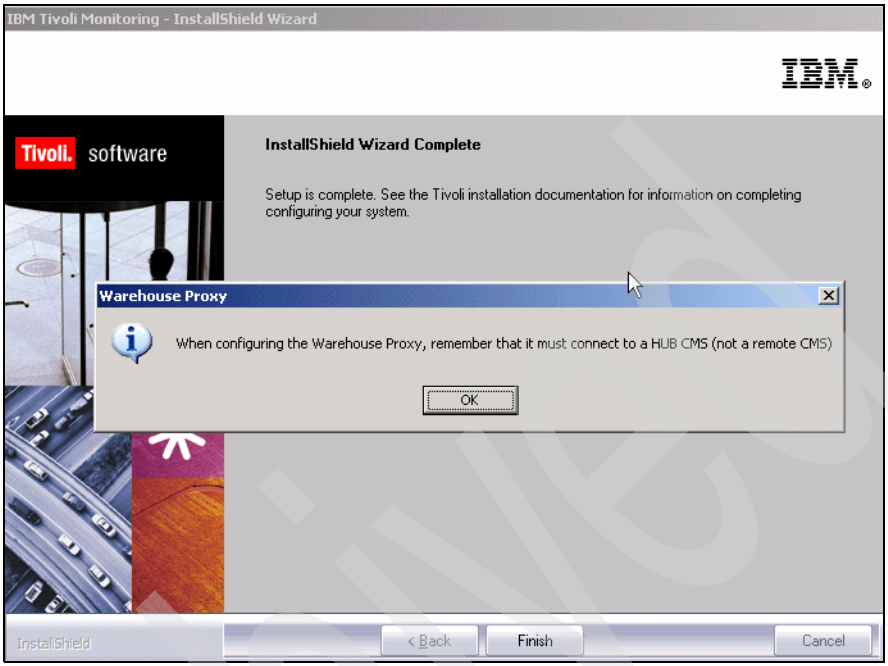

Figure 3-67 Warehouse Proxy confirmation window configuration

3. The primary TEMS communication protocol is already defined. Check the **Optional Secondary TEMS Connection** check box and configure the communication protocol the secondary TEMS will be using as shown in Figure 3-68.

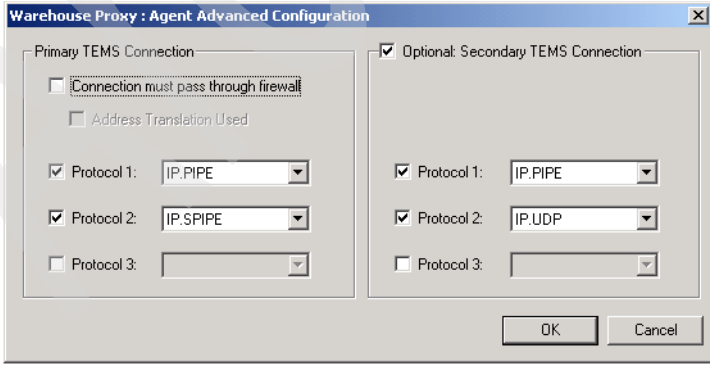

Figure 3-68 Warehouse Proxy Secondary TEMS communication configuration

4. Select **OK** on the next window or update the primary TEMS if it has changed (Figure 3-69).

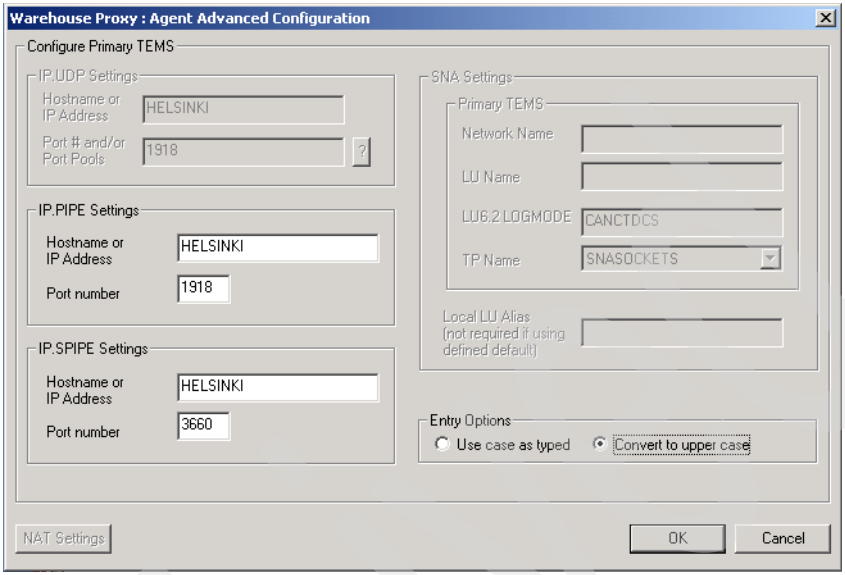

Figure 3-69 Warehouse Proxy primary TEMS configuration

5. Enter the secondary TEMS host name for each communication protocol chosen in Figure 3-68 on page 200 and click **OK.**
6. The Warehouse Proxy is thus configured to connect to the secondary Hub TEMS if the primary one fails.

Configuring the TEPS

The TEPS will have to be configured only if the primary Hub TEMS fails and the standby Hub TEMS becomes the primary. Use the following steps to configure the TEPS:

1. Open the Manage Tivoli Monitoring Services console.
2. Right-click the **Tivoli Enterprise Portal Server service**.
3. Select **Reconfigure** (Window) or **Configure** (Linux).
4. Specify the new Hub TEMS and click **OK.**
5. The window shown in Figure 3-70 on page 202 appears. Click **OK**.

Note: Clicking OK as shown in Figure 3-70 on page 202 saves the user IDs, queries, workspace, navigators, and terminal scripts in %CANDLEHOME%\CNPS\CMS*TEMS_HOSTNAME_PORT*\saveexport.sql.

(*TEMS_HOSTNAME* is the new TEMS host name and *PORT* is the port number the TEPS will connect to the TEMS. For example:

```
F:\IBM\ITM\CNPS\CMS\MADRID_1918\saveexeport.sql
```

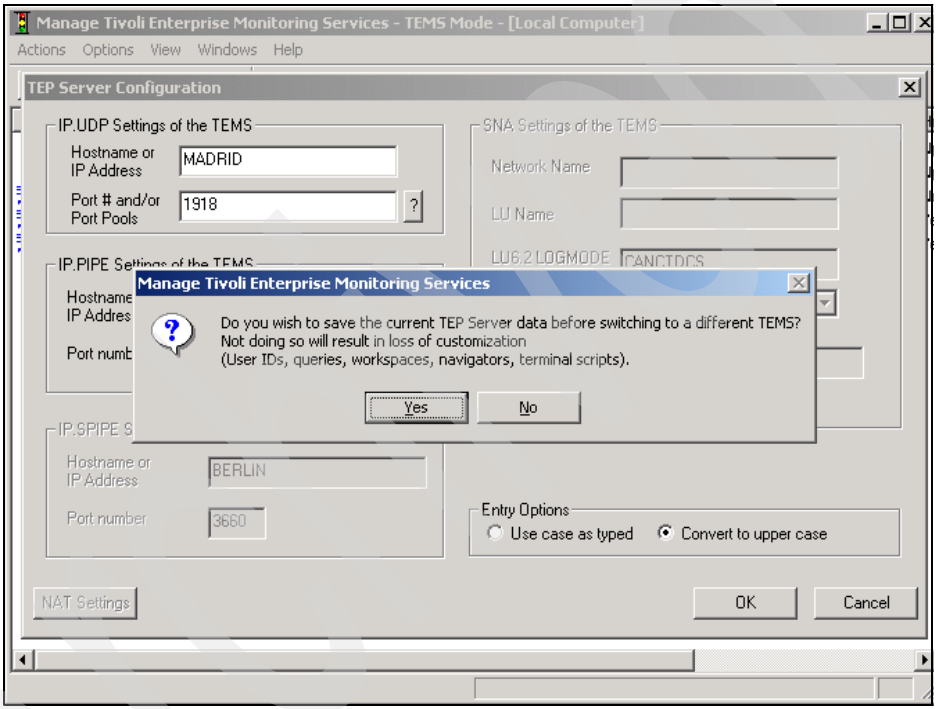

Figure 3-70 TEPS configuration window database backup confirmation

6. From the Enterprise Monitoring Server console, restart the TEPS.

Note: You do not have to reconfigure the TEPS database.

3.2.16 Installing and configuring the scenario 2 environment

This section describes the installation and configuration of IBM Tivoli Monitoring 6.1 components on an UNIX Hub TEMS environment.

Installing a Hub TEMS on a UNIX server

To install a Hub TEMS on a UNIX server, you can use either root or a different user with the proper permissions on the IBM Tivoli Monitoring 6.1 files and directories; see “Creating an IBM Tivoli account on UNIX servers” on page 98.

Use the following steps to install the monitoring server on a UNIX computer.

Notes:

- We will not show the installation of the Hub TEMS individually; we will only focus on how to install a Hub TEMS on UNIX environment.
- This procedure is also valid for Linux servers, so we will not make any distinction between UNIX and Linux configurations in this section.

1. In the directory where you extracted the installation files, run this command:
   ```
   ./install.sh
   ```
2. When prompted for the IBM Tivoli Monitoring home directory, press Enter to accept the default (opt/IBM/ITM). If you want to use a different installation directory, type the full path to that directory and press Enter.

   Note: If the directory you specified does not exist, you are asked whether to create it. Type y to create this directory.

   This displays the prompt shown in Example 3-16.

Example 3-16 Select one of the following prompt

```
Select one of the following:
1) Install products to the local host.
2) Install products to depot for remote deployment (requires TEMS).
3) Exit install.
```

Type **1** to start the installation process and press Enter. The following menu will be displayed to you (only the relevant information are shown to you):

Example 3-17 Software Licensing Agreement

```
Software Licensing Agreement
1. Czech
2. English
```

```
3. French
4. German
5. Italian
6. Polish
7. Portuguese
8. Spanish
9. Turkish
Please enter the number that corresponds to the language
you prefer.
```

3. Type the number that corresponds to the language that you want to display the software license agreement in and press Enter.
4. Press Enter to display the license agreement.
5. Type 1 to accept the agreement and press Enter. The message in Example 3-18 appears.

Example 3-18 Preparing to install the Global Security Kit message

```
runGSkit        :  Preparing to install the Global Security Kit.
runGSkit warning:  the 'root' ID or password is required for this phase,
continuing ...
 Will enable automatic agent initiation after reboot.

Please enter root password or press Enter twice to skip.
```

Notes:

- If you are installing the IBM Tivoli Monitoring 6.1 with root user you will not obviously be asked the root password for the GSKit installation.
- GSKit is Global Security Kit, an IBM toolkit that enables products to provide secure connections over TCP/IP among IBM Tivoli Monitoring 6.1 components.

  Two main functions to GSKit:

  – A toolkit that can be used for Secure Socket Layer (SSL) communications using public key encryption/decryption methodology
  – Key management functions using iKeyman (a Java-based application for managing keys and key requests)

6. Type the root password and press Enter if you want to use GSKit; otherwise press Enter twice.
7. Type a 32-character encryption key and press Enter. If you want to use the default key, press Enter without typing any characters.

Important: Save this key to use when you install the other components.

8. Type the number for the operating system for which you want to install products when the following menu is displayed, then press Enter.

Example 3-19 List of available OSs for IBM Tivoli Monitoring 6.1 installation

```
Product packages are available in /opt/itm61s1/unix

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

 1) AIX R5.1 (32 bit)
 2) AIX R5.1 (64 bit)
 3) AIX R5.2 (32 bit)
 4) AIX R5.2 (64 bit)
 5) AIX R5.3 (32 bit)
 6) AIX R5.3 (64 bit)
 7) Solaris R10 (32 bit)
 8) Solaris R10 (64 bit)
 9) Solaris R8 (32 bit)
10) Solaris R8 (64 bit)
11) Solaris R9 (32 bit)
12) Solaris R9 (64 bit)

Type the number for the OS or component support category you want, or type "q"
to quit selection
[ number "5" or "AIX R5.3 (32 bit)" is default ]:  5
```

Note: The default value is your current operating system.

9. Type y to confirm the operating system and press Enter. A numbered list of available components is displayed.
10. Type the number that corresponds to the Tivoli Enterprise Monitoring Server option and press Enter.
11. The available products to be installed are listed. You can choose more than one product by typing their corresponding numbers separated by a comma or a space. Example 3-20 shows the option list.

Example 3-20 Option list

```
The following products are available for installation:

 1) Monitoring Agent for UNIX Logs  V06.10.00.00
 2) Monitoring Agent for UNIX OS  V06.10.00.00
 3)Summarization and Pruning agent  V06.10.00.00
 4) Tivoli Enterprise Monitoring Server  V06.10.00.00
 5) Tivoli Enterprise Services User Interface  V06.10.00.00
```

```
 6) Universal Agent  V06.10.00.00
 7) all of the above

Type the numbers for the products you want to install, or type "q" to quit
selection.
If you enter more than one number, separate the numbers by a comma or a space.

Type your selections here:  4
```

12. Type `y` to confirm your selection or `n` to restart.
13. When prompted, type a name for your monitoring server:

    ```
    Please enter TEMS name: HUB_MADRID
    ```

    Do not use the fully qualified host name. Press Enter.
14. After all of the components are installed, you are asked whether you want to install components for a different operating system. Type `n` and press Enter.

Installation is complete. The next step is to configure your monitoring server.

Configuring the UNIX monitoring server

Use the following steps to configure the hub monitoring server.

Note: When we accept the default value on the various displayed options, we just press Enter. Thus, for some cases in the following examples you will not see any entry, because we simply press Enter.

1. At the command line, change to the opt/IBM/ITM/bin directory (or the directory where you installed IBM Tivoli Monitoring, actually the $CANDLEHOME/bin).

   ```
   cd $CANDLEHOME/bin
   ```
2. Run the following command:

   ```
   ./itmcmd config -S -t tems_name
   ```

   This produces the message shown in Example 3-21.

Example 3-21 itmcmd config output

```
CandleConfig        :  installer level  400 / 100.
CandleConfig        :  running li6243 jre.
Configuring CMS...

Hub or Remote [*LOCAL or *REMOTE] (Default is: *LOCAL):*LOCAL
TEMS Host Name (Default is: madrid): (ENTER (hitted)
```

Choose *LOCAL (the default) as you are installing a Hub TEMS.

3. Configure the communication protocol. Several options are offered: IP, SNA, IP.PIPE,IP.SPIPE. Select your preferred protocol. Refer to “Communications protocol selection” on page 22 for detailed information about protocol specifications.
4. If you want to use a secondary protocol in case the first one fails, enter it at the next option window (Example 3-22).

Example 3-22 Entering a secondary protocol

```
   Now choose the next protocol from one of these:
        - ip
        - sna
        - ip.spipe
        - none
   Network Protocol 2 (Default is: ip):

        Now choose the next protocol from one of these:
        - sna
        - ip.spipe
        - none
   Network Protocol 3 (Default is: none):

Network Protocol 1 [ip, sna, ip.pipe or ip.spipe] (Default is: ip.pipe):
   Now choose the next protocol from one of these:
        - ip
        - sna
        - ip.spipe
        - none
   Network Protocol 2 (Default is: ip):
   Now choose the next protocol from one of these:
        - sna
        - ip.spipe
        - none
Network Protocol 3 (Default is: none):
```

We have chosen IP.PIPE as the primary protocol and IP.UDP as the secondary protocol.

5. Set the ports for the communication protocols you have chosen; the default is 1918. You can choose another port if you want to, but you have to remember to use it when setting up the Remote TEMS and the TEMA that will be connected to the Hub TEMS. We select the default configuration:

```
IP Port Number (Default is: 1918):
IP.PIPE Port Number (Default is: 1918):
```

6. You are asked for the name of KDC_PARTITION as shown in Example 3-23 on page 208. This is used in environments using NAT across a firewall. We select the default.

