Tivoli software

IBM

Deployment Guide Series: IBM Tivoli Monitoring V6.2

- Deployment best practices, Agent Builder, and ITM 5.x migration
- Case studies and proof of concept scenarios
- Sales engagement planning

Vasfi Gucer
Ana Godoy
Fabrizio Salustri
Ghufran Shah
John Willis

Redbooks

ibm.com/redbooks

International Technical Support Organization

Deployment Guide Series: IBM Tivoli Monitoring V6.2

February 2008

SG24-7444-00

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

First Edition (February 2008)

This edition applies to IBM Tivoli Monitoring Version 6.2.0.

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

Trademarks

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

AIX 5L™
AIX®
CICS®
Domino®
DB2®
i5/OS®
IBM®
IMS™
iSeries®
Lotus®
Netcool/OMNIbus™
Netcool®
OMEGAMON®
PartnerWorld®
pSeries®
Redbooks®
Redbooks (logo) ®
System p™
Tivoli Enterprise Console®
Tivoli®
TME®
ViaVoice®
WebSphere®
z/OS®
zSeries®

The following terms are trademarks of other companies:

SAP R/3, SAP, and SAP logos are trademarks or registered trademarks of SAP AG in Germany and in several other countries.

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

IT Infrastructure Library, IT Infrastructure Library is a registered trademark of the Central Computer and Telecommunications Agency which is now part of the Office of Government Commerce.

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

AMD, AMD Opteron, the AMD Arrow logo, and combinations thereof, are trademarks of Advanced Micro Devices, Inc.

Java, JavaScript, JDBC, JMX, JRE, J2EE, Solaris, and all Java-based trademarks are trademarks of Sun Microsystems, Inc. in the United States, other countries, or both.

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

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

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

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

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

Preface

IBM® Tivoli® Monitoring Version 6.2 is a powerful monitoring product from IBM, that is easily customizable and provides real-time and historical data that enables you to quickly diagnose and solve issues through the IBM Tivoli Enterprise Portal component. This common, flexible, and easy-to-use browser interface helps users to quickly isolate and resolve potential performance problems.

This IBM Redbooks® publication presents a deployment guide for IBM Tivoli Monitoring V6.2. We cover planning, installing, and configuration of IBM Tivoli Monitoring V6.2 for small, medium, and large environments. In addition, we provide some case studies, such as IBM Tivoli Monitoring V5.x migration, event management integration, and Agent Builder.

Agent Builder is a very powerful tool that you can use to develop your own monitoring agents. In order to show you how this tool can be used in a real life scenario, we have created a 30 minute video that you can launch from the ITSO Web site.

We have also added an appendix that discusses IBM Tivoli Monitoring sales engagement planning for Business Partners and Solution Developers.

The target audience for this documentation is IT Specialists and Business Partners who will be working on IBM Tivoli Monitoring V6.2 implementations and proof of concepts.

The team that wrote this book

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

Vasfi Gucer is an IBM Certified Consultant IT Specialist at the ITSO Austin Center. He was 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 Brazil since 1996. She started working with hardware support for PC Company, worked two years for 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 V6.1 products.

Fabrizio Salustri is a Software Support Specialist working for Italy IMT in the Tivoli Customer Support team within IBM Global Technology Services. He has been working for IBM since 1996, and has extensive experience with the Tivoli products suite. Since 1996, he worked as a Certified AIX® System Administrator in the AIX Technical Support team. In 1998, he joined the Tivoli Technical Support team. Throughout his career, Fabrizio has been involved in several projects implementing Tivoli solutions for clients of IBM Italy for Tivoli Management Framework, Tivoli Enterprise Console®, Tivoli Configuration Manager, IBM Tivoli Monitoring Version 5.x and Version 6.1, Tivoli Storage Manager, and Tivoli Provisioning Manager V5.1. In March 2005 he received an IBM Tivoli Monitoring 5.1.1 Deployment Professional Certification, in April 2006 he received an IBM Tivoli Monitoring 6.1 Deployment Professional Certification, and in December 2006 he received an IBM Tivoli Provisioning Manager V5.1 Deployment Professional Certification. He took part in several residencies at the ITSO writing IBM Redbooks publications on implementing a Tivoli Solution for Central Management of Large Distributed Environments, IBM Tivoli Monitoring V6.1, and Tivoli Provisioning Manager V5.1.

Ghufran Shah is a Tivoli Certified Enterprise Consultant and Instructor with os-security.com in the United Kingdom. He has eight years of experience in Systems Development and Enterprise Systems Management. He holds a degree in Computer Science from the University of Bradford. His areas of expertise include Tivoli Systems Management Architecture, Implementation, and Tivoli Training, together with Business Process Improvement and Return on Investment modeling. He has written extensively about event Management, Monitoring, and Business Systems Management integration and has taught Tivoli courses worldwide.

John Willis is a Tivoli Enterprise Certified Instructor, Consultant, and Lead Architect for Capital Software (`http://www.capitalsoftware.com`). He has more than 20 years in IT with six years of experience working with Tivoli. John is a frequent speaker at SHARE.org on Distributed Monitoring, Tivoli Enterprise Console, and the Workbench. His current area of expertise includes working with CIM and WMI.

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

Arzu Gucer and Wade Wallace
International Technical Support Organization, Austin Center

Wade Allen, Ron Cherveny, Terry Copeland, Dave Fresquez, Scott J Kinane,
John Kuhn, Heath Newburn
IBM USA

Chris Phillips and Raffaella Nicolosi
IBM Italy

Ilda Y Yaguinuma
IBM Brazil

Dietger Bahn and Frank Markgraf
IBM Germany

Richard Fowkes
IBM UK

Wolfgang Schumacher
IBM Business Partner, Germany

Become a published author

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

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

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

ibm.com/redbooks/residencies.html

Comments welcome

Your comments are important to us!

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

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

  ibm.com/redbooks

- Send your comments in an e-mail to:

  redbooks@us.ibm.com

- Mail your comments to:

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

Part 1

Planning and architecture

In this part, we introduce the planning architecture considerations of IBM Tivoli Monitoring V6.2.

1

Introduction

This chapter introduces the concepts and components behind IBM Tivoli Monitoring Version 6.2. The following topics are described in this chapter:

- “IBM Tivoli at a glance” on page 4
- “IBM Service Management (ISM)” on page 4
- “Enterprise management challenges” on page 9
- “IBM Tivoli Monitoring solutions” on page 12
- “IBM Tivoli Monitoring V6.2 components” on page 14
- “IBM Tivoli Open Process Automation Library (OPAL)” on page 17
- “What is new in IBM Tivoli Monitoring V6.2” on page 18

1.1 IBM Tivoli at a glance

Tivoli's portfolio spans security, storage, enterprise asset, systems, and network management software that enables clients to reduce the complexity of technology through the integration of IT processes as services across an organization's infrastructure.

By automating the integration of business services, known as *Service Management*, companies can speed the flow of processes and free up their technology resources for more strategic projects. They can also ensure compliance with parameters set by Sarbanes-Oxley (Public Company Accounting Reform and Investor Protection Act), HIPPA (Health Insurance Portability and Accountability Act), Basel II (recommendations on banking laws and regulations), and other mandates, which can require clients to account for how resources are used and how sensitive data is accessed and stored.

1.2 IBM Service Management (ISM)

Today, companies focus on providing innovative services. To deliver these services, IT and operations departments must strive to guarantee compliance, security, and continuous uptime, which all play a part in helping to ensure these business services are effectively performed to support the organization's business goals. Yet it is common for companies with organizational silos and traditional implementations to become entrenched in managing things like IT infrastructure technologies, single product revenues and expenses, individual processes and organizational efficiencies, instead of managing integrated solutions and services delivered by the sum of all these components. When this happens, there can be penalties for noncompliance and service level violations.

Enter IBM Service Management, a revolutionary way to align your organization and all its related functions with your business. IBM Service Management encompasses the management processes, tactics, and best practices needed to deliver business services. IBM Service Management is about developing, deploying, and managing services, helping to reduce IT and operations costs by automating processes, and helping to more effectively manage compliance. It is about increasing flexibility and getting products, solutions, and services to market more quickly. It is about helping to respond to changes more efficiently and effectively than ever before.

IBM Service Management is designed with one thing in mind: to help you manage your business. Because IBM understands that IT and operations are very much a part of your business, we offer powerful tools to help you align the four primary components of your business:

- People
- Processes
- Information
- Technology

IBM Service Management lets you pull these critical components together with an array of tightly integrated solutions that can be viewed as three interconnected layers:

- IBM Process Management
- IBM Operational Management
- IBM Service Management platform

These solutions are based on IBM and industry best practices, such as the IT Infrastructure Library® (ITIL®), Control Objectives for Information and related Technology (COBIT), and enhanced Telecom Operations Map (eTOM), helping users to ensure IT and operational processes are consistently designed, automated, and executed, and are auditable for compliance adherence.

IBM Service Management helps you anticipate and plan for change by providing timely access to critical information. IBM Service Management can help you react more quickly to shifts in the marketplace and customer demand, and help you stay miles ahead of the competition.

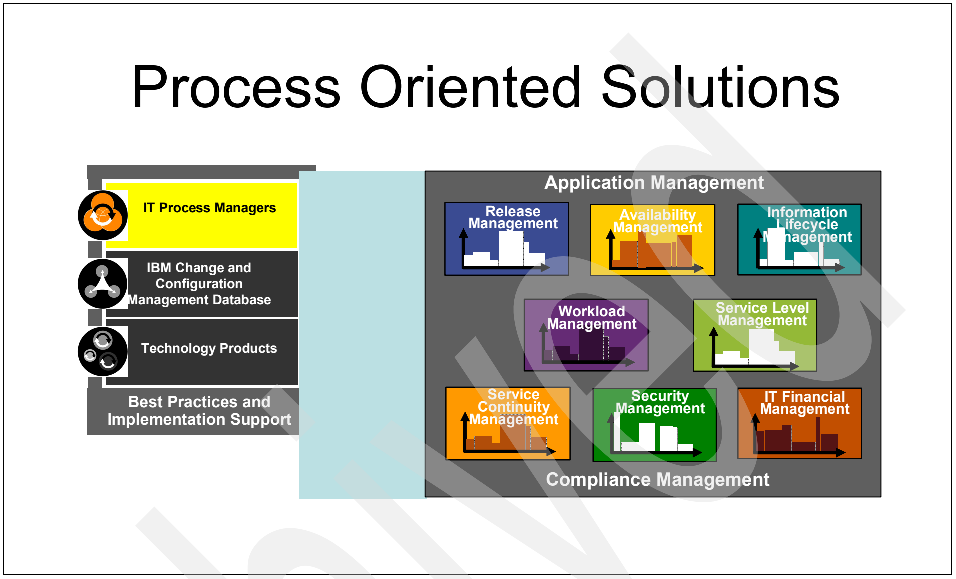
1.2.1 IBM Process Management products

IBM Process Management products work with your operational management products to automate repeatable processes, reduce manual tasks, and free staff to focus on business-critical priorities. Process managers fully integrate with IBM Tivoli Change and Configuration Management Database (CCMDB).

- IBM Tivoli Availability Process Manager automates tasks related to managing incidents and problems across the organization.
- IBM Tivoli Release Process Manager automates process steps and tasks related to managing software and related hardware deployments.
- IBM Tivoli Storage Process Manager automates tasks related to storage provisioning to optimize storage space and protect data integrity.
- IBM Tivoli Change Process Manager (included in Tivoli CCMDB) automates tasks to apply changes to your IT infrastructure.