Example 3-23 KDC_PARTITION question

```
Enter name of KDC_PARTITION (Default is: null):
Enter path and name of KDC_PARTITIONFILE (Default is:
/opt/IBM/ITM/tables/REMOTE_EDINBURG/partition.txt):
```

Note: When IBM Tivoli Monitoring components need to communicate across a firewall that performs NAT, those components must be able to retrieve an IP address of the other component that is valid on its side of the firewall. To support this capability, the location broker namespace is logically divided into partitions with unique partition IDs. Partition IDs are specified using the KDC_PARTITION environment variable. The partition file is the means to insert appropriate IP addresses into the location broker namespaces.

7. If you want to use Configuration Auditing, type y and press Enter. Otherwise, press Enter. (During the installation, we chose to audit the configuration.)
8. Press Enter to accept the default setting for Hot Standby (NO).

Tip: It is a good idea to wait until after you have fully deployed your environment to configure Hot Standby for your monitoring server. See 3.2.15, "Configuring the Hot Standby" on page 196.

9. Press Enter to accept the default for the Optional Primary Network Name (none).
10. Press Enter for the default security: Validate User setting (no). If you need to use security validation in your environment, you can enable it after initial configuration is complete. See "Configuring user security" on page 69 for more information.

Note: If you enable the security validation, you must create on the server the users who need to access the IBM Tivoli Monitoring 6.1 environment.

11. If you will be using event synchronization to view situation events, type y and press Enter to enable TEC Event Integration. Complete the following additional steps:
    a. Type the name of the IBM Tivoli Enterprise Console event server and press Enter.
    b. Type the port number for the event server and press Enter (if your event server is using port mapper; for example on a UNIX server, the port is 0. or if your event server is on a Windows machine the default port is 5529).

Note: If your Tivoli Enterprise Console is not yet set up, you can skip the previous section by typing NO and perform the configuration later using the same procedure.

c. Press Enter to not disable the Workflow Policy/Tivoli Emitter Agent.

12. Type `s` to save the SOAP configuration and exit the configuration. We will perform the SOAP configuration later, when configuring the event synchronization.

Installing agent support on (seeding) the hub monitoring server

After you have configured the TEMS, you must install the application support. Use the following steps to seed the hub monitoring server. Remember that seeding adds product-specific data to the monitoring server.

1. Start the monitoring server by running the following command from the $CANDLEHOME\bin directory:

   ```
   ./itmcmd server start <tems_name>
   ```

2. Run the following command to start the seeding process:

   ```
   ./itmcmd -t <tems_name> <pc pc pc>
   ```

   In this command, *tems_name* is the Hub TEMS name and *pc* is the product code for each agent whose data you want to send to the monitoring server. (You can retrieve the information by executing the command **`cinfo -i`**).

   Note: Seed the server with all available pc codes in advance.

3. Stop the monitoring server by running the following command:

   ```
   ./itmcmd server stop <tems_name>
   ```

4. Restart the monitoring server by running the following command:

   ```
   ./itmcmd server start <tems_name>
   ```

When you are done with the Hub TEMS, refer to Table 3-12 for installing the rest of the components.

Table 3-12 How to install IBM Tivoli Monitoring 6.1 components in scenario 2

Components	References
Install and configure the second UNIX Hub TEMS.	"Installing and configuring the scenario 2 environment" on page 203
Install and configure the remote TEMS.	"Installing a Remote TEMS on a Windows and UNIX server" on page 116
TEPS	"Tivoli Enterprise Portal Server - TEPS" on page 121
TEMAs	"Tivoli Enterprise Monitoring Agent" on page 129 and "Deploying TEMA from the command line interface" on page 158
TEP	"Tivoli Enterprise Portal (TEP)" on page 160
Warehouse Proxy agent	"Warehouse Proxy installation and configuration" on page 164
Summarization and Pruning agent	"Summarization and Pruning agent installation and configuration" on page 173
Event synchronization	"Event synchronization installation" on page 181
Hot standby	"Configuring the Hot Standby" on page 196

3.2.17 Replacing a Hub TEMS server with a new one

For any reason (hardware upgrade, for example) if you want to replace your Hub TEMS server with a new one from the same platform or a different platform, IBM Tivoli Monitoring 6.1 allows you to do so. This section describes the procedure we followed to replace our scenario 1 implementation (Windows TEMS servers) with scenario 2 (UNIX TEMS servers).

1. Install, configure, and seed the Hub TEMS on the madrid and milan servers. Depending on the platform you are using, refer to "Installing and configuring a Hub TEMS on a Windows server" on page 102 or "Installing a Hub TEMS on a UNIX server" on page 203.
2. Stop all Remote TEMS (copenhagen and edinburg) using either the Manage Tivoli Enterprise Monitoring Services console or, for UNIX servers, use the following command:

   ```
   itmcmd server stop tems_name
   ```

   tems_name is the of the TEMS host by the server your are stopping its TEMS service.

3. Stop the TEPS, Warehouse Proxy agent, and Summarization and Pruning agent from the Manage Tivoli Enterprise Monitoring Services console.
4. Stop the Hub TEMS (cairo and helsinki) using Manage Tivoli Enterprise Monitoring Services console or **itmcmd** command for UNIX servers as describe previously.
5. Configure the Remote TEMS (copenhagen and edinburg) to point to your new Hub TEMS (madrid and milan primary and Hot Standby TEMS, respectively). Use the Reconfigure option on the Manage Tivoli Enterprise Monitoring Services console on UNIX servers or the following procedure on UNIX servers:

```
itmcmd config -S -t tems_name
```

6. Configure the Warehouse Proxy agent and Summarization and Pruning agent to point to the primary and Hot Standby TEMS (madrid and milan) respectively. This operation is performed using the Manage Tivoli Enterprise Monitoring Services console.
7. Using the Manage Tivoli Enterprise Monitoring Services console, configure the TEPS to point to madrid.

Important: Before pointing TEPS to the new TEMS, you must save TEPS data using the migrate-export.bat facility, which detects the TEPS database and creates the SQL file script that will be used to restore your TEPS services. Use the following procedure to back up and import the data:

- Saving TEPS data

  Use the following procedure to back up your TEPS database:

  - **cd** to %CANDLEHOME%/CNPS
  - Run **migrate-export.bat**

  The migrate-export.bat facility stops the TEPS, creates a saveexport.sql, and restarts the TEPS.

- Importing backup data

  Use the following procedure to restore your TEPS initial state:

  - Import the data back into TEPS by copying the presentation files back to the CNP directory.
  - Copy the saveexport.sql file to the %CANDLEHOME%\cnps\sqllib directory and run migrate_import.bat.

  If you are using Linux as your TEPS, read $CANDLEHOME instead of %CANDLEHOME%.

8. Configure cairo to become a Remote TEMS. This is done using the Manage Tivoli Enterprise Monitoring Services console or itmcmd on a UNIX server. This step can be skipped if you do not want to reconfigure any of your old Hub TEMS to a Remote TEMS.
9. Configure agents on oslo and dakar to point to cairo and copenhagen, the primary and secondary Remote TEMS respectively. You do not have to reconfigure your agents to point to the new Hub; this operation was done to check whether the remote TEMS cairo is working as expected.
10. Start the Remote TEMS (edinburg, copenhagen, and cairo). Use the Manage Tivoli Enterprise Monitoring Services console or the `itmcmd` command for UNIX servers.
11. From the Manage Tivoli Enterprise Monitoring Services console, start the Warehouse Proxy agent, Summarization and Pruning agent, and TEPS.

Notes:

- This procedure is recommended only if you want to change your platform's Hub TEMS. If you want to build a two-Hub TEMS environment, you can install it from scratch.
- We were able to get all of the agents (from scenario 1) back up and running; we had to restart a few agents to have them reconnected. Others reconnected automatically.
- We lost our situations, workspace, and collections configuration because we did not save it to transfer it later on the new Hub TEMS.

Tips:

- If you want to change your Hub TEMS environment, back up the entire environment and plan the transition very carefully.
- If you are replacing one Hub TEMS with another one with the same platform and configuration (host name, TCP/IP configuration), you can back up the CANDLEHOME directory from the current Hub TEMS and restore it later onto the new Hub TEMS.
- If the new and old TEMS are installed on the same platform (such as both UNIX or Windows). you can back up your candle database from your current Hub TEMS and restore it later onto the new Hub TEMS. You must copy the following files from your old HUB TEMS.

  Windows: %CANDLEHOME%/CMS/QA1*.db and QA1*.idx

  UNIX: $CANDLEHOME/tables/TEMS_NAME/QA1*.db and QA1*.idx

3.3 Uninstalling IBM Tivoli Monitoring 6.1

In this section we uninstall IBM Tivoli Monitoring 6.1, both the whole environment and individual components.

3.3.1 Uninstalling the entire IBM Tivoli Monitoring environment

Use these procedures to remove the entire IBM Tivoli Monitoring environment.

Uninstalling the environment on Windows

Use the following steps to uninstall IBM Tivoli Monitoring from a Windows computer:

1. From the desktop, click **Start** → **Settings** → **Control Panel** (for Windows 2000) or **Start** → **Control Panel** (for Windows 2003).
2. Click **Add/Remove Programs.**
3. Select **IBM Tivoli Monitoring** and click **Change/Remove**.
4. Select **Remove** and click **Next**.
5. Click **OK**.
6. After Tivoli Enterprise services have stopped, you are asked if you want to remove the Tivoli Enterprise Portal database. Click **Yes**.
7. Type the password for the DB2 administrator in the Admin Password field and click **OK**.

   A pop-up window, indicating that GSKit is being uninstalled, is displayed.
8. Select **Yes** to restart your computer and click **Finish**.

Uninstalling the environment on UNIX

Before executing the uninstallation procedure, make sure that all IBM Tivoli Monitoring 6.1 components are shut down.

1. Stop the agent by executing this command from $CANDLEHOME/bin:

   ```
   ./itmcmd agent stop pc
   ```

   pc is the product code (lz, ux, ul, um, ui, cj, and so on).
2. Stop the TEMS by executing this command from $CANDLEHOME/bin:

   ```
   ./itmcmd server stop TEMS_NAME
   ```
3. Run the following command:

   ```
   ./uninstall.sh
   ```

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

4. Type the number for the installed product that you want to uninstall. Repeat this step for each additional installed product you want to uninstall (Example 3-24).

Example 3-24 Uninstalling the environment on UNIX

```
********** Mon Oct 10 15:08:29 EDT 2005 ******************
User      : itmuser      Group: itmuser
Host name : edinburg.itsc.austin.ibm.com         Installer Lvl: 400 / 100
CandleHome: /opt/IBM/ITM
***********************************************************

...Products available to uninstall

Num     Product [ Code  Platform Version:Release Description ]
1       cj  li6243       v610:r172  Tivoli Enterprise Portal Desktop Client
2       lz  li6263       v610:r115  Monitoring Agent for Linux OS
3       ms  li6243       v610:r215  Tivoli Enterprise Monitoring Server
4       sh  li6243       v610:r215  Tivoli Enterprise Monitoring SOAP Server
5       uf  li6243       v610:r100  Universal Agent Framework
6       ui  li6243       v610:r194  Tivoli Enterprise Services User Interface
7       um  li6243       v610:r229  Universal Agent

Enter number for a product to uninstall or "EXIT" to exit: 1
Confirm: cj  li6243  v610:r172 Tivoli Enterprise Portal Desktop Client ... OK
to delete? [y/n]: y
```

5. When finished, restart the computer to complete the uninstallation.

Notes:

- If for any reason the UNIX uninstallation is not successful, run the following command to remove all IBM Tivoli Monitoring directories:

  ```
  rm -r $CANDLEHOME
  ```

- If you are uninstalling the components using a user ID different from root user you might have errors like the following:

  ```
  rm: cannot remove `/etc/rc0.d/K10ITMAgents1': Permission denied
  rm: cannot remove `/etc/rc1.d/K10ITMAgents1': Permission denied
  rm: cannot remove `/etc/rc2.d/S99ITMAgents1': Permission denied
  rm: cannot remove `/etc/rc3.d/S99ITMAgents1': Permission denied
  rm: cannot remove `/etc/rc4.d/S99ITMAgents1': Permission denied
  rm: cannot remove `/etc/rc5.d/S99ITMAgents1': Permission denied
  rm: cannot remove `/etc/rc6.d/K10ITMAgents1': Permission denied
  rm: cannot remove `/etc/init.d/ITMAgents1': Permission denied
  ```

  Contact your system administrator to remove those files.

3.3.2 Uninstalling an individual agent or component

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

Uninstalling a component on Windows

Use the following steps to remove a component on a Windows computer. You can uninstall a single agent or the entire agent bundle (such as IBM Tivoli Monitoring for Databases).

1. From the desktop, click **Start** → **Settings** → **Control Panel** (for Windows 2000) or **Start** → **Control Panel** (for Windows 2003).
2. Click **Add/Remove Programs**.
3. Do one of the following:
   - 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. Take one of the following steps:
   - To uninstall a specific agent or component, select **Modify**.
   - To uninstall the entire agent bundle, select **Remove**.
6. Click **Next**.
7. Do one of the following:
   - If you are uninstalling an agent bundle, click **OK** to confirm the uninstallation.
   - If you are uninstalling an agent or component, do the following:
     i. For an agent, expand **Tivoli Enterprise Monitoring Agents** and select the agent you want to uninstall.
     ii. For a component, select the component (such as Tivoli Enterprise Portal Desktop Client).
     iii. Click **Next**.
     iv. Click **Next** on the confirmation screen.
     v. Depending on the remaining components on your computer, there might be a series of configuration panels. Click **Next** on each.
8. Click **Finish** to complete the uninstallation.
9. Restart the computer to complete the uninstallation.

Note: When removing a specific component (Modify/Remove), do not unselect any component other than the one you are removing. Deselecting any other component will uninstall it from the machine.

Uninstalling a component on UNIX

Use the following steps to remove a component from a UNIX computer. You can uninstall a single agent or the entire agent bundle (such as IBM Tivoli Monitoring for Databases).

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

   ```
   cd $CANDLEHOME/bin
   ```

   $CANDLEHOME is the path for the home directory for IBM Tivoli Monitoring.

2. Run the following command:

   ```
   ./uninstall.sh
   ```

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

3. Type the number for the agent or component that you want to uninstall. Repeat this step for each additional installed product you want to uninstall.
4. Restart the computer to complete the uninstallation.

3.3.3 Uninstalling TEC event synchronization

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

1. Stop event synchronization on the event server by running the following command:

   On Windows:

   ```
   <tec_installdir>\TME\TEC\OM_TEC\bin\stop.cmd
   ```

   On UNIX:

   ```
   <tec_installdir>/TME/TEC/OM_TEC/bin/stop.sh
   ```

2. Run the following uninstallation program:

   On Windows:

   ```
   <tec_installdir>\TME\TEC\OM_TEC\_uninst\uninstaller.exe
   ```

   On UNIX:

   ```
   tec_installdir/TME/TEC/OM_TEC/_uninst/uninstaller.bin
   ```

tec_installdir is the location of the IBM Tivoli Enterprise Console installation.

3. Follow the prompts in the uninstallation program.

Notes:

- You can also run this uninstallation program in silent mode (by running the program from the command line with the -silent parameter) or in console mode (by using the -console parameter).
- You must stop and restart the event server for these changes to take effect.
- If your event server is running on an HP-UX computer, ensure that the _uninst and _jvm directories are successfully removed by the uninstallation program. If they are not, manually delete these directories.

4

Working with IBM Tivoli Monitoring 6.1

In this chapter we show how to work with IBM Tivoli Monitoring 6.1. First we describe the Tivoli Enterprise Portal client, then we use some examples to describe how to work Tivoli Enterprise Portal client. Finally, we discuss IBM Tivoli Data Warehouse.

This chapter has the following sections:

- Understanding Tivoli Enterprise Portal client
- Working with Tivoli Enterprise Portal

4.1 Understanding Tivoli Enterprise Portal client

The Tivoli Enterprise Portal client provides a user interface for IBM Tivoli Monitoring 6.1. In this section, we cover how to get logged on to Tivoli Enterprise Portal and describe what we see.

4.1.1 Launching Tivoli Enterprise Portal

As we discussed in 2.2.2, "Launching Tivoli Enterprise Portal" on page 77, we can access Tivoli Enterprise Portal as either a desktop or Web-based application. The desktop version, which requires installing the client on a workstation, gives you more area to configure the workspace and requires more maintenance than Web-based. The Web-based is available via Internet Explorer and can be accessed by any workstation that has access to Tivoli Enterprise Portal Server.

You can use the following to launch Tivoli Enterprise Portal:

- "Launching Tivoli Enterprise Portal from Internet Explorer" on page 77
- "Launching Tivoli Enterprise Portal Client desktop application" on page 80

4.1.2 Tivoli Enterprise Portal components

After logging on to the Tivoli Enterprise Portal, we see the window shown in Figure 4-1.

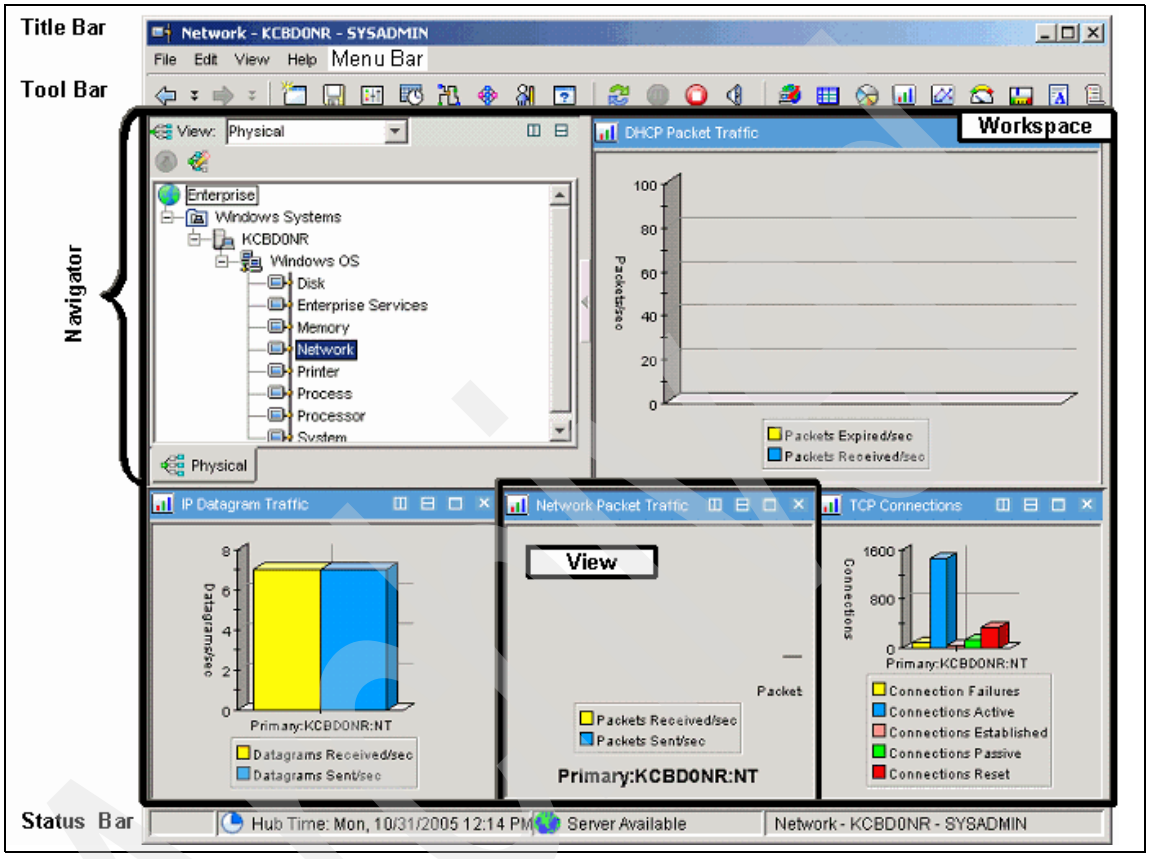

Figure 4-1 Tivoli Enterprise Portal desktop application

The three main components in Tivoli Enterprise Portal are the Navigator, workspace, and views.

Navigator

You can navigate through this tree view of the monitored environment by clicking items, each of which opens a different workspace. Navigator has two view choices: physical and logical.

Physical view

This shows the network hierarchy from a system point of view. It is organized by operating platform, system name, monitoring agent, and attribute groups.

Logical view

This enables you to organize your view according your logical hierarchy. For example, you could have a Navigator view for your departments.

Workspace

The workspace is the working area of the Tivoli Enterprise Portal window. Its panes show different types of views. Every time you select a Navigator item, you change the Workspace appearance.

Views

A view is a pane in the workspace that could contain data from a monitoring agent such as a chart or table. There are non-data views such as the browser view and terminal view.

4.2 Working with Tivoli Enterprise Portal

This section walks you through some examples of working with IBM Tivoli Monitoring 6.1 using the Tivoli Enterprise Portal desktop application.

4.2.1 Creating a new workspace and adding custom views

First, we create a new workspace and add custom views.

Navigating through workspaces

Navigating means to select or expand the items under Navigator. When you select or expand an item in Navigator, its default workspace opens. A Navigator item may have multiple workspaces and it may have links to other workspaces.

Expanding and collapsing the tree

Figure 4-2 shows the first view of Navigator upon starting Tivoli Enterprise Portal.

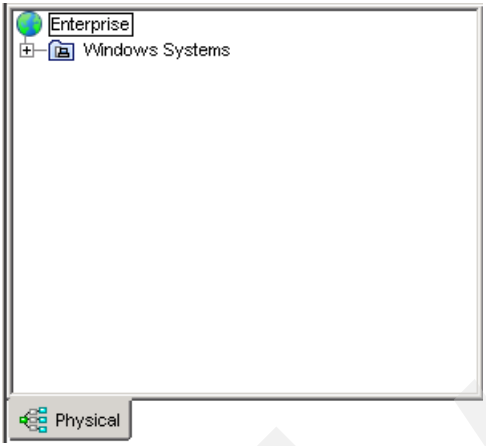

Figure 4-2 Navigator view

Expand ⊞ each level of the Navigator until you reach the lowest level (Figure 4-3). You can also collapse the Navigator tree by clicking ⊟ .

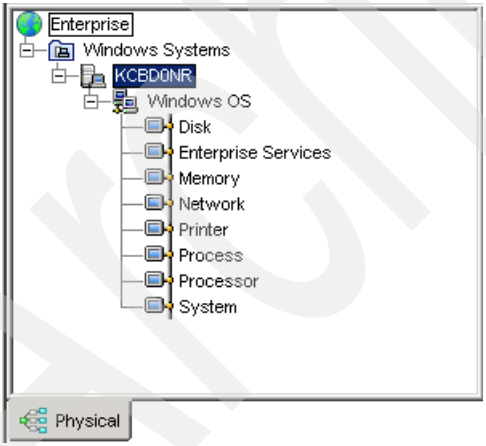

Figure 4-3 Navigator Lowest Level

Navigating through the workspaces

When you select an item under the Navigator tree, a new workspace opens. Views change every time you select a navigator item. Select Memory to open a workspace with views related to Memory attributes, as shown in Figure 4-4.

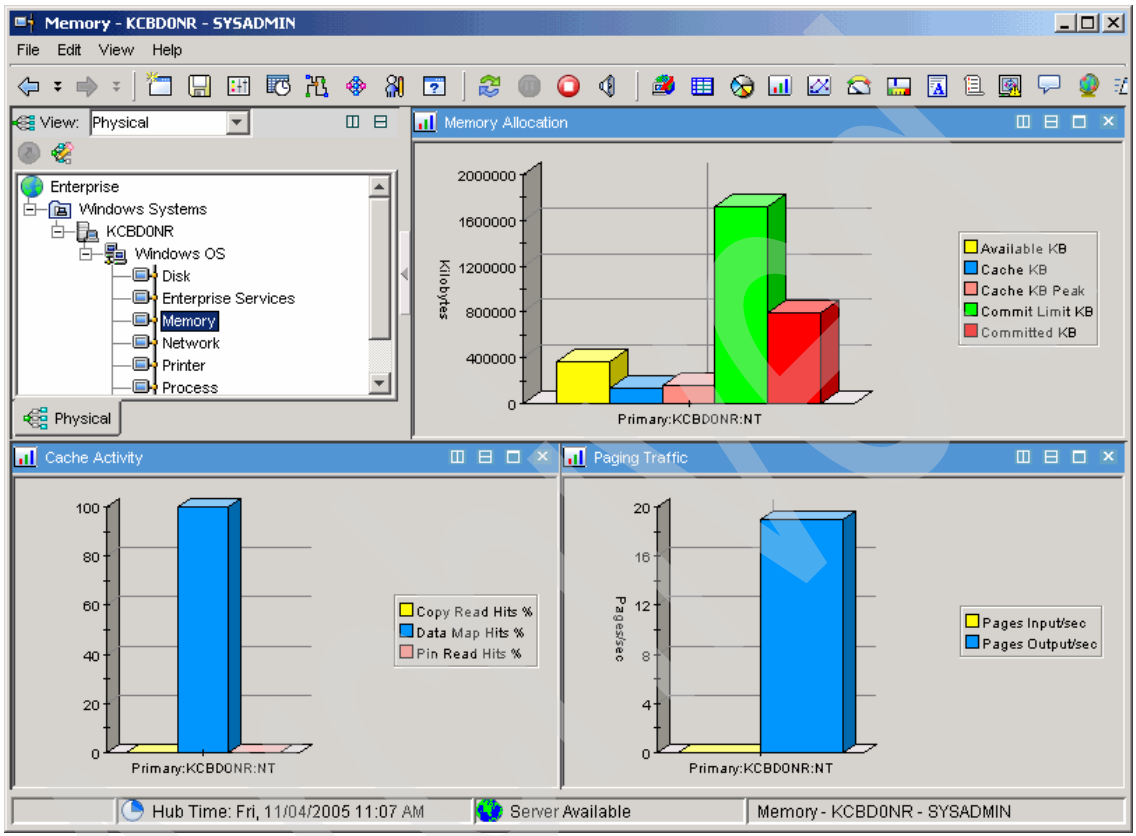

Figure 4-4 Selecting the Memory attribute

Saving the workspace

When you navigate from one workspace to another, the system warns about changing the workspace and asks whether to save. Also, you can save the workspace manually by selecting **File** → **Save Workspace**, or create a new workspace following these instructions:

1. Launch the Tivoli Enterprise Portal desktop client.
2. In the Navigator, select **Enterprise**.
3. In the menu bar, select **File** → **Save Workspace As**.

4. Click **Yes** in the Save Workspace message (Figure 4-5).

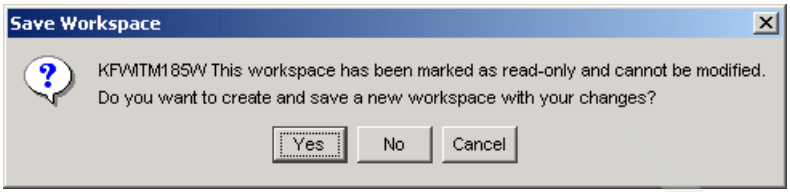

Figure 4-5 Save Workspace message

5. Type the name of this workspace as `NewWorkspace`, type a description (such as `Saving Workspace example`), and click **OK** as shown in Figure 4-6.

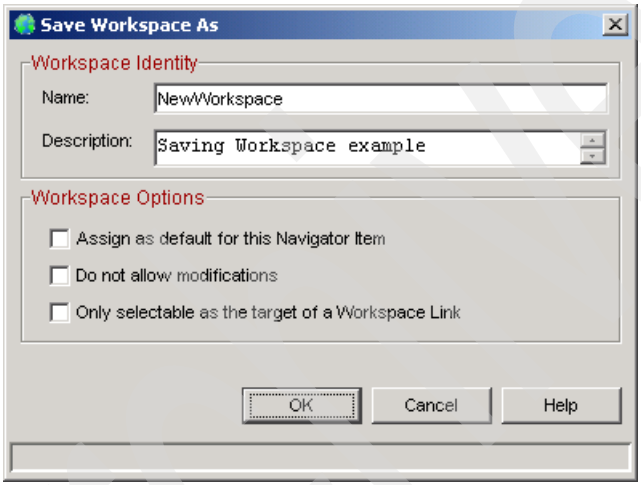

Figure 4-6 Save Workspace As

6. Close Tivoli Enterprise Portal: Select **File** → **Exit** and click **Yes.**

Note: The title bar now shows the name of the saved workspace as NewWorkpace.

Selecting the workspace

The default workspace is the System Enterprise Workspace. To select other workspaces:

1. Launch the Tivoli Enterprise Portal desktop client.

2. In the Navigator, right-click **Enterprise** and select **Workspace** → **NewWorkspace** as shown in Figure 4-7.

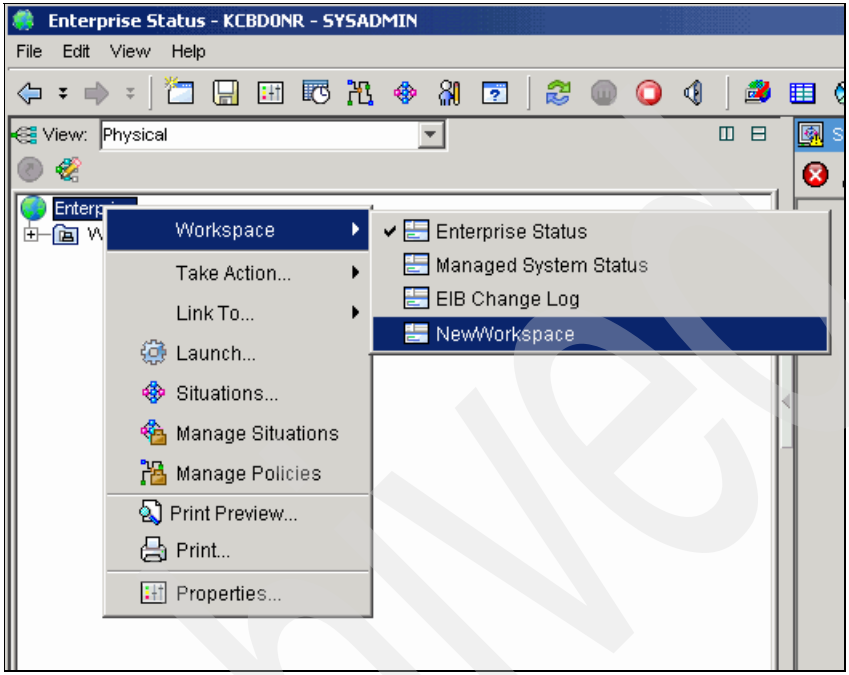

Figure 4-7 Selecting the workspace

Note: According to Navigator item we could have other workspaces.

Working with views

Several kinds of views can be added in the workspace. In the next steps we show how to add a view.

View types

The workspace has the following views:

The Tivoli Enterprise Console view displays events from the Tivoli Enterprise Console Server and can integrate them with situation events from the Tivoli Enterprise Monitoring Server.

Table view and chart views display data that the monitoring agents have gathered from the systems where they are running. They can also show data from any ODBC-compliant database you write a custom query for.

The Notepad view opens a simple text editor for writing text that can be saved with the workspace.

The Message log view shows the status of all situations distributed to the managed systems in your enterprise.

The Situation event console view shows the status of all situations associated with items on this branch of the Navigator view, and has tools for instant filtering and event handling.