- IBM Tivoli Configuration Process Manager (included in Tivoli CCMDB) automatically manages the configuration of your IT infrastructure.

Figure 1-1 shows the Process Oriented Solutions from IBM.



Process Oriented Solutions

IT Process Managers

IBM Change and Configuration Management Database

Technology Products

Best Practices and Implementation Support

Application Management

Release Management

Availability Management

Information Lifecycle Management

Workload Management

Service Level Management

Service Continuity Management

Security Management

IT Financial Management

Compliance Management

Figure 1-1 Process Oriented Solutions from IBM

1.2.2 IBM Operational Management products

IBM Operational Management products help users to ensure the availability, reliability, and performance of business-critical software and hardware, aid in optimizing storage requirements, and help meet ongoing needs for data security.

- Business Application Management helps maintain availability and optimal performance of business-critical software applications spanning multiple servers, operating systems, and databases:
  - IBM Tivoli Composite Application Manager for WebSphere®
    - Helps increase the performance and availability of business-critical applications through real-time problem determination across subsystems: WebSphere, CICS®, and IMS™.
  - IBM Tivoli Composite Application Manager for Response Time Tracking
    - An end-to-end transaction management solution that can proactively recognize, isolate, and resolve user response time performance problems.

  - IBM Tivoli Business Service Manager
    - IBM Tivoli Business Service Manager V4.1 provides operational and business audiences with the service visibility and intelligence needed to effectively manage real-time service health and business activity, including automated service modeling, service impact analysis, root cause analysis, and tracking of key performance indicators and SLAs in targeted dashboards.
  - IBM Tivoli Change and Configuration Management Database (CCMDB)
    - Discovers and federates IT information spread across the enterprise, including details about servers, storage devices, networks, middleware, applications, and data.
  - IBM Tivoli Application Dependency Discovery Manager (TADDM)
    - Provides complete and detailed application maps of business applications and its supporting infrastructure, including cross-tier dependencies, runtime configuration values, and complete change history.
    - The IBM Tivoli Monitoring integration with TADDM provides comprehensive monitoring of application resources, automatically identifies all resources that are unmonitored, and automatically provisions agents.
    - The benefits of using TADDM with IBM Tivoli Monitoring is faster closed loop troubleshooting, identification of infrastructure changes, and the reduction of Mean-Time-To-Resolution (MTTR) by the correlation of infrastructure health to changes.
- Server, Network, and Device Management helps users to optimize availability and performance of underlying IT architecture, including networks, operating systems, databases, and servers.
  - IBM Tivoli Monitoring
    - Proactively manages the health and availability of your IT infrastructure, end-to-end, including operating systems, databases, and servers, across distributed and host environments.
  - IBM Tivoli Network Manager IP Edition
    - Real-time network discovery, topology, and root cause analysis for layer 2 and 3 networks.
  - IBM Tivoli Provisioning Manager
    - Provisions and configures servers, operating systems, middleware, applications, storage, and network devices.

- IBM Tivoli Netcool/OMNIbus™
  - Consolidated fault monitoring for real-time service management.

- Storage Management helps users to optimize storage space, protect data integrity, and comply with data retention regulations and policies.
- Security Management automates identity management and security event management.

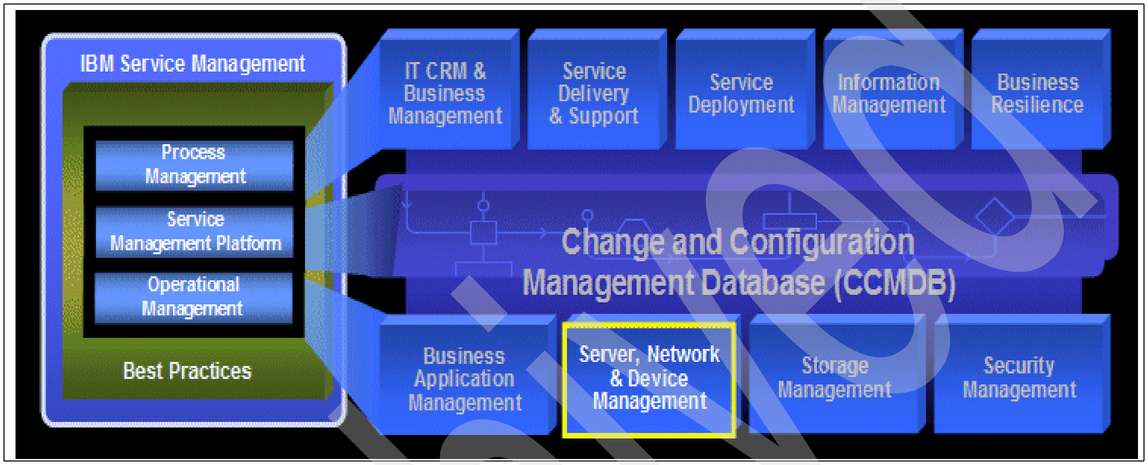

IBM Service Management
Process Management
Service Management Platform
Operational Management
Best Practices
IT CRM & Business Management
Service Delivery & Support
Service Deployment
Information Management
Business Resilience
Change and Configuration Management Database (CCMDB)
Business Application Management
Server, Network & Device Management
Storage Management
Security Management

Figure 1-2 ISM Service Management

1.2.3 IBM Service Management platform

One of the key elements of the integration platform in IBM Service Management is Tivoli CCMDB, which collects, stores, and shares dynamic information required for automation. It establishes processes for managing both configuration and change and works with IBM Process Management products and IBM Operational Management products to help users ensure that the organization is using current, consistent information by providing:

- Traceable, auditable changes
- Automated application discovery
- Detail on the interactions between systems
- An open platform for data and process integration

1.3 Enterprise management challenges

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

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

Traditional enterprise management has to change, as their modus operandi tend to include most if not all of the following:

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

1.3.1 Business driving forces

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

- The need to increase revenues, reduce costs, and compete more effectively.

- Companies need to deploy informational applications rapidly, and provide business users with easy and fast access to business information that reflects the rapidly changing business environment. Enterprise Management solutions must be transparent to the business solutions being delivered, and they must be proactive to detect, resolve, and escalate potential issues that may impact the business service being delivered.
- The need to manage and model the complexity of today's business environment.
- Corporate mergers and deregulation means that companies today are providing and supporting a wider range of products and services to a broader and more diverse audience than ever before. Understanding and managing such a complex business environment and maximizing business investment is becoming increasingly more difficult. Enterprise management systems provide more than just basic monitoring mechanisms; they also offer sophisticated issue detection, event correlation, and application and transaction discovery and performance management tools that are designed to handle and process the complex business information associated with today's business environment.
- The need to reduce IT costs and leverage existing corporate business information.
- The investment in IT systems today is usually a significant percentage of corporate expenses, and there is a need not only to reduce this impact, but also to gain the maximum business benefits from the information managed by IT systems. New information technologies like corporate intranets, thin-client computing, and subscription-driven information delivery help reduce the cost of deploying business intelligence systems to a wider user audience, especially information consumers like executives and business managers. Maintaining the maximum uptime of these systems is becoming more and more critical.
- Any solution needs to consist of well defined processes, which fit into the business model, and provide a vehicle for optimum service delivery. Processes should not hinder creativity or operational practices, but rather support them and provide an environment for growth and service improvement.

1.3.2 Sample end-to-end scenario of an IBM Tivoli solution: Automated Problem Resolution

Figure 1-3 on page 11 shows a sample end-to-end scenario of an IBM Tivoli solution: Automated Problem Resolution. The scenario is used to orchestrate and integrate data between IBM Tivoli Monitoring, Service Desk, CCMDB, and IBM Tivoli Provisioning Manager, so problems are detected and remediation actions are implemented immediately. Using the scenario, you can answer questions such as:

- What is happening with the infrastructure?
- What is the business service?
- What action do I take?

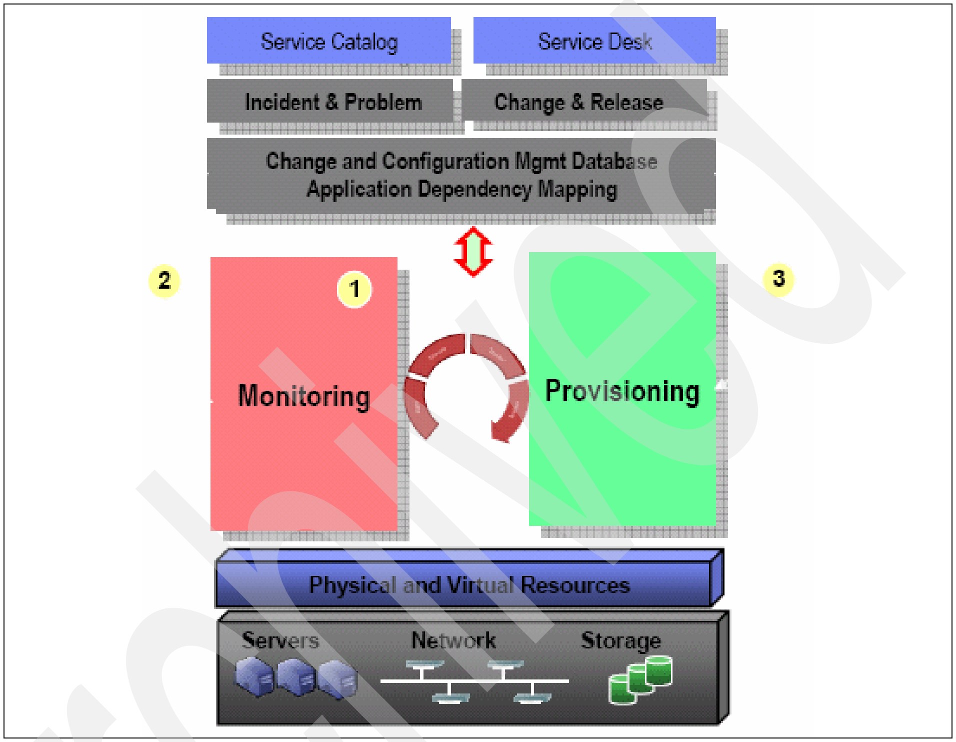


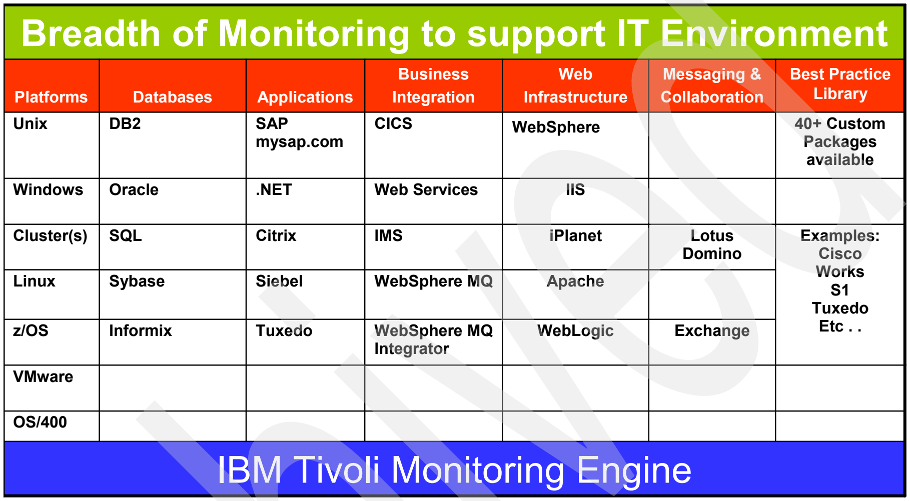
Figure 1-3 Automated Problem Resolution scenario

Here are the highlights of the scenario:

1. Use IBM Tivoli Monitoring to visualize monitoring information in the portal on how infrastructure resources are performing.
2. If a problem is detected require provisioning action (for example, patch distribution, new resource allocation, or virtual server expansion), a Change Request is initiated, and data is automatically passed into CCMDB and IBM Tivoli Provisioning Manager based on predefined policies.
3. IBM Tivoli Provisioning Manager takes automated action, reports back the completion status to CCMDB, and we see results in the portal.