The Universal message console view shows situation and policy activity, and messages received as the result of universal message generation.

The Graphic view places Navigator items as icons on a map or picture of your choosing.

The Take action view enables you to send a command to a managed system.

The Terminal view starts a 3270, 5250, or Telnet session, and enables you to write scripts for working with z/OS applications.

The Browser view opens the integrated browser for accessing Web pages.

We can add as many views to a workspace as you can easily see within the confines of the window.

Adding a non-data view

Open the workspace where you want the view.

1. In the Navigator, expand  **Windows System**.
2. Select **KCBD0NR**.
3. In the toolbar, select the  Situation Event Console view.

   Note that when you select a view, the  mouse pointer changes to  a pointing finger.

4. Click inside the view at the right side of the top plane. This view becomes a Situation Event Console view, as shown in Figure 4-8.

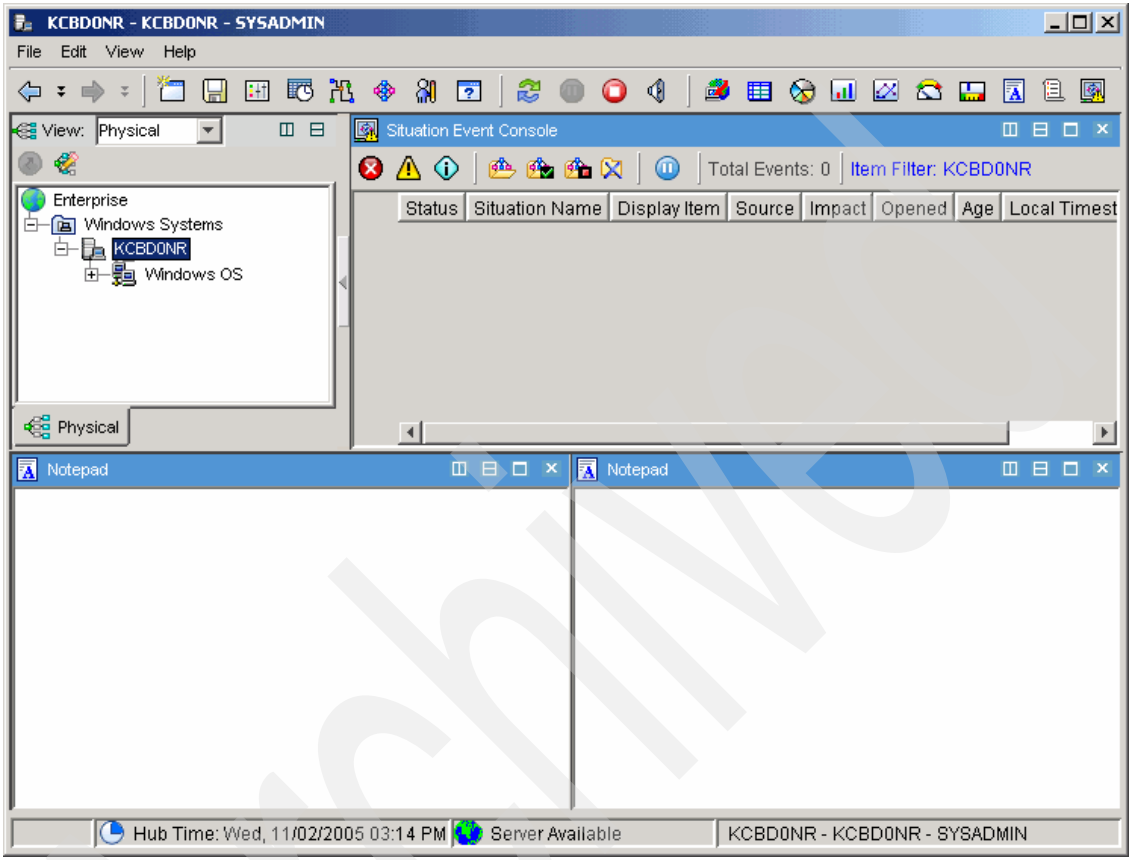

Figure 4-8 Adding a view

5. Click **File** → **Save Workspace** to save that change.

4.2.2 Working with queries

The chart and tables views show the attribute values from Tivoli Monitoring Agents or ODBC data source. Your IBM Tivoli Monitoring products come with queries that are used to populate the table and chart views in workspaces. When we add a table or a chart view over a non-data view (as Message Log or Notepad view) we have to define the query. So before we show you how to add a data view, we install IBM Tivoli Monitoring Agent for Databases.

Working with data view

This section shows how to add a view that queries for Monitoring Agent data.

Adding table view

1. In the Navigator, expand **Windows System**.
2. Select **KCBD0NR**.
3. In the toolbar, click the Table view.
4. Click inside the view at the left side of the bottom plane. This opens the Select option window (Figure 4-9). Click **Yes**.

Figure 4-9 Assigning a query

5. In Properties - KCBD0NR (Figure 4-10), select **Click here to assign a query** in the middle of the window.

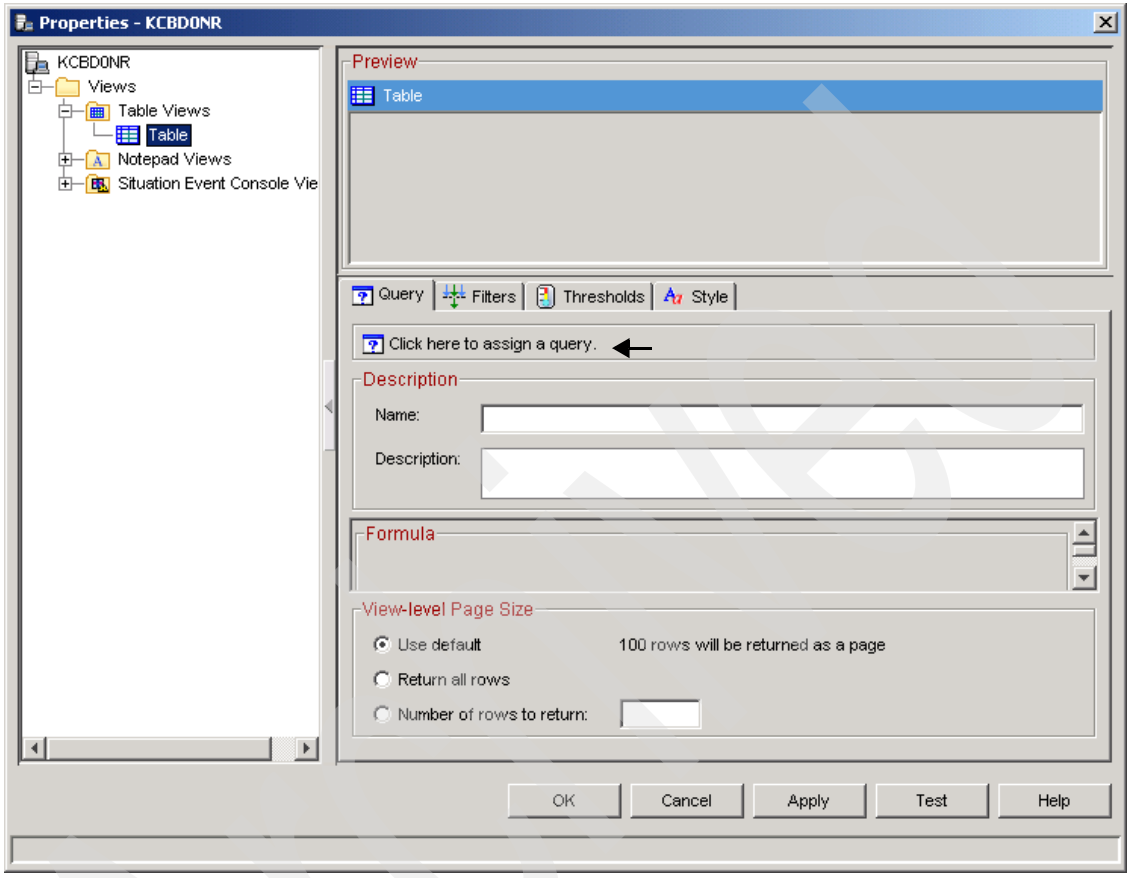

Figure 4-10 Click here to assign query

6. The Query editor opens as shown in Figure 4-11.

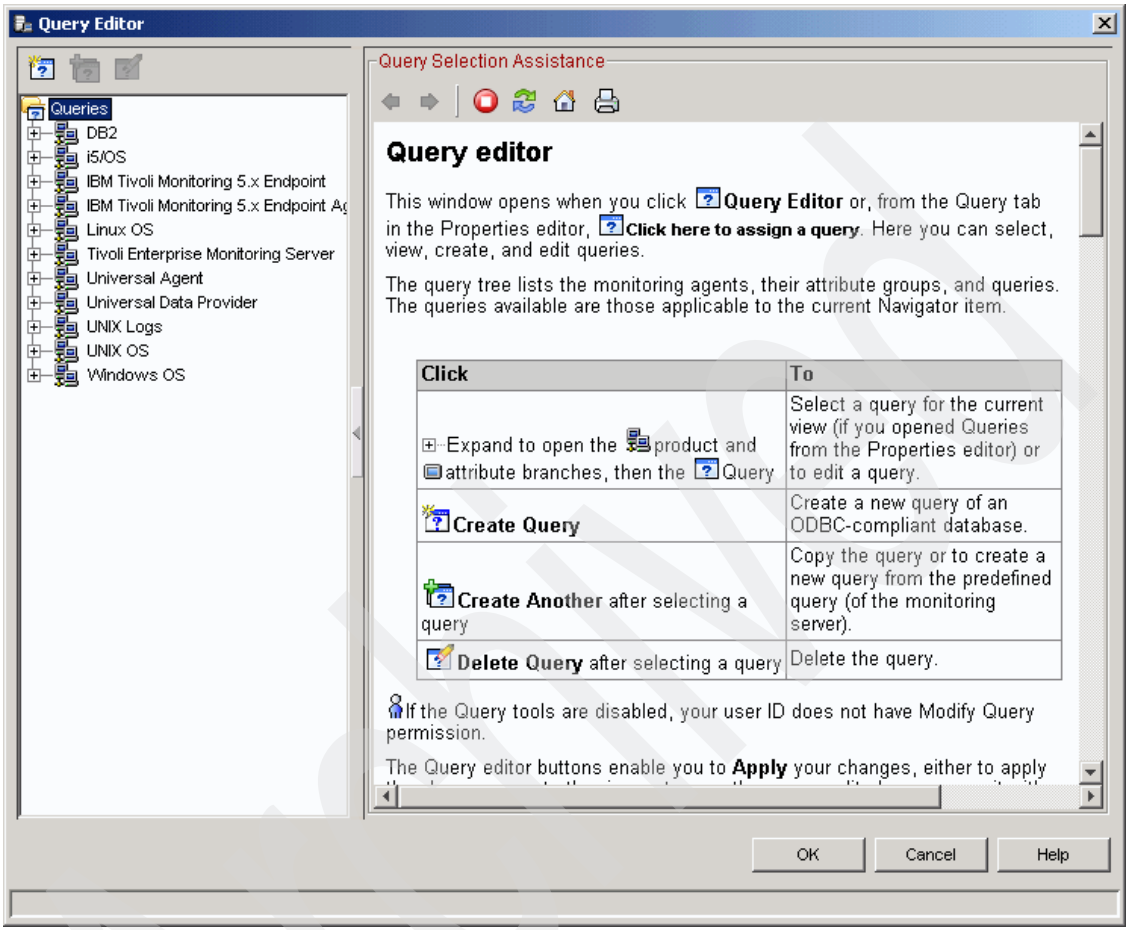

Figure 4-11 Query Editor

7. Select the **Create Query** icon to open the Create Query window. Name that query `Service_status_example` and choose **Service status.**

> **Attention:** Changing queries affects every view where this query is being used. Be careful because it can change other users' views.

8. In the Category, select **Windows OS**.

9. For Data Sources, select **TEMS** as shown in Figure 4-12 on page 232 and click **OK**.

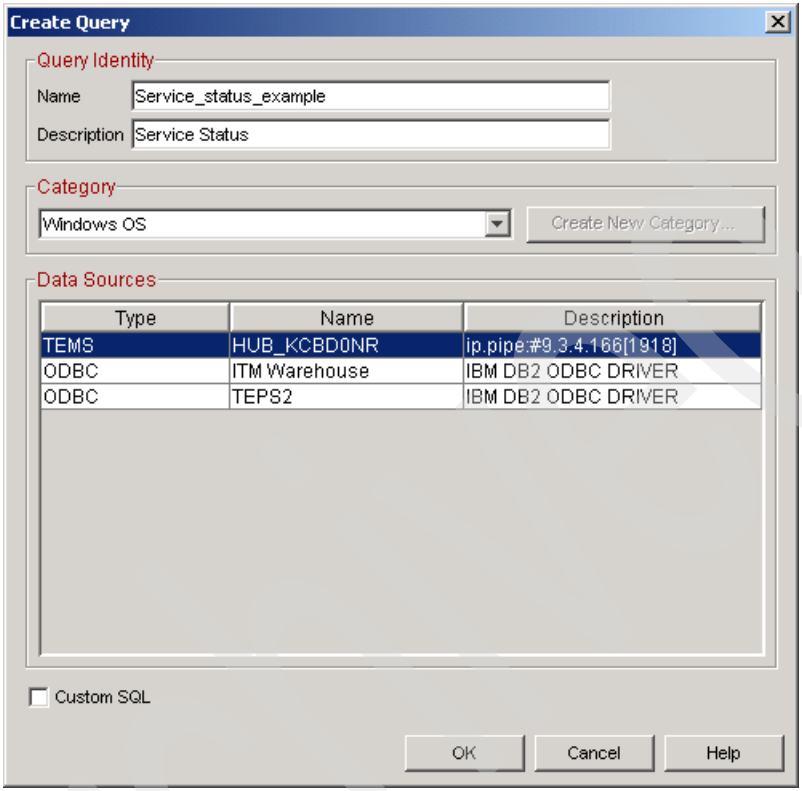

Figure 4-12 Create Query

10. The Select attribute window opens. Select Attribute Group **NT Services** and press the CTRL key to also select Attribute items **Current State, Display Name, Server Name**, and **Service Name**, as shown in Figure 4-13. Click **OK** to finish the selecting attributes.

> **Note:** Monitoring agents are made up of attributes that represent the properties of systems or networks, such as the amount of CPU usage or the message ID.
>
> Attributes are organized into attribute groups. The attributes in a group can be displayed in a table view or chart view or used to specify a condition for testing in a situation. When you open the view or start the situation, data samples are taken of the selected attributes. IBM Tivoli Monitoring comes with a set of common attribute groups that can be applied to any managed system.

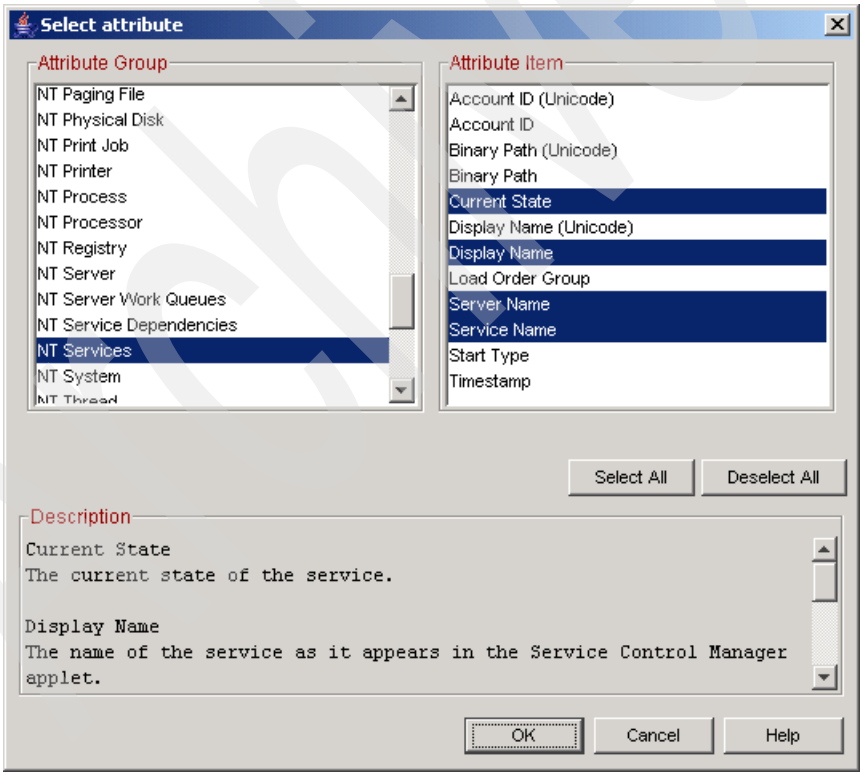

Figure 4-13 Selecting attributes

11. The new query now appears in the Query Editor (Figure 4-14), and it must be configured.

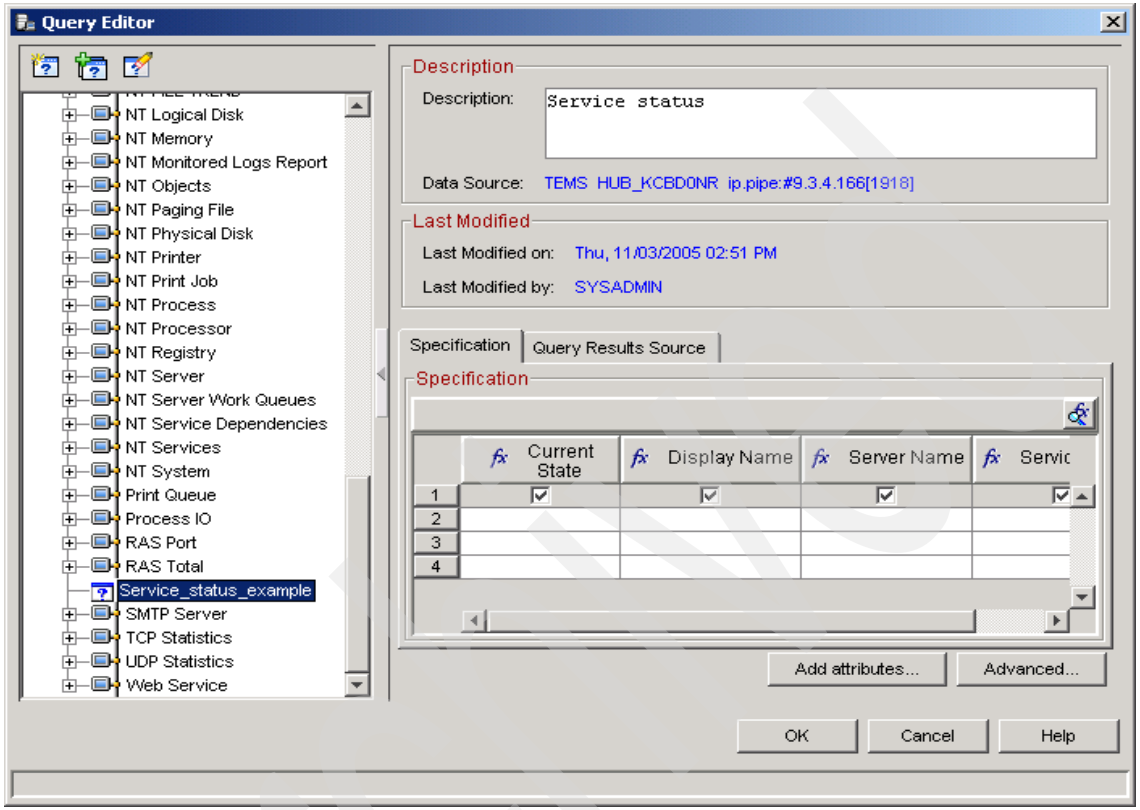

Figure 4-14 New query

12. In Specifications, click the **Current State** column and change the operator to **!= (Not equal)** and type **Stopped**.
13. Click the **Server Name** column. Type `$NODE$` and leave the operator as == (equal signs), as shown Figure 4-15.
14. Click **Advanced**.

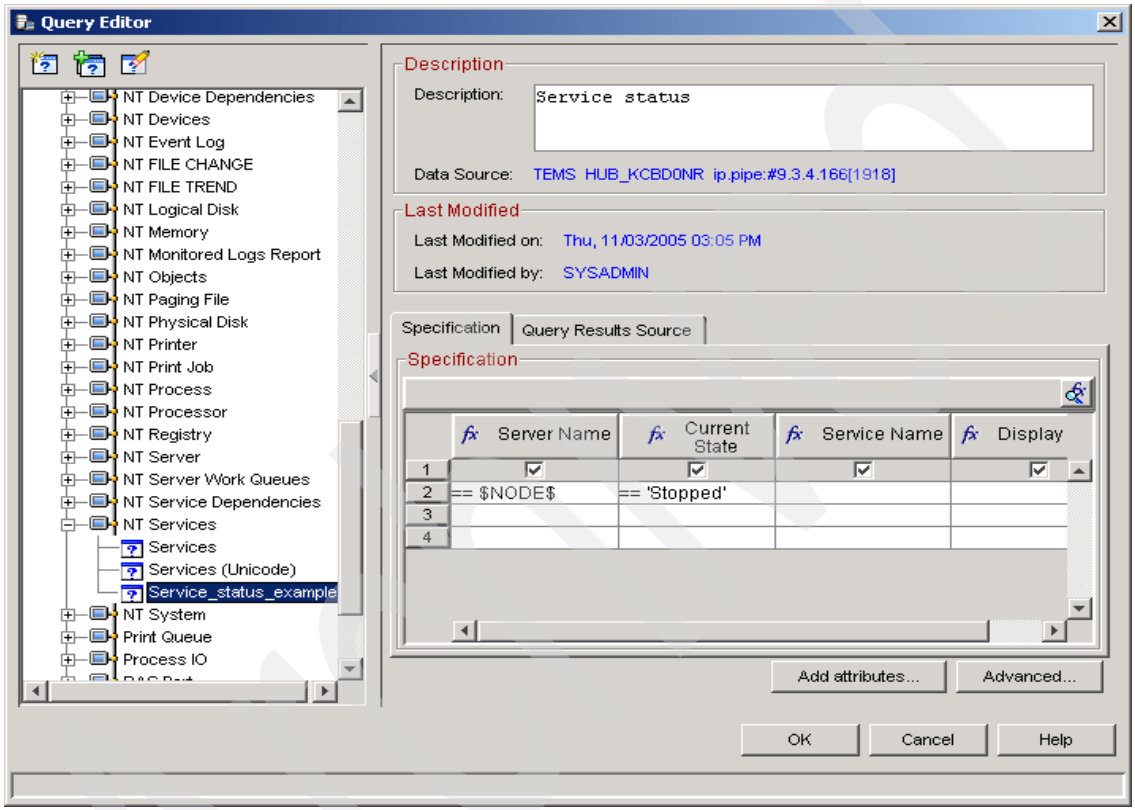

Figure 4-15 Query Editor Specification

15. In the Advanced Options window, sort by **Ascending** and **Display_Name** (Figure 4-16). Click **OK**.

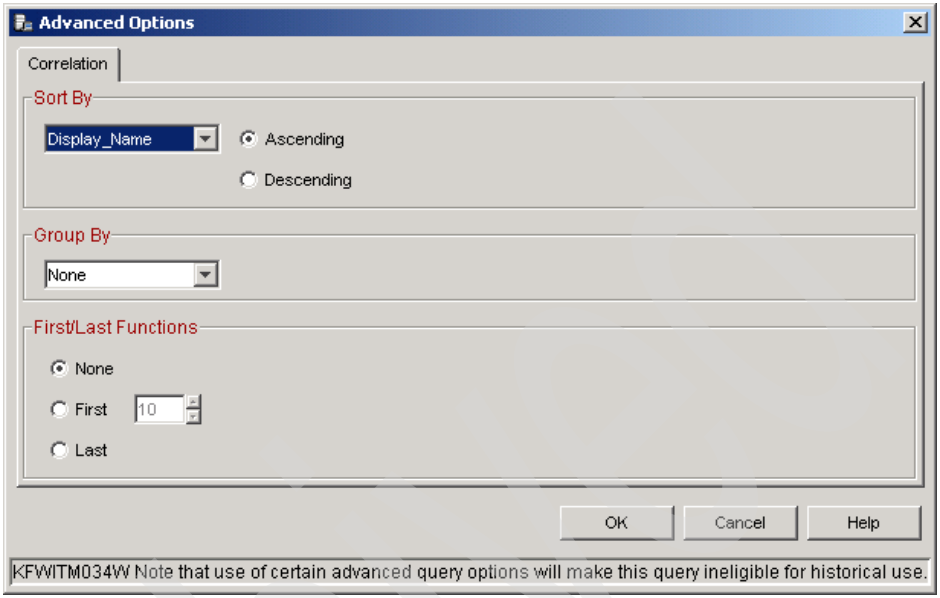

Figure 4-16 Advance Options

16. The Preview shows any Service with Service Status as Stopped.

17. We can filter this to track certain services' status. Click the **Filters** tab. Under Service Name select **==** and type `Messenger` as shown in Figure 4-17.

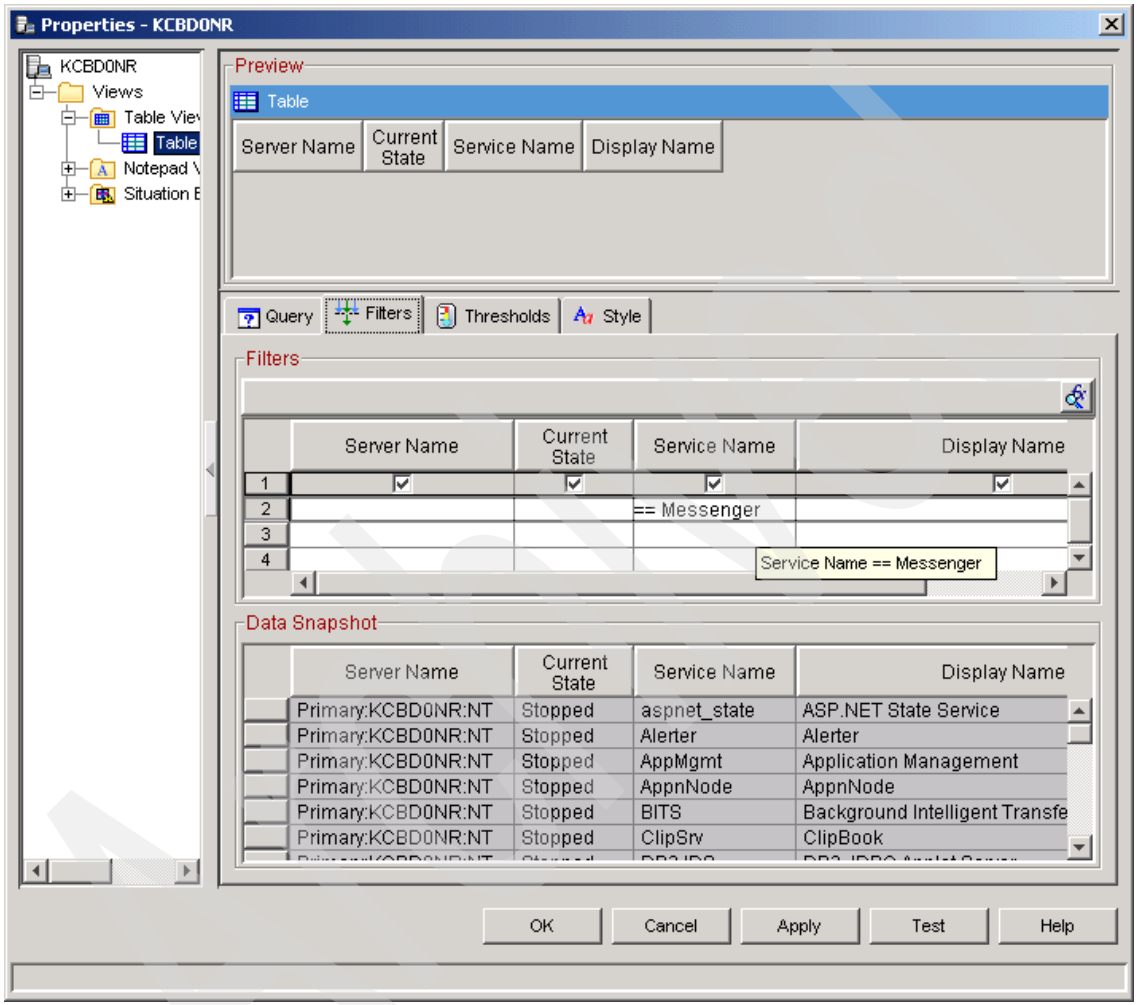

Figure 4-17 Filter Service Name

18. Click the **Style** tab to change the table name. In the Options, select the **Show** check box, in the Title types select **Service Status Stopped**, and click **OK**.

Now we have the Services Status Stopped table view added. Select **File** → **Save Workspace** to save this last configuration.

Because Messenger service is running, we cannot see any rows in table view, as shown Figure 4-18.

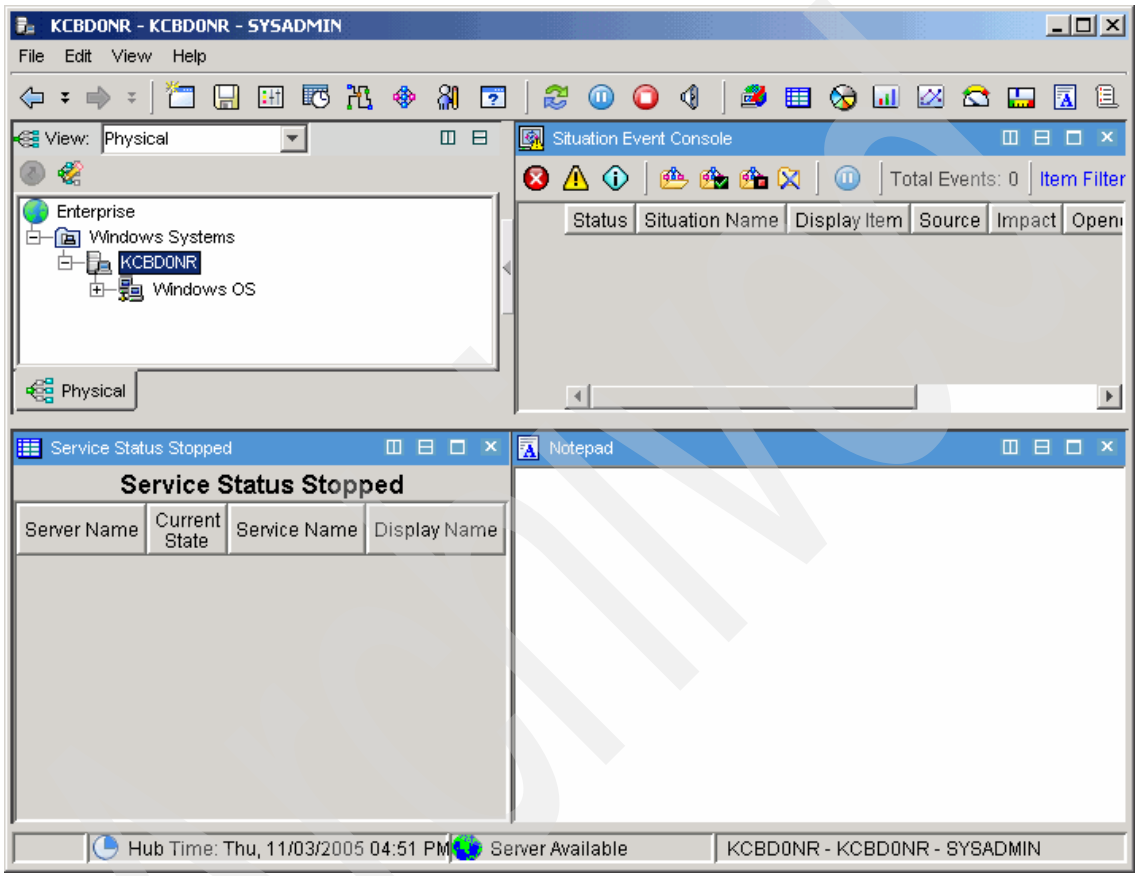

Figure 4-18 New view - Service Status Stopped

We can reproduce the service stopping to see the view behavior.