1.4 IBM Tivoli Monitoring solutions

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



Breadth of Monitoring to support IT Environment

Platforms	Databases	Applications	Business Integration	Web Infrastructure	Messaging & Collaboration	Best Practice Library
Unix	DB2	SAP mysap.com	CICS	WebSphere		40+ Custom Packages available
Windows	Oracle	.NET	Web Services	IIS		
Cluster(s)	SQL	Citrix	IMS	iPlanet	Lotus Domino	Examples: Cisco Works S1 Tuxedo Etc . .
Linux	Sybase	Siebel	WebSphere MQ	Apache		
z/OS	Informix	Tuxedo	WebSphere MQ Integrator	WebLogic	Exchange	
VMware						
OS/400						

IBM Tivoli Monitoring Engine

Figure 1-4 IBM Tivoli Monitoring solutions - Integrated end-to-end support for heterogeneous environments

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

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

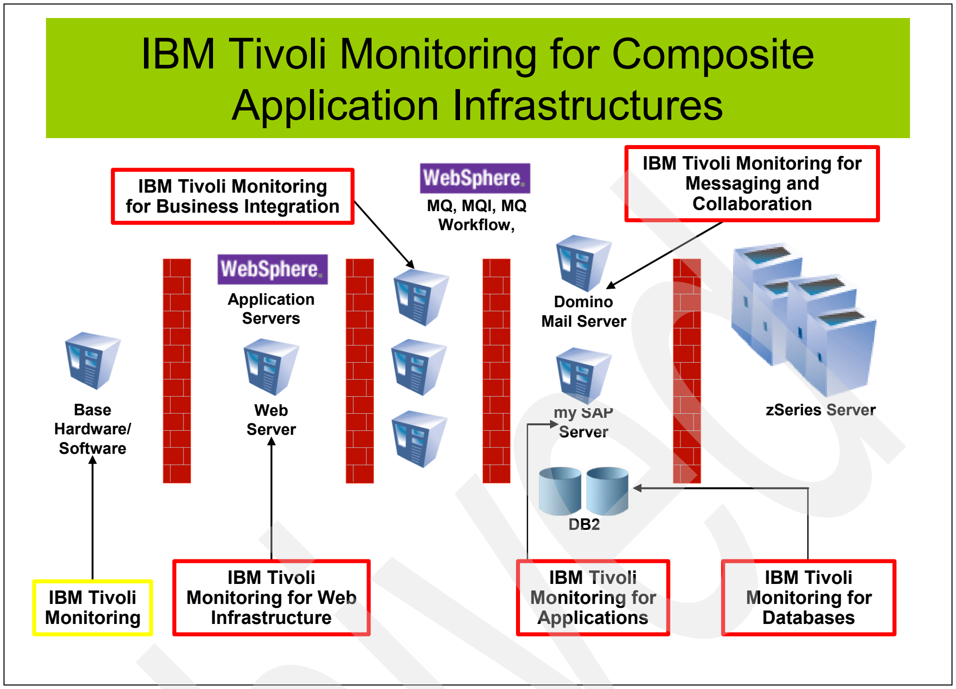

IBM Tivoli Monitoring for Composite Application Infrastructures
IBM Tivoli Monitoring for Business Integration
WebSphere
MQ, MQI, MQ Workflow,
IBM Tivoli Monitoring for Messaging and Collaboration
WebSphere
Application Servers
Domino Mail Server
Base Hardware/ Software
Web Server
my SAP Server
zSeries Server
DB2
IBM Tivoli Monitoring
IBM Tivoli Monitoring for Web Infrastructure
IBM Tivoli Monitoring for Applications
IBM Tivoli Monitoring for Databases

Figure 1-5 Monitoring composite application infrastructures

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

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

1.5 IBM Tivoli Monitoring V6.2 components

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

Figure 1-6 shows the IBM Tivoli Monitoring components.

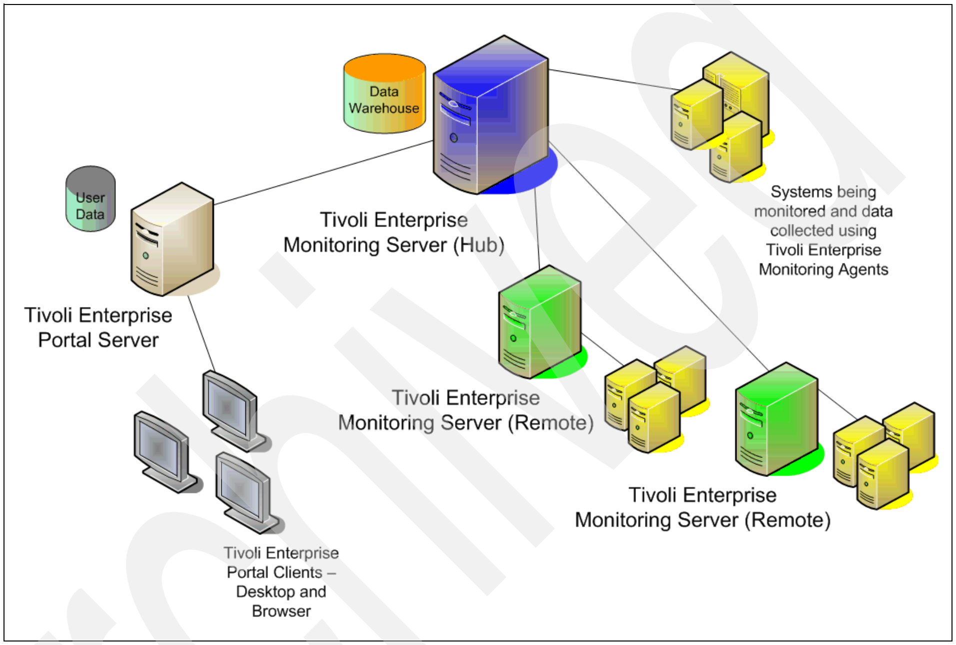

Data Warehouse
User Data
Tivoli Enterprise Monitoring Server (Hub)
Systems being monitored and data collected using Tivoli Enterprise Monitoring Agents
Tivoli Enterprise Portal Server
Tivoli Enterprise Monitoring Server (Remote)
Tivoli Enterprise Monitoring Server (Remote)
Tivoli Enterprise Portal Clients – Desktop and Browser

Figure 1-6 IBM Tivoli Monitoring V6.2 components

1.5.1 Tivoli Enterprise Monitoring Server (monitoring server)

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

The monitoring server is responsible for tracking the heartbeat request interval for all Tivoli Enterprise Monitoring Agents connected to it. The monitoring server stores, initiates, and tracks all situations and policies, and is the central repository for storing all active conditions on every Tivoli Enterprise Monitoring Agent. Additionally, it is responsible for initiating and tracking all generated actions that invoke a script or program on the Tivoli Enterprise Monitoring Agent.

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

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

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

1.5.2 Tivoli Enterprise Portal Server (portal server)

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

1.5.3 Tivoli Enterprise Portal (portal or portal client)

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

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

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

1.5.4 Tivoli Enterprise Monitoring agent (monitoring agent)

The Tivoli Enterprise Monitoring agent (also referred to as monitoring agents or managed systems) are installed on the system or subsystem requiring data collection and monitoring. The agents are responsible for 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 Tivoli Enterprise Portal displays an alert icon when a threshold is exceeded or a value is matched. The tests are called situations.

Tivoli Enterprise Monitoring Agents are grouped into:

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

1.5.5 Warehouse Proxy agent (WPA)

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

1.5.6 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 large amounts of data processing requirements, we recommend that the S&P be always installed on the same physical system as the Tivoli Data Warehouse repository.

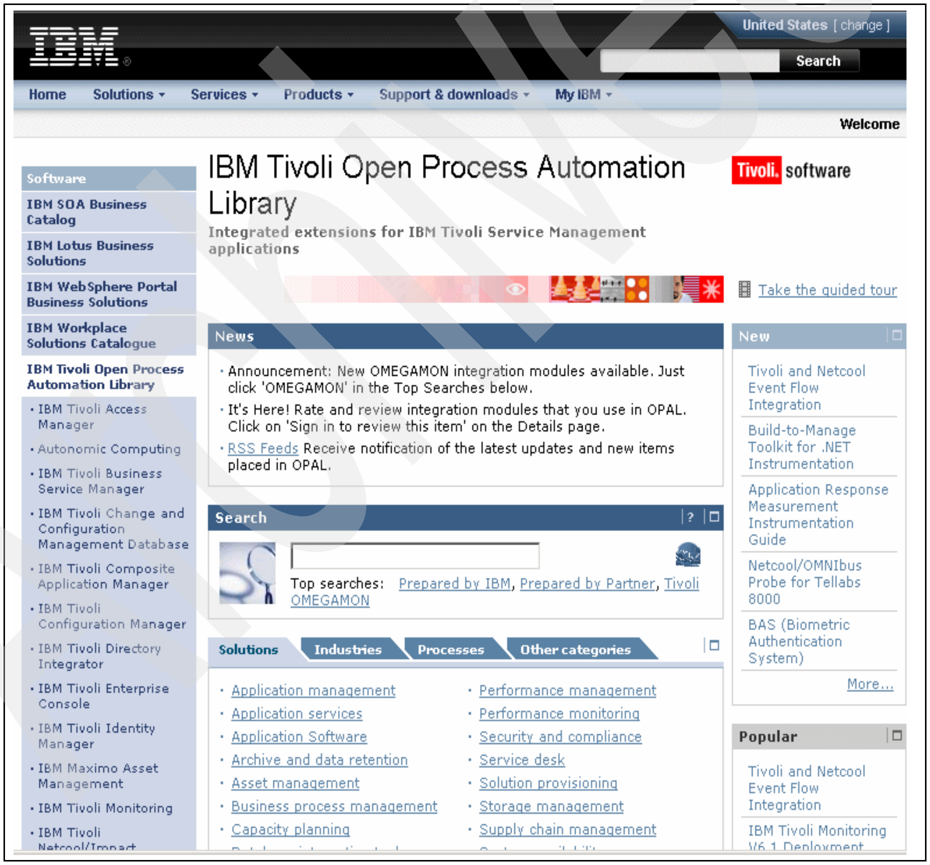
Note: To know the current supported platforms for above components, refer to the latest Fix Pack readme file. At the time of writing, Fix Pack 5 readme had the most current list.

1.6 IBM Tivoli Open Process Automation Library (OPAL)

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

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

Figure 1-7 shows the home page of the site.