1. In Windows click **Start** → **Run** and type `cmd` in the Open window.
2. Click **OK**.
3. At the command prompt, type `net stop messenger`. The following message appears:

```
The Messenger service is stopping.
The Messenger service was stopped successfully.
```

4. Open Tivoli Enterprise Portal Client (Figure 4-19), which shows the service listed as stopped.

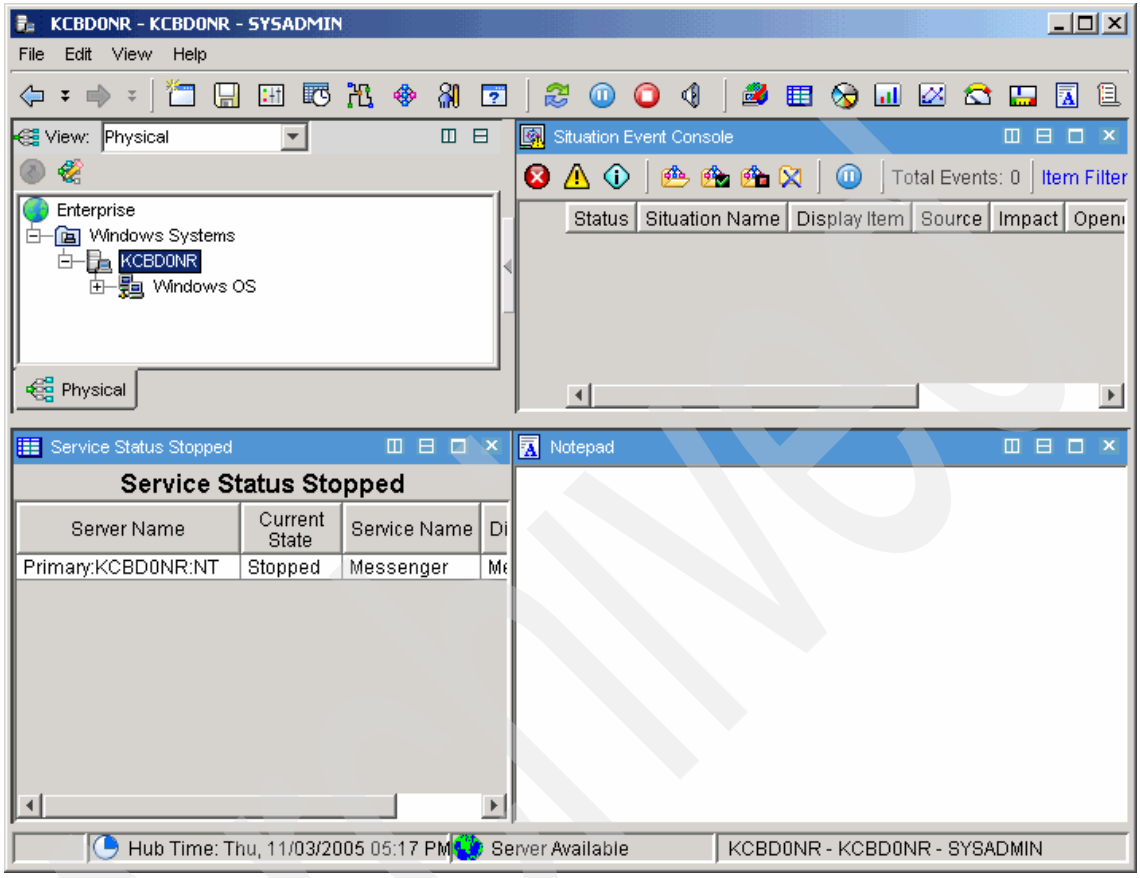

Figure 4-19 Service stopped

Adding a chart view

Now that we have a table view, we can add a chart view in our workspace.

1. In Tivoli Enterprise Portal, select the Pie Chart view and click in the right side at the bottom. Answer **Yes** to the Assign query now question.
2. In the Properties window, click **Click here to assign a query**.
3. In the Query Editor Navigator, expand **Windows OS** → **NT Logical Disk** → **Logical Disk** and click **OK.**
4. Select the **Filters** tab to filter what we want to show in our pie chart.

Note: Unlike Queries, using Filters does not affect other views.

5. Select **%Used** and **%Free.** Under Disk Name select **==** and type `C:`
6. Select the **Style** tab to name the view. In Options, select the **Show** check box and in the Text box type `Disk Space`. Click **OK** to add this view to our workspace as shown in Figure 4-20.

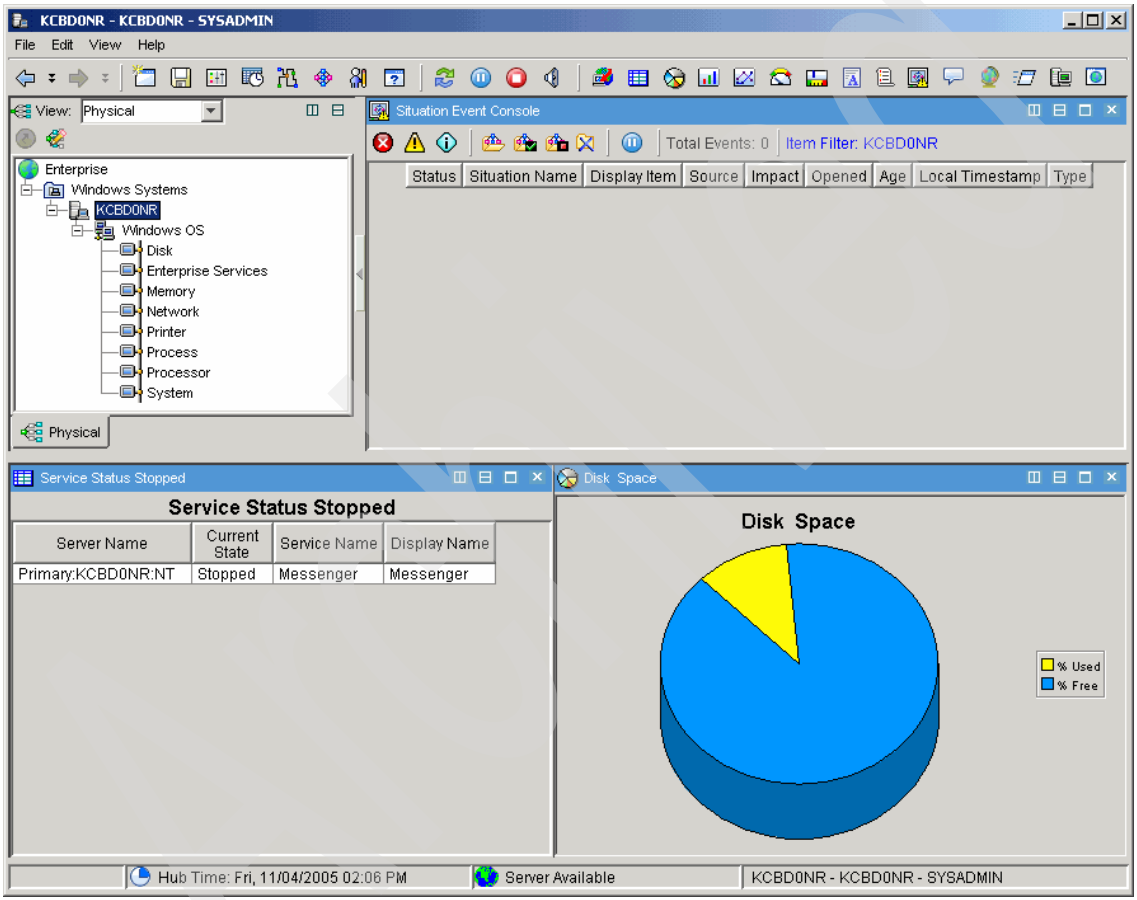

Figure 4-20 Disk Space Chart Pie view

Installing IBM Tivoli Monitoring Agent for Databases

Because we have only one Monitor Agent running, in this next step we install Monitoring Agent for Databases DB2:

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

2. Access the IBM Tivoli Monitoring 6.1 installation image. In our case, it is under C:\ITM61_image\db_agent.

> **Tip:** You can also install IBM Tivoli Monitoring 6.1 Databases from the CD image.

3. Open the **Windows** folder and launch **setup.exe**. This launches the IBM Tivoli Monitoring for Databases - InstallShield Wizard.
4. In the Welcome window, click **Next**.
5. In the Software License Agreement window, click **Accept** to accept the license information.
6. Expand each of the four sections and check the box that corresponds to the DB2 Agent, as shown in Figure 4-21. Click **Next**.

> **Attention:** Do not unselect Tivoli Enterprise Monitoring Agent for Framework.

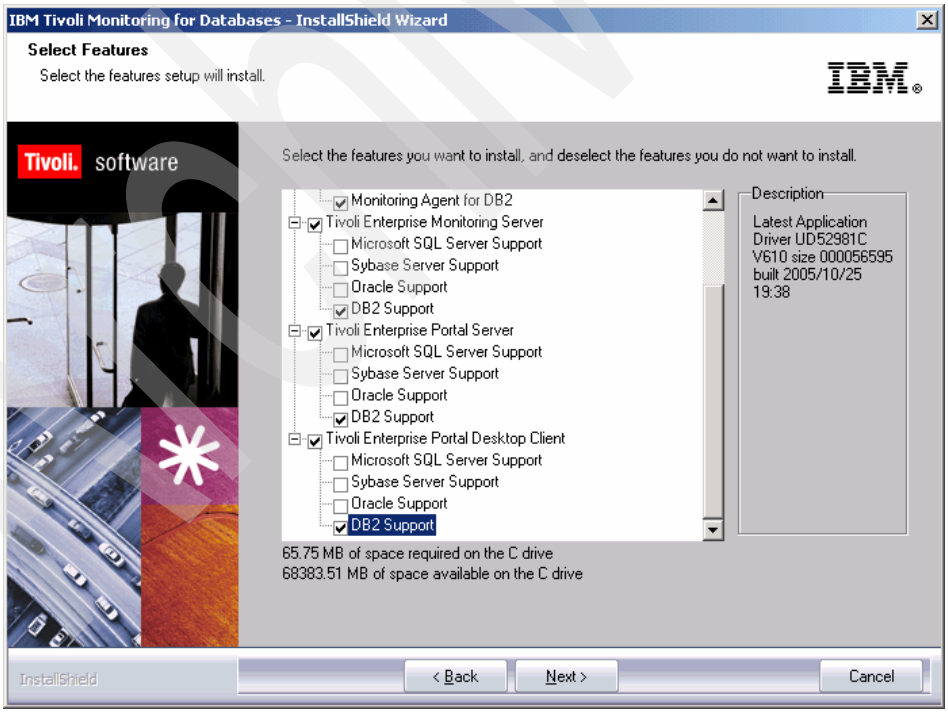

Figure 4-21 Select Features

7. Select **Monitoring Agent DB2** in Agent Deployment and click **Next**.
8. Click **Next** in Start Copying Files.
9. After the files finish copying, we need to configure the components. Click **Next** in Setup Type window as shown in Figure 4-22.

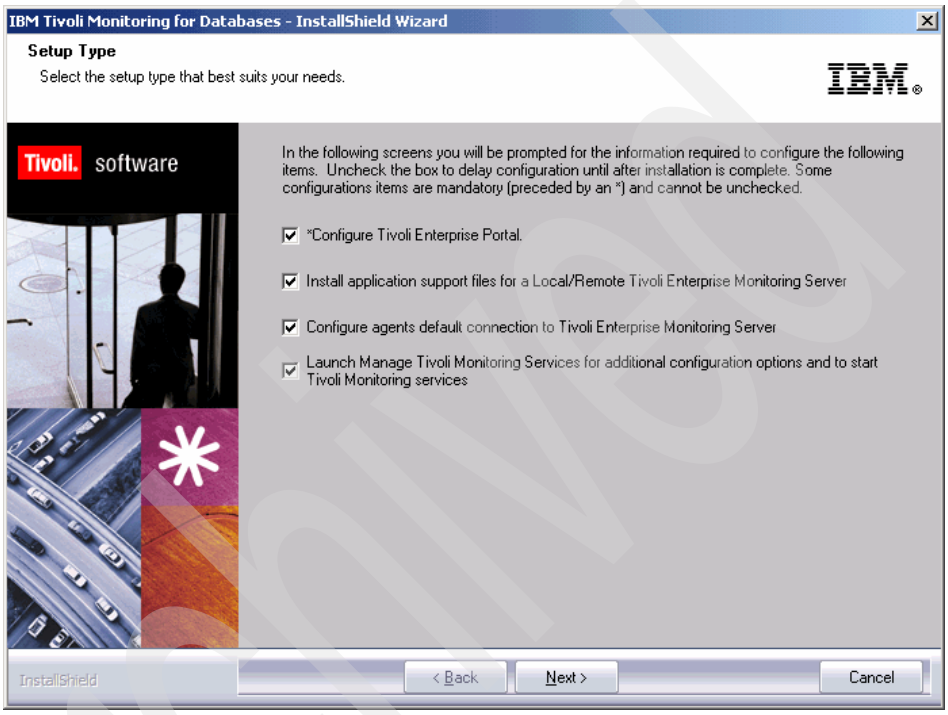

Figure 4-22 Setup Type

10. Click **Next** in Define TEP Host Information.
11. After a while, the Tivoli Enterprise Monitoring Server Configuration windows pop up. Click **OK** to accept the TEMS configuration, and **OK** again in Hub TEMS Configuration window.
12. Click **OK** in Add application support to the TEMS window and **OK** again in Manage Tivoli Enterprise Monitoring Services.

13. Click **OK** in Select the application support to add to the TEMS (Figure 4-23). This adds DB2 Support to TEMS.

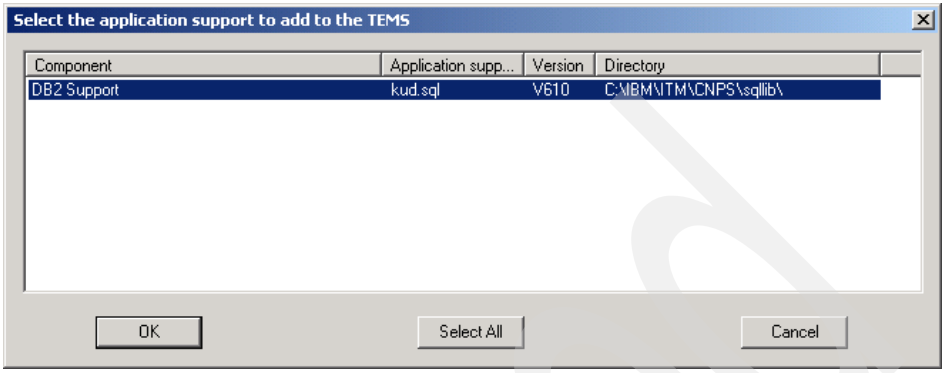

Figure 4-23 Select the application support to add to the TEMS

14. In the Application support addition complete window, which shows installation status. `rc:0` (Figure 4-24) indicates that no error has occurred. Click **Next**.