Software

IBM SOA Business Catalog

IBM Lotus Business Solutions

IBM WebSphere Portal Business Solutions

IBM Workplace Solutions Catalogue

IBM Tivoli Open Process Automation Library

- IBM Tivoli Access Manager
- Autonomic Computing
- IBM Tivoli Business Service Manager
- IBM Tivoli Change and Configuration Management Database
- IBM Tivoli Composite Application Manager
- IBM Tivoli Configuration Manager
- IBM Tivoli Directory Integrator
- IBM Tivoli Enterprise Console
- IBM Tivoli Identity Manager
- IBM Maximo Asset Management
- IBM Tivoli Monitoring
- IBM Tivoli Netcool/Impact

IBM Tivoli Open Process Automation Library

Integrated extensions for IBM Tivoli Service Management applications

News

- Announcement: New OMEGAMON integration modules available. Just click 'OMEGAMON' in the Top Searches below.
- It's Here! Rate and review integration modules that you use in OPAL. Click on 'Sign in to review this item' on the Details page.
- RSS Feeds Receive notification of the latest updates and new items placed in OPAL.

Search

Top searches: Prepared by IBM, Prepared by Partner, Tivoli OMEGAMON

Solutions | Industries | Processes | Other categories

- Application management
- Application services
- Application Software
- Archive and data retention
- Asset management
- Business process management
- Capacity planning
- Performance management
- Performance monitoring
- Security and compliance
- Service desk
- Solution provisioning
- Storage management
- Supply chain management

New

Tivoli and Netcool Event Flow Integration

Build-to-Manage Toolkit for .NET Instrumentation

Application Response Measurement Instrumentation Guide

Netcool/OMNIbus Probe for Tellabs 8000

BAS (Biometric Authentication System)

More...

Popular

Tivoli and Netcool Event Flow Integration

IBM Tivoli Monitoring V6.1 Deployment

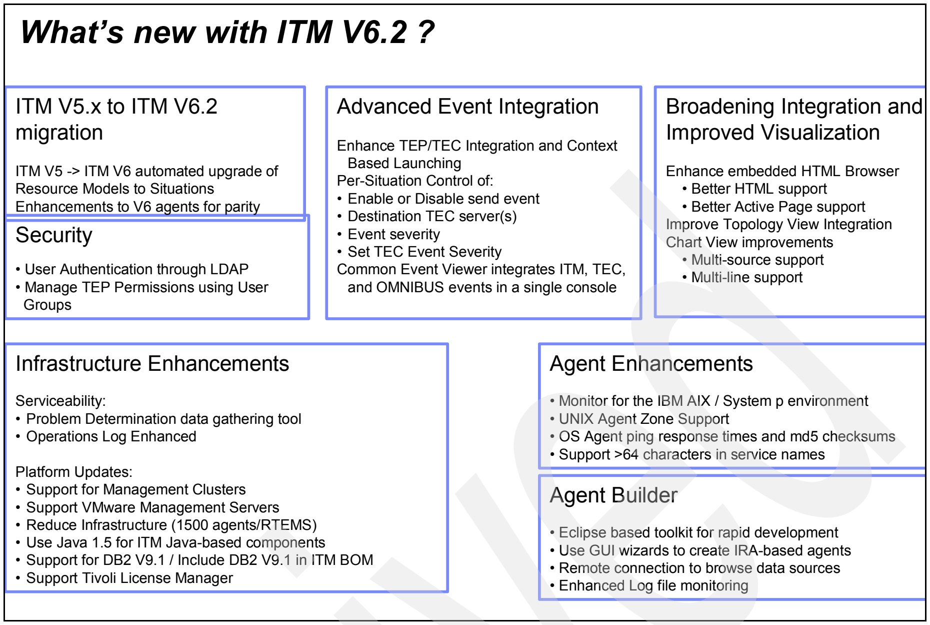
Figure 1-7 IBM Tivoli Open Process Automation Library

The Web site provides:

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

1.7 What is new in IBM Tivoli Monitoring V6.2

Figure 1-8 on page 19 gives an overview of what is new in IBM Tivoli Monitoring V6.2.



What's new with ITM V6.2 ?

ITM V5.x to ITM V6.2 migration

ITM V5 -> ITM V6 automated upgrade of Resource Models to Situations
Enhancements to V6 agents for parity

Security

- User Authentication through LDAP
- Manage TEP Permissions using User Groups

Advanced Event Integration

Enhance TEP/TEC Integration and Context Based Launching
Per-Situation Control of:
- Enable or Disable send event
- Destination TEC server(s)
- Event severity
- Set TEC Event Severity

Common Event Viewer integrates ITM, TEC, and OMNIBUS events in a single console

Broadening Integration and Improved Visualization

Enhance embedded HTML Browser
- Better HTML support
- Better Active Page support

Improve Topology View Integration
Chart View improvements
- Multi-source support
- Multi-line support

Infrastructure Enhancements

Serviceability:
- Problem Determination data gathering tool
- Operations Log Enhanced

Platform Updates:
- Support for Management Clusters
- Support VMware Management Servers
- Reduce Infrastructure (1500 agents/RTEMS)
- Use Java 1.5 for ITM Java-based components
- Support for DB2 V9.1 / Include DB2 V9.1 in ITM BOM
- Support Tivoli License Manager

Agent Enhancements

- Monitor for the IBM AIX / System p environment
- UNIX Agent Zone Support
- OS Agent ping response times and md5 checksums
- Support >64 characters in service names

Agent Builder

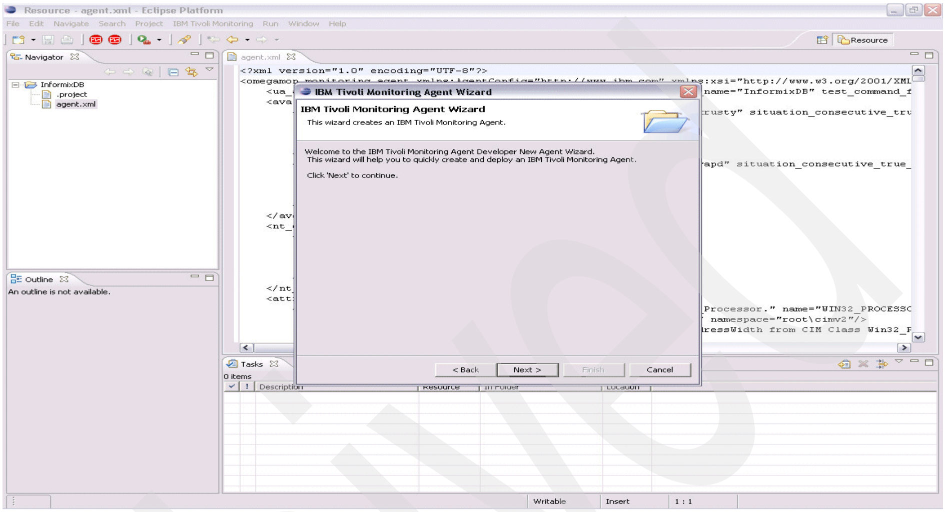
- Eclipse based toolkit for rapid development
- Use GUI wizards to create IRA-based agents
- Remote connection to browse data sources
- Enhanced Log file monitoring

Figure 1-8 A summary of what is new in IBM Tivoli Monitoring V6.2

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

Agent Builder

Agent Builder was introduced with IBM Tivoli Monitoring V6.1 Fix Pack 5 and has been enhanced in IBM Tivoli Monitoring V6.2. Figure 1-9 shows the Agent Builder.


Resource - agent.xml - Eclipse Platform
File Edit Navigate Search Project IBM Tivoli Monitoring Run Window Help
Resource
Navigator
InformixDB
.project
agent.xml
Outline
An outline is not available.
agent.xml
Tasks
0 items
Description
Resource
In Folder
Location
Writable
Insert
1 : 1

```
<?xml version="1.0" encoding="UTF-8"?>
```

IBM Tivoli Monitoring Agent Wizard

IBM Tivoli Monitoring Agent Wizard

This wizard creates an IBM Tivoli Monitoring Agent.

Welcome to the IBM Tivoli Monitoring Agent Developer New Agent Wizard.
This wizard will help you to quickly create and deploy an IBM Tivoli Monitoring Agent.

Click 'Next' to continue.

Figure 1-9 Agent Builder

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

See Chapter 6, "Agent Builder" on page 347 for more information about the Agent Builder. You can also watch a video on this topic at:

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

See 6.7, "Agent Builder Demonstration Video" on page 356 for more information about this video.

IBM Tivoli Monitoring V5.x to IBM Tivoli Monitoring V6.2 migration

IBM Tivoli Monitoring V6.2 will provide an “automation-supported upgrade process” for migrating IBM Tivoli Monitoring V5.x resource models to situations.

Security

Product security features will be enhanced in IBM Tivoli Monitoring V6.2 by enabling user authentication through Lightweight Directory Access Protocol (LDAP). You will also be able to manage portal permissions using User Groups.

Infrastructure enhancements

This version will see a number of enhancements in the area of infrastructure:

- Serviceability:
  - Problem determination data gathering tool
  - Operations Log enhanced
- Platform updates:
  - Support for Management Clusters
  - Support VMware Management Servers
  - Reduce infrastructure (1500 agents/remote monitoring server)
  - Use Java 1.5 for IBM Tivoli Monitoring Java-based components
  - Support for DB2® V9.1 (DB2 V9.1 is included in the IBM Tivoli Monitoring installation media)
  - Support for Tivoli License Manager

Advanced event integration

IBM Tivoli Monitoring V6.2 will enhance the existing Tivoli Enterprise Console integration and allow context based launching. It will allow enable or disable send events, setting the destination IBM Tivoli Enterprise Console server(s) and event severity per situation.

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

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

Common Event Viewer will integrate IBM Tivoli Monitoring, IBM Tivoli Enterprise Console, and OMNIBUS events in a single console.

Broadening integration and improved visualization

There are also some enhancements in the visualization area. The embedded HTML Browser will be enhanced to provide better HTML and Active Page support.

There are also a number of Topology View Integration Chart View improvements, such as multi-source support and multi-line support.

The visualization enhancements are further discussed in 1.7.1, “Portal enhancements in IBM Tivoli Monitoring V6.2” on page 22.

Agent enhancements

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

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

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

1.7.1 Portal enhancements in IBM Tivoli Monitoring V6.2

The new features in the Tivoli Enterprise Portal (portal) are:

Client deployment options

All deployment options supported in IBM Tivoli Monitoring V6.1 continue to be supported in IBM Tivoli Monitoring V6.2. IBM Tivoli Monitoring V6.2 also introduces a new deployment option based on Java Web Start. This provides improved desktop performance, central administration, support for multiple JREs, much faster initial download, and broad platform coverage.

Workspace enhancements

You can now establish your own “Home Workspace”, which will be the first workspace you see when you log on to the portal. You can return anytime through the new Home Workspace tool button. Also, the quadrants that views occupy in a workspace can be swapped using "drag-n-drop", which eliminates tedious workspace re-definition. (This feature was actually introduced in IBM Tivoli Monitoring V6.1 Fix Pack 2).

View enhancements In IBM Tivoli Monitoring V6.1, when a navigator view is collapsed, there is no way to select other navigator views without first restoring the collapsed navigator. In IBM Tivoli Monitoring V6.2, any assigned navigator view can now be selected from the view's collapsed button, or from the View option off the main menu.

View tools New view-level tools, added for increased usability, such as a "Hide/Show view-level toolbar", a "Properties" tool, and a "Find" tool.

Chart views In Bar Charts, a new overlay feature has been introduced that allows one or more related attributes to be plotted against the bar chart. Plot Charts now support multi-row, multi-attribute result sets, and a separate auto-refresh interval can be set that is independent of any workspace refresh interval; new plot chart views will be auto-refreshed every 30 seconds. The plot chart view can be "primed" with historical data, allowing historical and real-time information to be combined in the same view.

Table view Thresholds in table views can now be visualized using both icons and colors, and you can use your own icons and assign your own severities. Icon-based thresholds can be combined with color-based thresholds within the same view.

Topology view IBM Tivoli Monitoring V6.2 now allows the workspace author to easily create topology views from relational data sources. There is also a Link Wizard enabled that supports contextual-driven navigation, together with numerous styling and customization features.

Browser view The browser view is enhanced to support the vast majority of *de facto* Web content, such as Javascipt, Applets, PDF, Flash, Multimedia, plug-ins, XML, XHTML, XSL, HTML 4.01, CSS 1 and 2, and HTTPS.

Common Event Console

The Comment Event Console (CEC) is a new view that has been introduced in IBM Tivoli Monitoring V6.2 to provide an extensible consolidated console, allowing new event sources to be "connected in" with future releases. Events that would normally appear in the three consoles

(Situation Event Console, TEC Event Console, and Active Event List) can now be viewed in the CEC. See 5.4.1, “Common Event Console Configuration window” on page 332 for more information about CEC.

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

2

IT environment

This chapter describes the prerequisites to install IBM Tivoli Monitoring V6.2. In 2.3, “Sizing and sample of deployment scenarios” on page 39, we show some examples of IBM Tivoli Monitoring V6.2 installations for small, medium, and large environments

The following topics are described in this chapter:

- “Hardware prerequisites” on page 26
- “Software prerequisites” on page 28
- “Sizing and sample of deployment scenarios” on page 39

2.1 Hardware prerequisites

In the following sections, we described the hardware requirements for the IBM Tivoli Monitoring V6.2 infrastructure for distributed systems. We cover the following components:

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

2.1.1 Processor requirements

For best performance, we recommend processor speeds of at least 1 GHz for RISC architectures and 2 GHz for Intel® architectures. Except for the Tivoli Data Warehouse, single processor systems are suitable when an IBM Tivoli Monitoring infrastructure component is installed on a separate computer from the other components.

You should use multiprocessor systems in the following scenarios:

- Running Tivoli Enterprise Portal client on a computer that is also running one of the server components.
- Monitoring environment of 1000 or more monitored agents with multiple server components on the same computer. For example:
  - Portal server and hub monitoring server
  - Monitoring server (hub or remote) and Warehouse Proxy agent
  - Warehouse Proxy agent and Summarization and Pruning agent
- Running a small environment with all the server components (monitoring server, portal server, Warehouse Proxy agent, and Summarization and Pruning agent) on a single computer.
- For the Tivoli Data Warehouse database server. Except for a very small installation, you should you a multiprocessor system for the Tivoli Data Warehouse database.
  - If you install the Warehouse Proxy agent on the warehouse database server, consider using a two-way or four-way processor.

– If you install the Summarization and Pruning agent on the Warehouse database server (with or without the Warehouse Proxy agent), consider using a four-way processor. For large environments where more CPU resources might be needed, we can run the Summarization and Pruning agent on a computer separate from the Warehouse database server. In this case, ensure that a high-speed network connection exists (100 Mbps or faster) between the Summarization and Pruning agent and the database server.

2.1.2 Memory and disk requirements

Table 2-1 shows estimated memory and disk storage for IBM Tivoli Monitoring components on distributed systems.

Table 2-1 Memory and disk requirements

Component	Processor memory requirements[a]		Disk storage requirements [b]
	Small environment[c]	Large environment [d]	
Hub monitoring server	70 MB	100 MB	650 MB [e]
Remote monitoring server	100 MB	300 MB	250 MB [e]
Portal server	100 MB [f]	300 MB [f]	800 MB
Portal client (browser or desktop)	150 MB	300 MB	150 MB
Tivoli Data Warehouse	2 - 4 GB depending on database configuration parameters	2 - 8 GB depending on database configuration parameters	Following ITM Install Guide to estimate the database size. [g]
Warehouse Proxy agent	50 MB	100 MB	150 MB
Summarization and Pruning agent	150 MB	300 MB	150 MB

a. The memory and disk sizings shown in this table are the amounts required for the individual component beyond the needs of the operating system and any concurrently running applications.

b. The disk storage estimates apply to any size monitoring environment and are considered high estimates. The size of log files affect the amount of storage required.

c. A small environment is considered to be a monitoring environment with 500 to 1000 agents, with 100 to 200 monitored agents per remote monitoring server.

d. A large environment is considered to be a monitoring environment with 3000 or more monitored agents, with 500 to 1000 monitored agents per remote monitoring server.

e. The storage requirements for the hub and remote monitoring servers do not include storage for the agent depot, which can require an additional 1 GB or more.

f. The memory requirement for the portal server does not include database processes for the portal server database, which require up to 400 MB of additional memory, depending on configuration settings.

g. One of the factors to consider when planning the size of database that we need is the amount and type of information we will collect for agent history data collection. Please refer to "Planning considerations for the Tivoli Data Warehouse" in *IBM Tivoli Monitoring Version 6.2.0 Installation and Setup Guide*, GC32-9407 to estimate database size.

2.1.3 Additional requirements

The additional requirements for IBM Tivoli Monitoring V6.2 installation are:

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

2.2 Software prerequisites

The software prerequisites to install IBM Tivoli Monitoring V6.2 are discussed in this section.

2.2.1 Required software for IBM Tivoli Monitoring

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

Table 2-2 Required software for IBM Tivoli Monitoring

Product	Supported version	Component where the software is required				
		Monitoring server	**Portal server**	**Portal desktop client**	**Portal browser client**	**Monitoring agent**
IBM Runtime Environment for Java	JRE™ V1.5	X	X	X	X	
For Linux® computers: a Korn shell interpreter	pdksh-5.2.14	X	X	X		

Product	Supported version	Component where the software is required				
		Monitoring server	**Portal server**	**Portal desktop client**	**Portal browser client**	**Monitoring agent**
For Red Hat Enterprise Linux 4.0 computers: libXp.so.6 (available in xorg-x11-deprecated-libs)						X
AIX only: xlC Runtime Environment (required for GSkit)		X				
Microsoft® Internet Explorer	V6.0 with all critical Microsoft updates applied	X			X	
Database	A supported RDBMS is required for the Tivoli Enterprise Portal Server and the Tivoli Data Warehouse. Supported database platforms for the portal server and Tivoli Data Warehouse are listed in 2.2.5, “Supported databases for Tivoli Enterprise Portal Server and Tivoli Data Warehouse” on page 37.					
IBM Tivoli Enterprise Console	Version 3.9 with Fix Pack 03					
For TCP/IP communication: ► Windows 2000 Professional or Server with Service Pack 3 or above ► Microsoft Winsock v1.1 or later ► Microsoft TCP/IP protocol stack		X	X	X	X	

Product	Supported version	Component where the software is required				
		Monitoring server	Portal server	Portal desktop client	Portal browser client	Monitoring agent
For SNA communication: ► Windows 2000 Professional or Server with Service Pack 3 or above ► Microsoft SNA Server V3.0 or later ► IBM Communications Server V5.0 or 5.2	Microsoft SNA Server V4.0 requires Service Pack 1. IBM Communications Server V5.0 requires fixes JR10466 and JR10368.	X				

2.2.2 Required software for event integration with Netcool/OMNIbus

In order to install event synchronization and configure event forwarding for Netcool/OMNIbus, you must install and configure the following products:

- Netcool/OMNIbus V7.x
- Netcool/OMNIbus V7.x probe for Tivoli EIF
- IBM Tivoli Monitoring V6.2

2.2.3 Required software for event integration with the Tivoli Enterprise Console

In order to install event synchronization and configure event forwarding for Tivoli Enterprise Console, you must install and configure the following products:

- Tivoli Enterprise Console must have at least Fix Pack 3 installed.
- IBM Tivoli Monitoring V6.2

2.2.4 Supported operating systems

The following tables show which operating systems are supported for the different IBM Tivoli Monitoring components: monitoring server, portal server, portal client, monitoring agent, Warehouse Proxy, and Warehouse Proxy Summarization and Pruning agent. For additional information about the operating systems supported, see http://www-306.ibm.com/software/sysmgmt/products/support/Tivoli_Supported_Platforms.html. Table 2-3 shows the support for monitoring components on Windows computers.

Table 2-3 Supported Windows operating systems

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

a. The Tivoli Enterprise Portal desktop client is supported on marked platforms. However, the browser client can be accessed only from Windows computers running Internet Explorer 6 or 7.

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

c. For the Windows XP and Windows Vista® operating systems, the Microsoft End User License Agreement (EULA) does not license these operating systems to function as a server. Tivoli products that function as a server on these operating systems are supported for demonstration purposes only.

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

Table 2-4 shows the support for monitoring components on UNIX (non-Linux), i5/OS®, and z/OS® computers.

Table 2-4 Supported UNIX, i5/OS, and z/OS operating systems

Operating system	**Monitoring server**	**Portal server**	**Portal client**	**OS TMA**[a] [b]	**WPA** [c]	**SPA**
AIX V5.2 (32-bit and 64-bit) [d]	(32)			X		
AIX V5.3 (32-bit and 64-bit) [d]		(32)		X		
Solaris™ Operating Environment V8 (32-bit and 64-bit) [e]				X		
Solaris V9 (SPARC) (32/34) [f]	(32)			X		(32)
Solaris V10 (SPARC) (32/34)	(32)			(32,64N)/ (32,64N)		(32)
Solaris V10 (x86-64) on AMD™ Opteron™	(32)			(32,64N)/ (64N)		
Solaris Zones	(32)[g]			(32,64N)/ (32,64N)[g] [h]		(32)[g]
HP-UX 11i v1 (B.11.11) (32) on PA-RISC[i]				X		
HP-UX 11i v2 (B.11.23) (64) on PA-RISC[i]				X		
HP-UX 11i v3 (B.11.31) (32/64) on PA-RISC[i]				X		
HP-UX 11i v2 (B.11.23) on Integrity (IA64)[j]	(32)			(32,64N)/ (32,64N)	(32)	(32)
HP-UX 11i v3(B.11.31) on Integrity (IA64)[j]				X		
i5/OS 5.3 (64)				X		
i5/OS 5.4 (64)				X		
z/OS 1.6[k] [l]	(31)			(31/64)		
z/OS 1.7[k] [l]	(31)			(31/64)		
z/OS 1.8[k] [l]	(31)			(31/64)		

a. The OS monitoring agent column indicates the platforms on which an operating system monitoring agent is supported. This column does not indicate that any agent runs on any operating system. For example, to monitor a Linux computer, we must use a Linux monitoring agent, not a Windows monitoring agent. For information about the operating systems supported for non-OS agents, see the documentation for the specific agents.

b. If we are installing the OMEGAMON® XE for Messaging agent on a 64-bit operating system, we must install the 32-bit version of the agent framework. See the IBM Tivoli Monitoring Fix Pack 005 Readme and Documentation Addendum for details on installing this framework.

c. A X11 GUI interface is required to configure the Warehouse Proxy agent.

d. Supported AIX systems must be at the required maintenance level for IBM Java 1.5. Refer to the following Web site for the Java 5 AIX maintenance level matrix: `http://www-128.ibm.com/developerworks/java/jdk/aix/service.html`. Component xlC.aix50.rte must be at 8.0.0.4. See the following Web site for installation instructions: `http://www-1.ibm.com/support/docview.wss?uid=swg1IY84212.` Version 8 of the AIX XC C/C++ runtime must be installed. To determine the current level, run the following AIX command: **`lslpp -l | grep -i xlc`**. For the Tivoli Enterprise Portal server, AIX V5.3 must be at TL5.

e. Solaris V8 32-bit requires patches 108434-17 and 109147-07. Solaris V8 64-bit requires 108435-17 and 108434-17. Both 32-bit and 64-bit versions require 111721-04.

f. Solaris V9 32-bit requires patch 111711-11. Solaris V9 64-bit requires 111712-11 and 111711-11. Both 32-bit and 64-bit versions require 111722-04.

g. The monitoring server and the Warehouse Summarization and Pruning agent can run in both local and global zones on Solaris; however, the OS monitoring agent can run only in global zones.

h. We cannot use the remote deployment function for the agents on this operating system for either fresh installations and upgrades. We must install locally.

i. For HP-UX, patch PHSS_30970 is required.

j. IBM Tivoli Monitoring does not support remote deployment for HP-UX 11i v2/v3 on Integrity computers.

k. For information about installing the monitoring server on z/OS, refer to the program directory that comes with that product.

l. The OS monitoring agent for z/OS computers is part of the IBM Tivoli OMEGAMON for z/OS product.