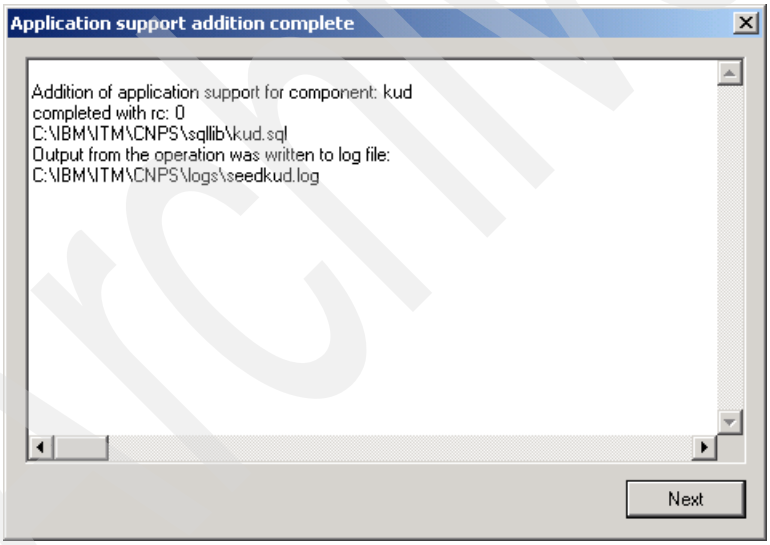

Figure 4-24 Application support addition complete

15. Select **OK** for Configuration Defaults for Connecting to a TEMS server and **OK** in Configuration Defaults for Connecting to a TEMS IP.PIPE Settings.

16. The IBM Tivoli Monitoring Services will be recycled and we can click **Finish**.

After the installation finishes, the Tivoli Enterprise Monitoring Services windows pops up, showing a new line (Figure 4-25), but there is no (running man) next to it and the Task/SubSystem column shows `Template` for this item. We use this item to configure a database instance.

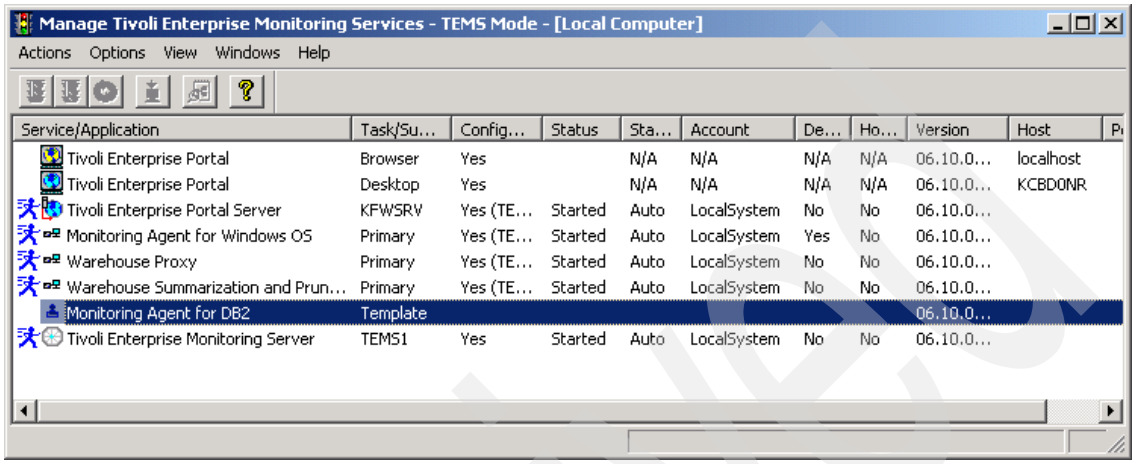

Figure 4-25 Monitoring Agent for DB2 Template

Configuring IBM Tivoli Monitoring Agent for Databases DB2

To configure the agent:

1. Right-click the **Monitoring Agent for DB2** and select **Configure Using Defaults**.
2. In Monitoring Agent for DB2, type `DB2` as the DB2 instance name and click **OK** as shown in Figure 4-26.

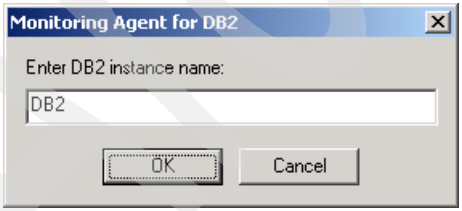

Figure 4-26 Enter DB2 instance name

3. Another service appears in Manage Tivoli Enterprise Monitoring Service, as shown in Figure 4-27.

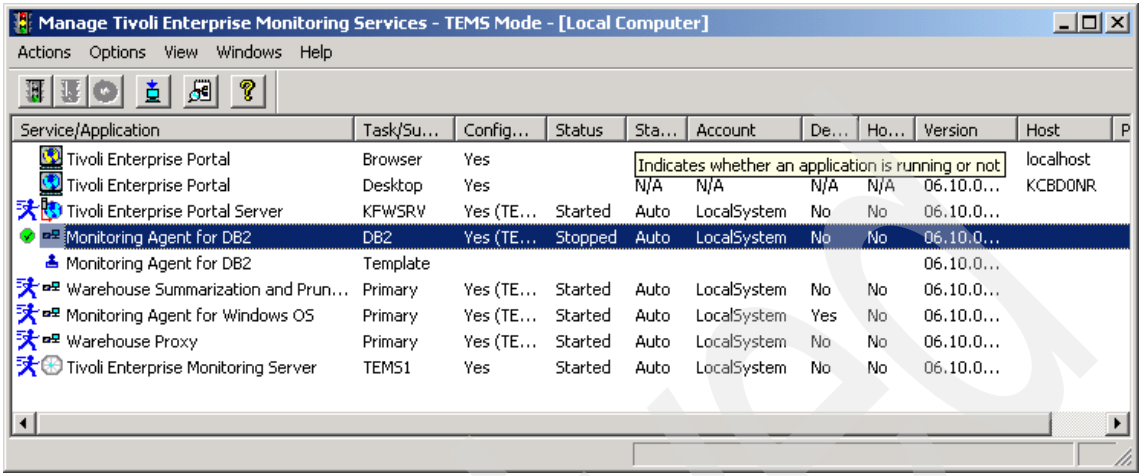

Figure 4-27 Monitoring Agent for DB2 instance DB2

4. To start the new Monitoring Agent for DB2, right-click **Monitoring Agent for DB2** and select **Change Startup,** as shown in Figure 4-28.

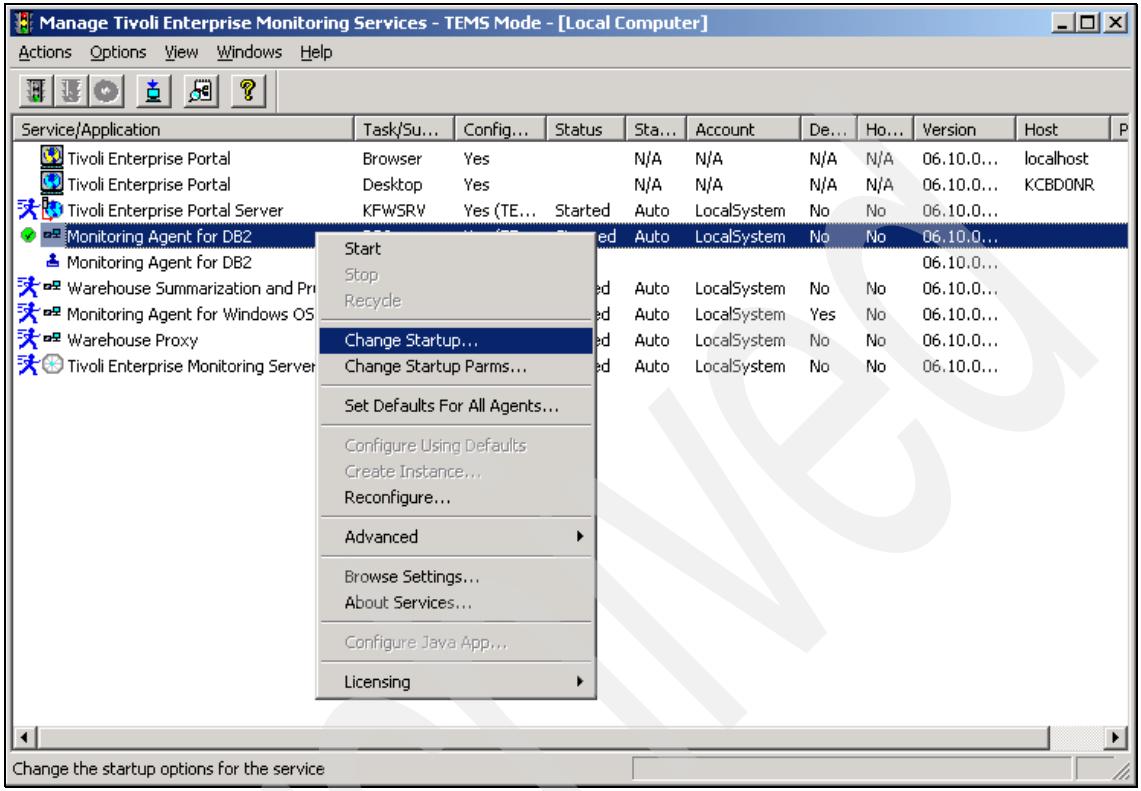

Figure 4-28 Change Startup

5. In the Service Startup for Monitoring Agent for DB2 window, click **This Account**, enter the user ID `db2admin`, password `itm61rbdg`, and click **OK** as shown in Figure 4-29.

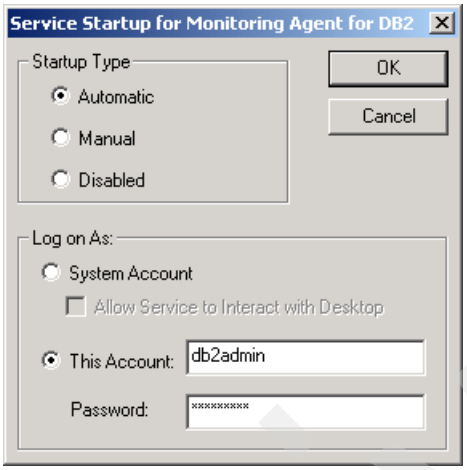

Figure 4-29 Service Startup for Monitoring Agent for DB2

6. The Service Logon Change message pops up (Figure 4-30) explaining that service will start with another account. Click **OK**.

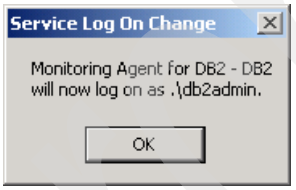

Figure 4-30 Service Log On Change

7. Double-click **Monitoring Agent for DB2** to start it.

Now we return to Tivoli Enterprise Portal client. Notice that a green icon appears in Navigator view (Figure 4-31). This means that updates are pending in the Navigator tree.

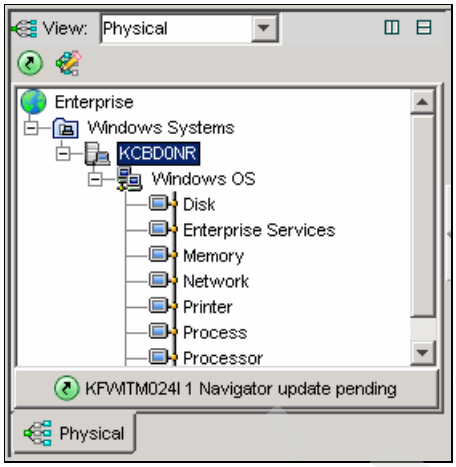

Figure 4-31 Navigator update pending

When one Monitoring Agent is added or deleted, refresh the Navigator.

Note the new Monitoring Agent to see that there is a new agent listed in Navigator as shown in Figure 4-32.

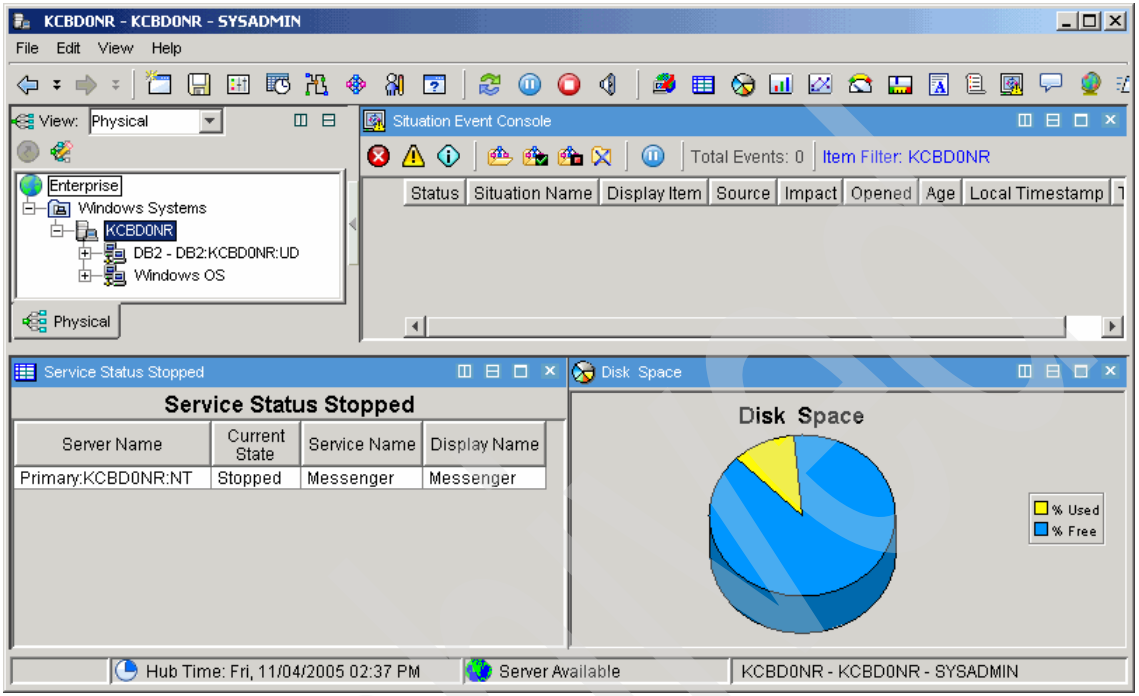

Figure 4-32 New agent add to Navigator

Finally we can add a table view with some information about Monitoring Agent for Databases, but before we do that we need create another view.

The view toolbar has these tools for creating the view:

- Split view horizontally
- Split view vertically
- Maximize the view
- Close the view

Follow these instructions in order to divide and add this new view:

1. Click to split the Service Status Stopped view horizontally.

Note: We have two views with the same query, so before we add a table view, we should clean the previous query. We can add a Notepad view to clean it.