Table 2-5 shows the monitoring components supported on Linux operating systems.

Table 2-5 Supported Linux operating systems

Operating system	**Monitoring server**	**Portal server** [a]	**Portal client**	**OS TMA** [b h]	**WPA** [c]	**SPA**
Asianux 2.0 for Intel (32-bit)	X	X	X	X	X	X
Red Flag 4.1 for Intel (32-bit)	X	X	X	X	X	X
Red Flag 5.1 for Intel	X	X	X	X	X	X
Red Hat Enterprise Linux 2.1 Intel (32-bit)				X		

Operating system	Monitoring server	Portal server [a]	Portal client	OS TMA [b] [h]	WPA [c]	SPA
Red Hat Enterprise Linux 3 on Intel (32-bit)				X		
Red Hat Enterprise Linux 3 on zSeries® (31-bit)				(31,64 N)		
Red Hat Enterprise Linux 3 on zSeries (64-bit)				X		
Red Hat Enterprise and Desktop Linux 4 Intel (32-bit)	X	X	X	X	X	X
Red Hat Enterprise Linux 4 on AMD64/EM64T (64-bit)	(32)			(64N)/ (64N)		
Red Hat Enterprise Linux 4 on Itanium® (64-bit)				(64N)/ (64N)		
Red Hat Enterprise Linux 4 on iSeries® and pSeries®				(32,64 N)(64 N)		
Red Hat Enterprise Linux 4 on z/Series (31-bit)	X	X		(31,64 N)/(31 ,64N)	X	X
Red Hat Enterprise Linux 4 on zSeries (64-bit)	X [d]	X [d] [f]		(31,64 N)/(31 ,64N)	X	X
Red Hat Enterprise Linux 4 for Intel on VMWare ESX Server V2.5.2 and V3.0 (32-bit)	X	X	X	(31,64 N)/(31 ,64N)	X	X
Red Hat Enterprise and Desktop Linux 5 Intel (32-bit)	X	X	X	X	X	X
Red Hat Enterprise Linux 5 on AMD64/EM64T	(32)			X		
Red Hat Enterprise Linux 5 on Itanium 64-bit				X		
Red Hat Enterprise Linux 5 on iSeries and pSeries				(32,64 N)/(64 N)		

Operating system	Monitoring server	Portal server [a]	Portal client	OS TMA [b][h]	WPA [c]	SPA
Red Hat Enterprise Linux 5 on z/Series (31-bit)	X	X	X	X	X	X
Red Hat Enterprise Linux 5 on zSeries (64-bit)	X [e]	X [e][g]		(31,64 N)/(31 ,64N)	X	X
SUSE Linux Enterprise Server 8 Intel (32-bit)				X		
SUSE Linux Enterprise Server 8 for z/Series (31-bit)				X		
SUSE Linux Enterprise Server 8 for z/Series (64-bit)				X		
SUSE Linux Enterprise Server 9 Intel (32-bit)	X	X	X	X	X	X
SUSE Linux Enterprise Server 9 on AMD64/EM64T (64-bit)				X		
SUSE Linux Enterprise Server 9 on Itanium (64-bit) [d]				X		
SUSE Linux Enterprise Server 9 for iSeries and pSeries				(32,64 N)/(64 N)		
SUSE Linux Enterprise Server 9 for z/Series (31-bit)	X	X	X	X	X	X
SUSE Linux Enterprise Server 9 for z/Series (64-bit)	X [e]	X [e][g]		(31,64 N)/(31 ,64N)	(31)	(31)
SUSE Linux Enterprise Server 10 Intel (32)	X	X	X	X	X	X
SUSE Linux Enterprise Server 10 on AMD64/EM64T (64-bit) [f]				X		
SUSE Linux Enterprise Server 10 on Itanium (64-bit) [d][f]				X		
SUSE Linux Enterprise Server 10 for iSeries and pSeries6 (64-bit)				(32,64 N)/(64)		

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

a. The Tivoli Enterprise Portal desktop client is supported on marked platforms. However, the browser client can be accessed only from Windows computers running Internet Explorer 6 or 7.

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

c. A X11 GUI interface is required to configure the Warehouse Proxy agent.

d. This component supports the operating system in 64-bit tolerance mode.

e. See Technote 1247529 for minor known problems and workarounds for SUSE Linux Enterprise Server 10 on 64-bit operating systems.

f. We must install the Tivoli Enterprise Portal Server and its IBM DB2 database in a 31-bit mode session. Each time we start the Tivoli Enterprise Portal Server, we must be in a 31-bit mode session. To enter a 31-bit mode session, type `s390 sh` at the command line. The `s390` command is included in the s390-32 rpm package and the 31-bit libraries. SUSE Linux Enterprise Server 9 must be at SP3 or higher. SUSE 10 must be at pdksh-5.2.14 or higher.

g. The Linux OS Monitoring Agent requires the installation of the latest versions of the following libraries: libstdc++ libgcc compat-libstdc++ libXp. These libraries are available on the Linux operating system installation media and Service Packs. Each library could have multiple packages, and each should be installed.

During the Tivoli Monitoring installation, the IBM Global Security Toolkit (GSKit) is installed. Table 2-6 provides the OS requirements to install it.

Table 2-6 Operating system requirements for IBM GSKit

Operating system	Patch required
Solaris V8	108434-14, 111327-05, 108991, 108993-31, 108528-29, 113648-03, 116602-01, 111317-05, 111023-03, and 115827-01
Solaris V9	111711-08
Solaris V10	None
HP-UX V11i	PHSS_26946, PHSS_33033
AIX V5.x	xlC.aix50.rte.6.0.0.3 or later
Windows Server 2003	None
Red Hat Enterprise Linux 2.1 Intel	pdksh-5.2.14-13.i386.rpm

Operating system	Patch required
Red Hat Enterprise Linux 4 Intel	compat-gcc-32-c++-3.2.3-46.1.i386.rpm compat-gcc-32-3.2.3-46.1.i386.rpm compat-libstdc++-33-3.2.3-46.1.i386.rpm
SUSE Linux Enterprise Server 8 Intel	None
SUSE Linux Enterprise Server 9 Intel	None

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

IBM Tivoli Monitoring V6.2 requires database installation to work with Tivoli Enterprise Portal Server and Tivoli Data Warehouse. The following two tables describe which databases are supported.

> **Note:** IBM provides DB2 UDB Enterprise Edition V9.1 for use with the portal server and the Tivoli Data Warehouse only. Each instance of the database must be registered using `db2licm` command, as described in “Registering the DB2 product license key” on page 39.

Table 2-7 shows the supported databases for the portal server.

> **Note:** The database and the portal server must be installed on the same computer.

Table 2-7 Supported databases for the portal server

Portal server operating system	Portal server database (TEPS)[a b c]	
	IBM DB2 [d]	MS SQL
AIX	IBM DB2 UDB V8.1 with Fix Pack 10 or higher fix packs, V8.2 with Fix Pack 3 or higher fix packs, and V9.1 and fix packs.	
Linux	IBM DB2 UDB V8.1, with Fix Pack 10 or higher fix packs, V8.2 with Fix Pack 3 or higher fix packs, and V9.1 and fix packs.	
Windows	IBM DB2 UDB V8.1, with Fix Pack 10 or higher fix packs, V8.2 with Fix Pack 3 or higher fix packs, and V9.1 and fix packs.	MS SQL 2000 SP3 [e]

a. TEPS is the default database name for the database used by the portal server.

b. Support is for 32- or 64-bit databases, except that IBM DB2 UDB V9.1 is supported for 32-bit only.
c. The portal server database must be located on the computer where the portal server is installed.
d. If, in the environment, we are using products whose licenses require us to collect software use information and report it to IBM using IBM Tivoli License Manager, we must ensure that use of this instance of IBM DB2 is not included in the report. To do this, create a Tivoli License Manager license, selecting a license type that does not involve reporting to IBM, and associate this instance of the product with it.
e. IBM Tivoli Monitoring supports MS SQL Server® 2000 only if the data is limited to codepoints inside the Basic Multilingual Plane (range U+0000 to U+FFFF). This restriction does not apply to IBM DB2.

Table 2-8 shows the supported databases for the Tivoli Data Warehouse.

Table 2-8 Supported databases for the Tivoli Data Warehouse

Tivoli Data Warehouse database (*WAREHOUS*)[a] [b]		
IBM DB2	**MS SQL**[c]	**Oracle®** [d]
IBM DB2 UDB V8.1, Fix Pack 10 and higher fix packs, V8.2, Fix Pack 3 and higher fix packs, and V9.1 and fix packs on the following operating systems:[e] ► AIX V5.3 v HP-UX 11iv3 ► Solaris 10 v Windows 2003 Server ► SUSE Linux Enterprise Server 9 and 10 for Intel ► Red Hat Enterprise Linux 4 for Intel	MS SQL 2000 EE[f] MS SQL 2005	Oracle V9.2, 10g Release 1, and 10g Release 2 on the following operating systems: ► AIX V5.3 ► HP-UX 11iv3 ► Solaris 10 ► Windows 2003 Server ► SUSE Linux Server 9 and 10 for Intel and Red Hat Enterprise Linux 4 for Intel

a. WAREHOUS is the default database name for the database used by Tivoli Data Warehouse. Support is for 32- or 64-bit databases except that IBM DB2 UDB V9.1 is supported for 32-bit only. Tivoli Data Warehouse database can be located on the same computer as the portal server or on a remote computer.
b. If, in the environment, we are using products whose licenses require to collect software use information and report it to IBM using IBM Tivoli License Manager, we must ensure that use of this instance of IBM DB2 is not included in the report. To do this, create a Tivoli License Manager license, selecting a license type that does not involve reporting to IBM, and associate this instance of the product with it.
c. The Tivoli Enterprise Portal Server supports Microsoft SQL only when the Tivoli Enterprise Portal Server is running on a Windows system.
d. See the Oracle company support Web site (`http://www.oracle.com`) for information about installing and configuring Oracle on Solaris V10.
e. Do not use DB2 V9 Fix Pack 2 for the Tivoli Data Warehouse. Use of DB2 V9 FP2 can cause the Warehouse Proxy Agent and the Summarization and Pruning Agent not to function properly. Use an earlier version, such as DB2 V9 Fix Pack 1, or upgrade to a level that contains the fix for APAR JR26744, such as DB2 V9 Fix Pack 3.

f. IBM Tivoli Monitoring supports MS SQL Server 2000 only if the data is limited to code points inside the Basic Multilingual Plane (range U+0000 to U+FFFF). This restriction does not apply to IBM DB2.

Registering the DB2 product license key

The DB2 product uses the license key information contained in the nodelock file. The nodelock file is created or updated by running the **db2licm** command and specifying the license file for the DB2 product. Creating or updating the nodelock file is referred to as registering the DB2 product license key. You must register the DB2 product license key by running the **db2licm** command on each computer where DB2 is installed. Or you can copy the license key to the /db2/license directory; the license key will be added automatically during the installation.

The IBM Tivoli Monitoring V6.2 license file is named db2ese_o.lic.txt, and is located in the root of IBM Tivoli Monitoring V6.2 installation media for a mounted CD. To register the license key, follow the instructions at the following location on the DB2 Information Center:

http://publib.boulder.ibm.com/infocenter/db2luw/v9/topic/com.ibm.db2.udb.uprun.doc/doc/t0006749.htm

2.3 Sizing and sample of deployment scenarios

In this section, we describe several deployment scenarios for IBM Tivoli Monitoring V6.2.

2.3.1 Sizing

At the time of the writing of this book, the following were best practices for the number of instances per IBM Tivoli Monitoring V6.2 component:

- One hub monitoring server per 10,000 agents
- One remote monitoring server per 1500 agents
- One portal server per 50 concurrent clients

> **Note:** Do not forget that agents are not the total number of servers that are monitored. An agent is a component monitored on a server like the UNIX OS Agent, UNIX Log Agent, or DB2 agent. For example, if you have a UNIX server running DB2 and an application that logs its errors to a file, you would install three agents on the one server: KUX, KDB, and KUL. On average for large deployments, a server will have at least two agents per server.

2.3.2 Sample deployment scenarios

In this section, we discuss three example deployment scenarios for your deployment planning. These are for small, medium, and large IBM Tivoli Monitoring V6.2 environments.

Small monitoring environment

You can deploy a small IBM Tivoli Monitoring environment on a single computer. This type of environment might be useful for a teaching environment, for advanced prototyping and testing of solutions, or for monitoring a small, but critical, server environment. Figure 2-1 shows a small monitoring environment.

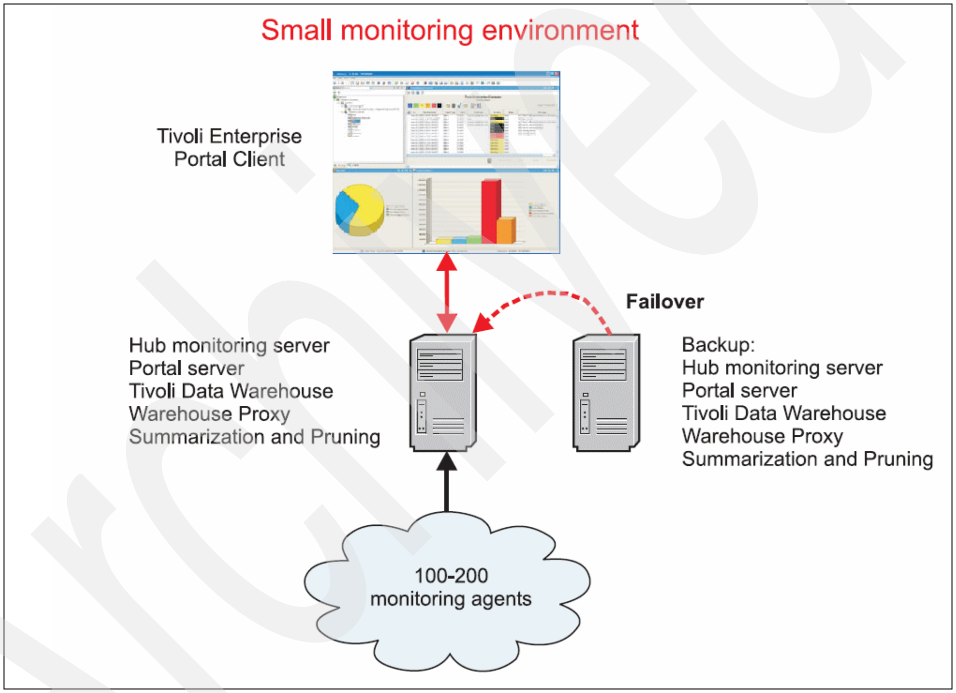


Figure 2-1 Small IBM Tivoli Monitoring environment

The small environment is limited to 100 to 200 agents. It can perform minimal historical data collection and does not use the IBM Tivoli Enterprise Console. Adding significant data collection or enterprise-wide event correlation requires additional servers. The advantage of a small environment is it is simple to set up. The disadvantages are that you can only support a small number of agents. Also, large amount of historical data collection or situation events could overwhelm the capacity.

Medium monitoring environment

You can build a medium monitoring environment with five to ten computers. This level of deployment is typically used in a medium-sized company, or within a large company to monitor different server groups independently. For example, depending on the organizational boundaries, you can use one remote hub to monitor a group of servers (such as SAP® servers, or servers at a specific location) and the other to monitor another group of servers.

Figure 2-2 shows an example of medium monitoring environment.

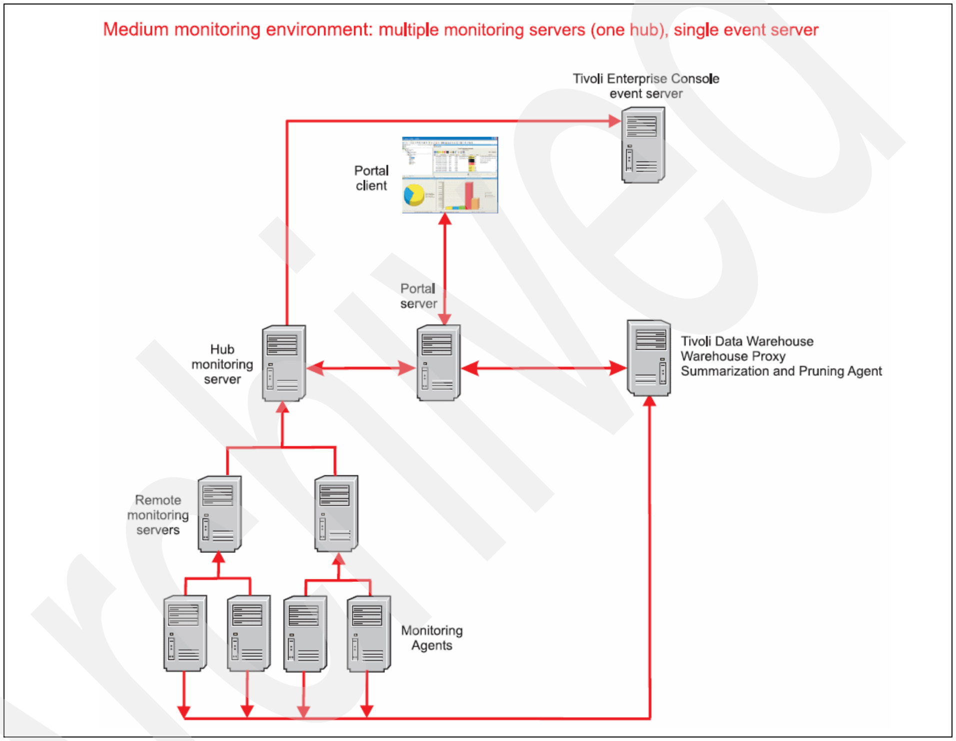

Medium monitoring environment: multiple monitoring servers (one hub), single event server
Tivoli Enterprise Console event server
Portal client
Portal server
Hub monitoring server
Tivoli Data Warehouse
Warehouse Proxy
Summarization and Pruning Agent
Remote monitoring servers
Monitoring Agents

Figure 2-2 Medium IBM Tivoli Monitoring environment

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

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

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

We can follow these guidelines for the medium monitoring environment:

- When selecting hardware for the monitoring servers and portal server, we should use system configurations that meet or exceed the recommended hardware requirements.
- We can scale the Tivoli Data Warehouse server according to how much historical data we plan to collect and retain.
- We can use a simple one-server Tivoli Enterprise Console deployment for event correlation.
- We can keep the Tivoli Data Warehouse, Warehouse Proxy, and Summarization and Pruning agent on the same computer to minimize server deployments, simplify configuration, and eliminate network transmission overhead.

Large monitoring environment: single hub installation

We can use a single hub monitoring deployment to build a large monitoring environment. Figure 2-3 on page 43 shows an example of a large monitoring environment, which is similar to the medium environment. The difference is that the large single hub installation contains multiple Warehouse Proxy agents and additional remote monitoring servers to support a larger number of agents. (The difference in the number of remote monitoring servers and agents is not represented in the diagram.) As with the medium monitoring environment, we can deploy a single hub installation or multiple independent hub installations to monitor different server groups according to organizational boundaries.

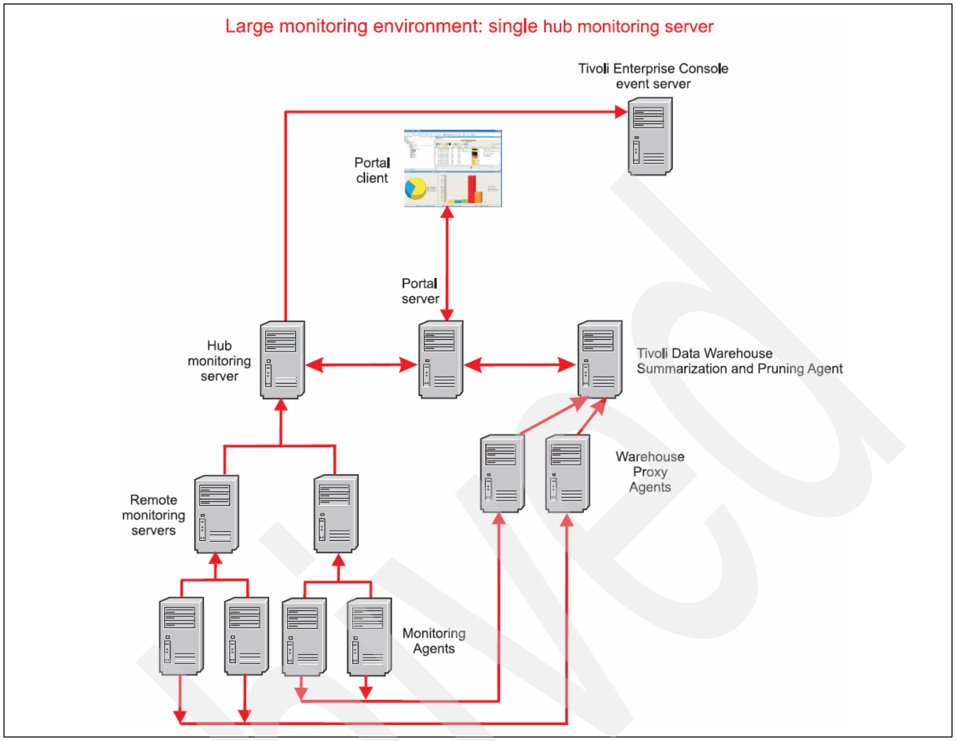

Large monitoring environment: single hub monitoring server
Tivoli Enterprise Console event server
Portal client
Portal server
Hub monitoring server
Tivoli Data Warehouse Summarization and Pruning Agent
Warehouse Proxy Agents
Remote monitoring servers
Monitoring Agents

Figure 2-3 Large deployment of IBM Tivoli Monitoring: single hub installation

The large single-hub environment could support a large number of monitoring agents. But we still have scale limitations, which could be solved by deploying multiple independent hub installations, as shown in “Large monitoring environment: multiple hub installation” on page 44.