2. Click Notepad view and click **Service Status Stopped.1** view. Now we have a Notepad view as show in Figure 4-33.

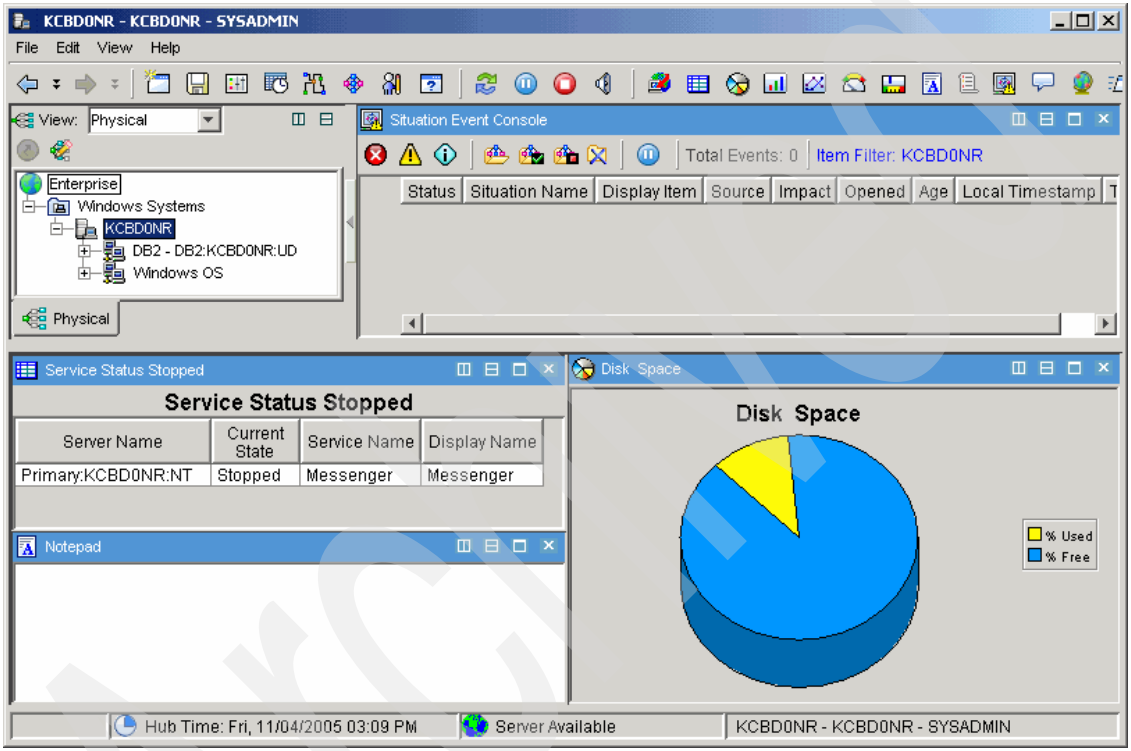

Figure 4-33 Notepad view.

3. Select Table view and click the Notepad view.
4. Click **Yes** for the “Assign query now” question.
5. In the Properties window, click **Click here to assign a query**.
6. In the Query Editor, expand **DB2** → **KUDINFO00** → **System Overview** and click **OK.**

7. Click the **Filters** tab, and select only **Node Name**, **db2 status**, and **db2start time** as shown in Figure 4-34.

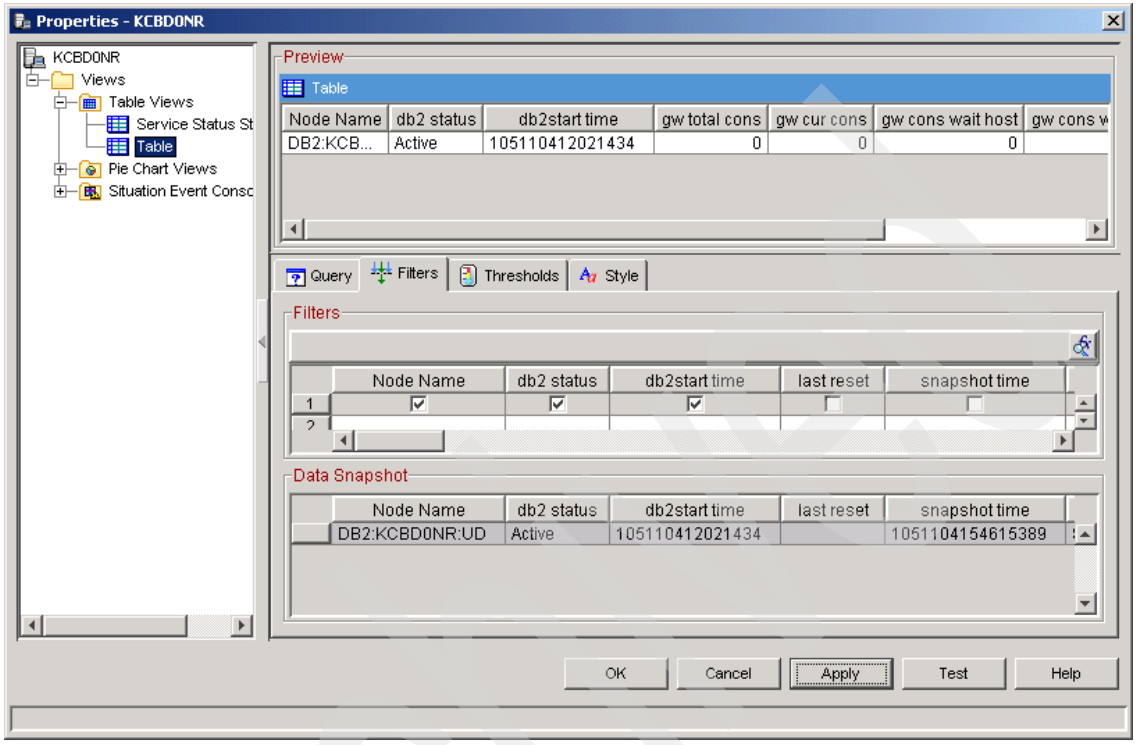

Figure 4-34 Selecting Filters

8. Click the **Style** tab, select the **Show** check box, and type `DB2 Status` for Title.
9. Click **OK** to see the new view as shown in Figure 4-35.

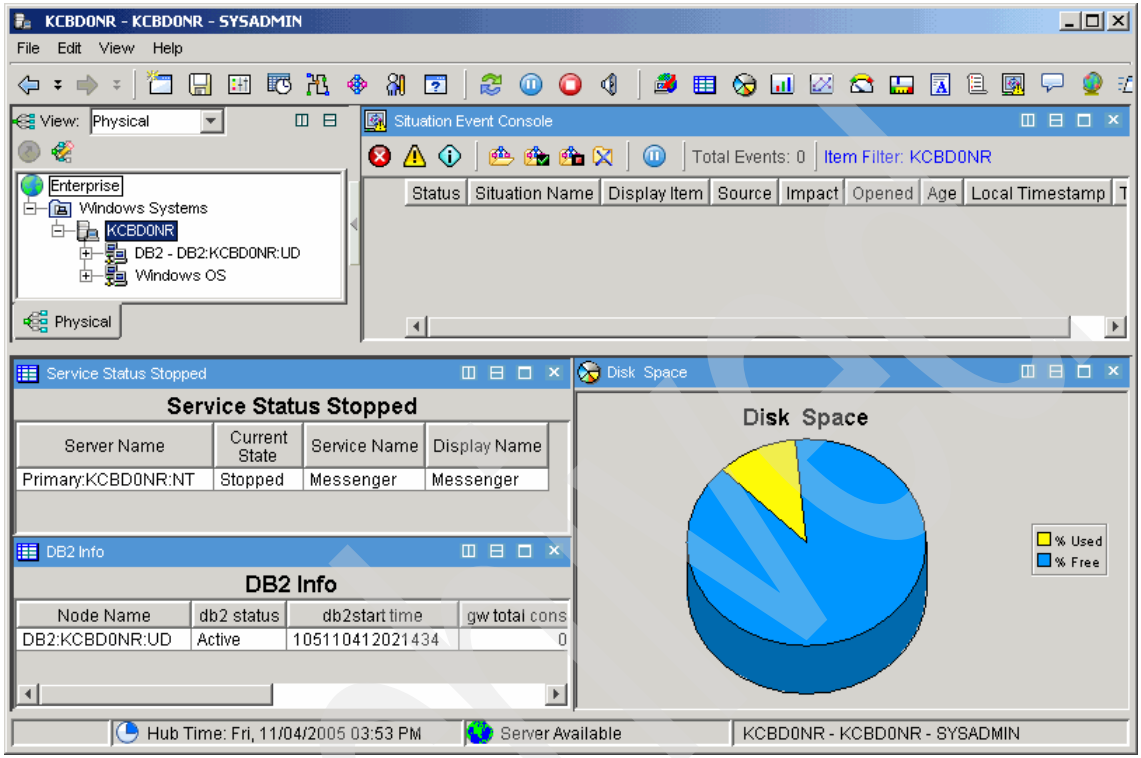

Figure 4-35 DB2 Info view

Working with thresholds

In table views, we can add thresholds to highlight cells whose values meet the threshold set. We also can have thresholds for circular gauge charts and linear gauge charts.

In this example, we will split vertically the DB2 Info table to add another table view and work with a threshold.

1. Click to split the DB2 Info view horizontally.
2. Click Notepad view, and click **DB2 Info.1.**
3. Select Table view and click the Notepad view.
4. Click **Yes** for “Assign query now.”
5. In the Properties window, select **Click here to assign a query**.

6. In the Query Editor, expand **Windows OS** → **NT Process** → **Process Overview** and click **OK.**
7. Click the **Filters** tab, and select only **Node Name**, **db2 status**, and **db2start time**.
8. Click the **Thresholds** tab and set the Thresholds values for **%User Time** as shown in Figure 4-36.

		Process Name	ID Process	% User Time
1	Critical			> 20
2	Warning			> 10
3	Informational	abc == Idle		< 5

Figure 4-36 Thresholds values

9. Click the **Style** tab, select the **Show** check box, and type `Process %User Time` for the title. Click **OK** to add this new view.

10. In Process %User Time, click **%User Time** to order the values.

Now we can see the thresholds working as shown in Figure 4-37.

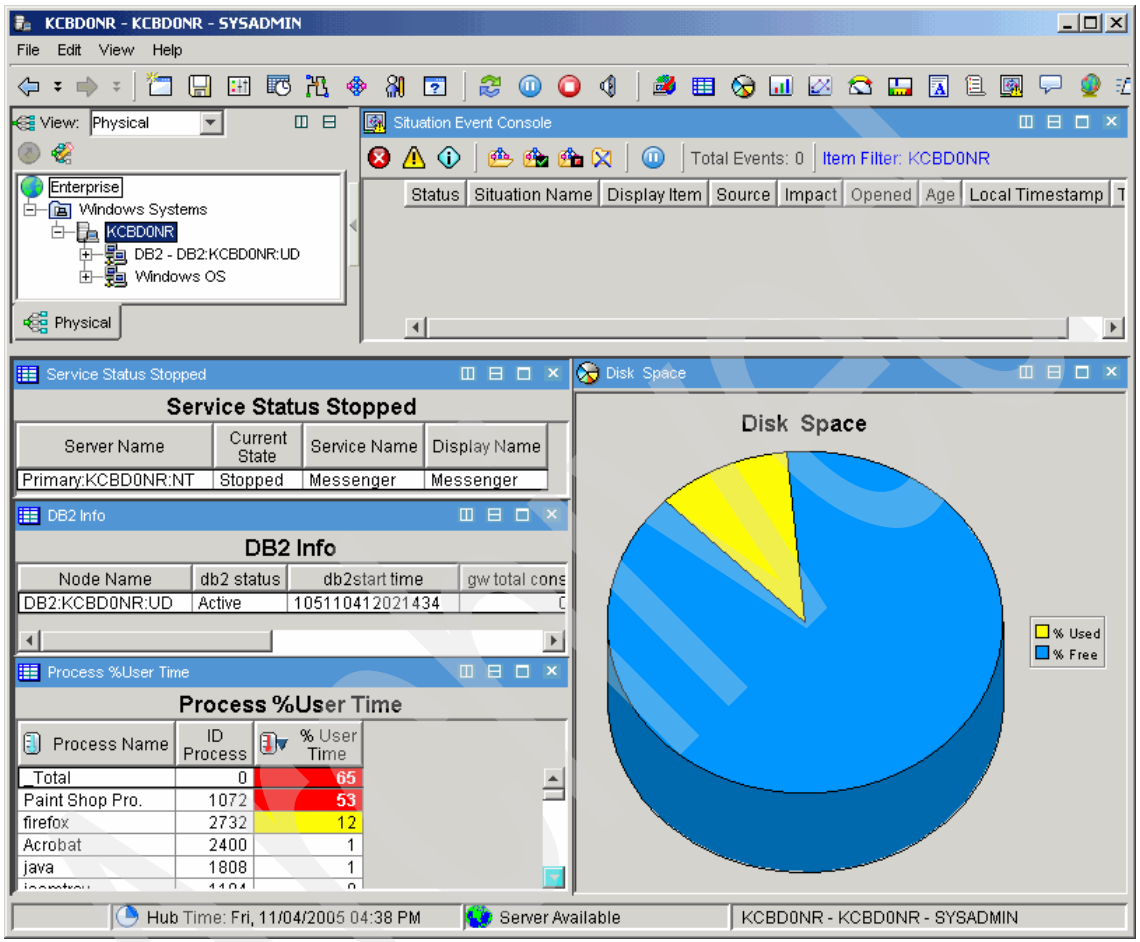

Figure 4-37 Thresholds

4.2.3 Working with a situation and events

A situation describes conditions you want to test on a managed system. When you start a situation, Tivoli Enterprise Portal compares the situation with the values collected by the Tivoli Enterprise Monitoring Agent and registers an event if the conditions are met. You are alerted to events by indicator icons that appear in the Navigator.

Create a situation

Each Tivoli Enterprise Monitoring Agent has a set of predefined situations ready to use. You can also create and customize your own situations to monitor specific conditions in your enterprise. If a situation already exists that is similar to one you want, you can copy the original and edit the copy.

Open the Situation Editor

There are several ways to open the Situation Editor:

- In Tivoli Enterprise Portal Toolbar, click **Situation**.
- Right-click a Navigator item and click **Situation**.
- Right-click the event item in the Navigator and click **Edit Situation**.
- Right-click an open event in the event console view or in the event flyover list and, click **Edit Situation**.

Related publications

The publications listed in this section are considered particularly suitable for a more detailed discussion of the topics covered in this redbook.

Other publications

These publications are also relevant as further information sources:

- *IBM Tivoli Monitoring Installation and Setup Guide*, GC32-9407
- *IBM Tivoli Monitoring Administrator's Guide, SC*32-9408
- *IBM Tivoli Monitoring User's Guide, SC*32-9409
- *Introducing IBM Tivoli Monitoring, V6.1.0,* GI11-4071

Online resources

These Web sites and URLs are also relevant as further information sources:

- DB2 Fix Pack web site

  http://www.ibm.com/software/data/db2/udb/support/downloadv8.html

- Microsoft SQL server drivers web site

  http://www.microsoft.com/sql/downloads/default.asp

- Oracle ODBC drivers web site

  http://www.oracle.com/technology/software/tech/windows/odbc/htdocs/utilsoft.html

- IBM Java JRE web site

  http://www.ibm.com/developerworks/java/jdk

- IBM Tivoli Support web site

  ftp://ftp.software.ibm.com/software/tivoli_support/patches/

How to get IBM Redbooks

You can search for, view, or download Redbooks, Redpapers, Hints and Tips, draft publications and Additional materials, as well as order hardcopy Redbooks or CD-ROMs, at this Web site:

ibm.com/redbooks

Help from IBM

IBM Support and downloads

ibm.com/support

IBM Global Services

ibm.com/services

Index

F

G

H

I

J

K

L

M

N

O

P

Q

R

S

T

U

V

W

X

Deployment Guide Series: IBM Tivoli Monitoring 6.1

(0.5” spine)
0.475”<->0.875”
250 <-> 459 pages

Deployment Guide Series: IBM Tivoli Monitoring 6.1

Redbooks

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

Covers small to large environments

Discusses best practices for a deployment plan

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

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

IBM Tivoli Monitoring 6.1 is easily customizable and provides real-time and historical data that enables you to quickly diagnose and solve issues with the new GUI via the IBM Tivoli Enterprise Portal component. This common, flexible, and easy-to-use browser interface helps users to quickly isolate and resolve potential performance problems.

The target audience for this book is IT Specialists who will be working on new IBM Tivoli Monitoring 6.1 installations.

INTERNATIONAL TECHNICAL SUPPORT ORGANIZATION

BUILDING TECHNICAL INFORMATION BASED ON PRACTICAL EXPERIENCE

IBM Redbooks are developed by the IBM International Technical Support Organization. Experts from IBM, Customers and Partners from around the world create timely technical information based on realistic scenarios. Specific recommendations are provided to help you implement IT solutions more effectively in your environment.

For more information:
ibm.com/redbooks

SG24-7188-00 ISBN 0738494208