We can follow these guidelines for the large single-hub monitoring environment:

- When selecting hardware for the monitoring servers and portal server, we should use system configurations that meet or exceed the recommended hardware requirements.
- We can scale the Tivoli Data Warehouse server according to how much historical data we plan to collect and retain.
- When installing Tivoli Data Warehouse on a separate computer from the Summarization and Pruning agent, we should ensure that we have a high-speed network connection between them for best performance. We can install one of the Warehouse Proxy agents on the same computer as the Tivoli Data Warehouse. Additional Warehouse Proxy agents must be installed on separate computers.

Large monitoring environment: multiple hub installation

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

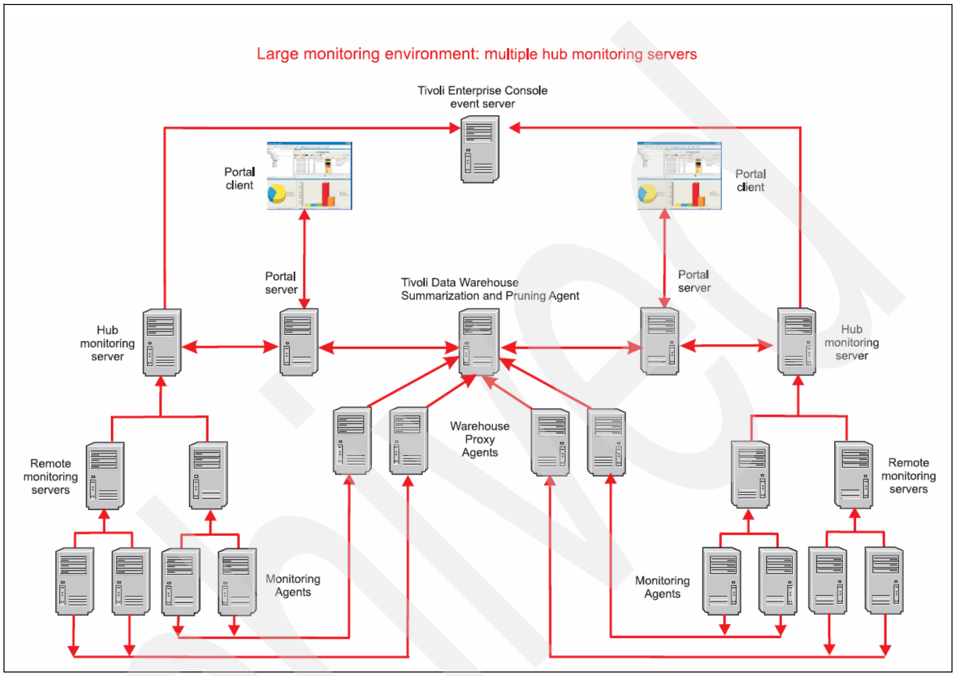

Large monitoring environment: multiple hub monitoring servers
Tivoli Enterprise Console event server
Portal client
Portal client
Portal server
Tivoli Data Warehouse Summarization and Pruning Agent
Portal server
Hub monitoring server
Hub monitoring server
Warehouse Proxy Agents
Remote monitoring servers
Remote monitoring servers
Monitoring Agents
Monitoring Agents

Figure 2-4 Large monitoring environment: multiple hub installation

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

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

- When selecting hardware for the monitoring servers and portal server, we should use system configurations that meet or exceed the recommended hardware requirements.
- We can scale the Tivoli Data Warehouse server according to how much historical data we plan to collect and retain.
- When installing Tivoli Data Warehouse on a separate computer from the Summarization and Pruning agent, we should ensure that we have a high-speed network connection between them for best performance. We can install one of the Warehouse Proxy agents on the same computer as the

Tivoli Data Warehouse. Additional Warehouse Proxy agents must be installed on separate computers.

- We should identify one of the hub installations as the primary installation. (The primary installation is a logical designation only.)
  - If the hub monitoring servers are at different maintenance levels, designate the primary installation as the installation with the hub monitoring server at the highest maintenance level.
  - Configure the Summarization and Pruning agent to report to the hub monitoring server of the primary installation.
  - Install application support for all agent types that exist in the multi-hub installation on the hub monitoring server, remote monitoring servers, portal server, and portal desktop clients that belong to the primary hub installation.

3

Installation and configuration

This chapter describes the detailed steps to implement IBM Tivoli Monitoring V6.2. The following topics are discussed in this chapter:

- “Installing IBM Tivoli Monitoring V6.2” on page 48
- “Remote agent deployment” on page 116
- “Tivoli Data Warehouse” on page 122

3.1 Installing IBM Tivoli Monitoring V6.2

In order to walk you through the steps of an IBM Tivoli Monitoring V6.2 installation, we build a test environment, as shown in Figure 3-1. Here, we can see the topology using the one of new features: the self-monitoring topology.

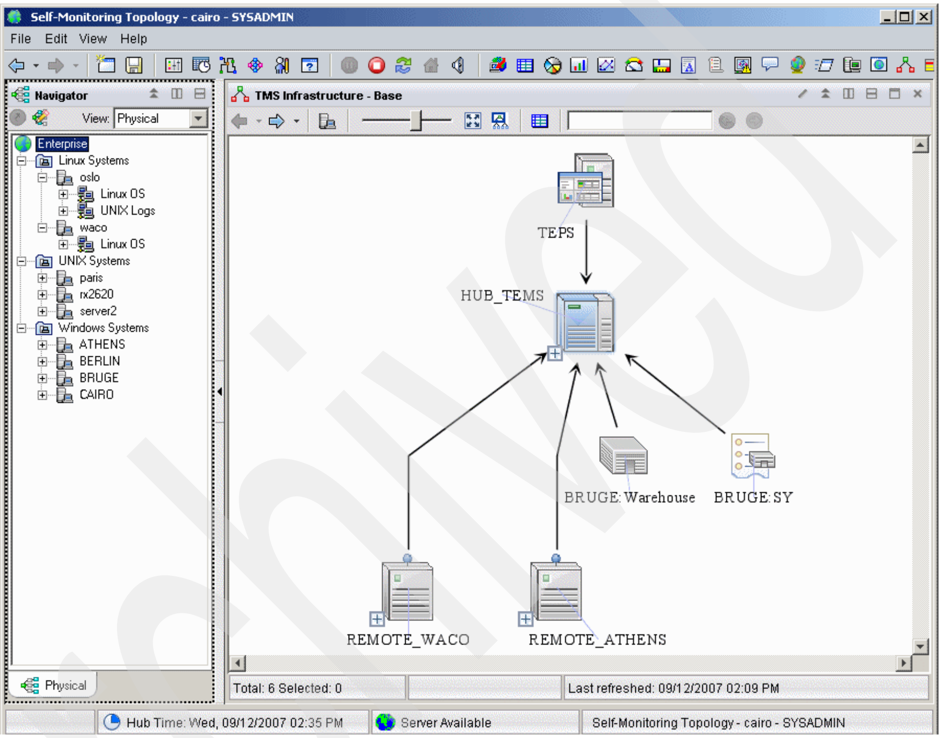


Figure 3-1 Test environment self-monitoring topology

When we double-click one of the remote monitoring servers or the hub monitoring server, we can see the connected agents, as shown in Figure 3-2 on page 49.

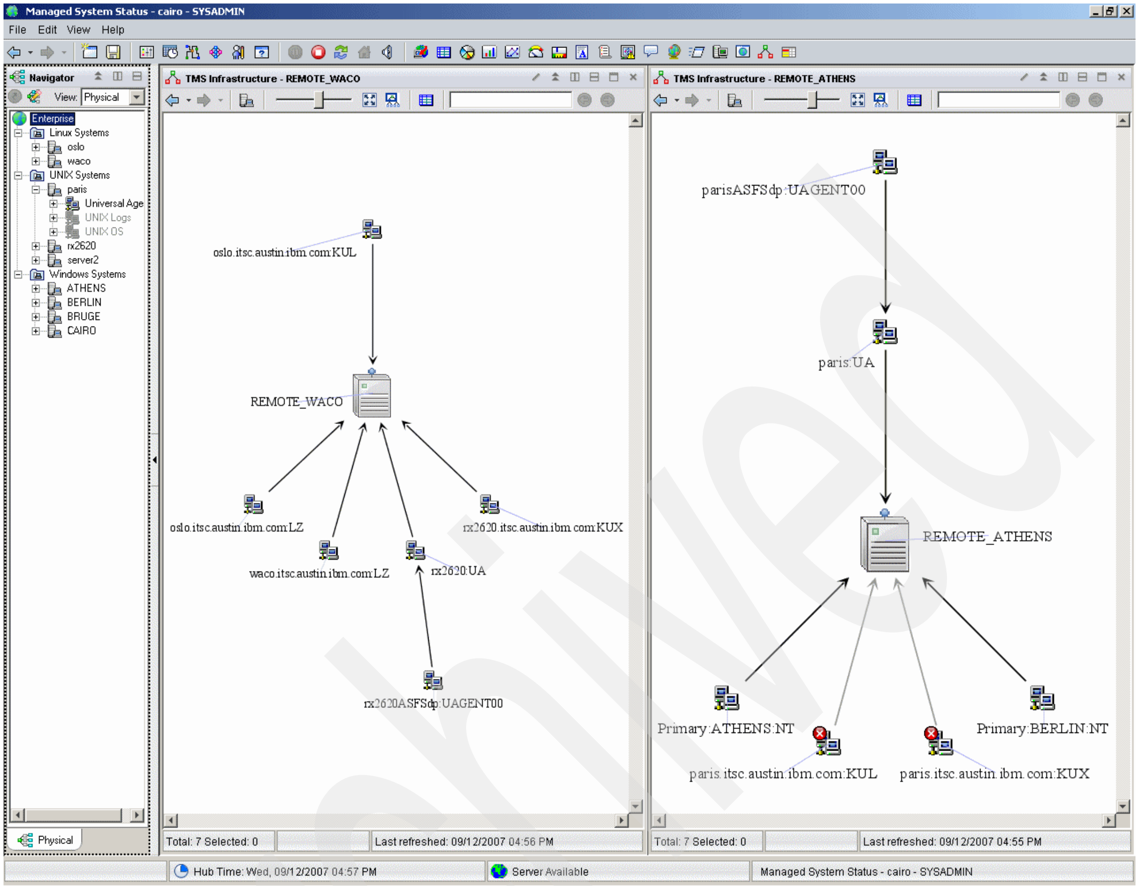

Managed System Status - cairo - SYSADMIN
File Edit View Help
Navigator
View: Physical
Enterprise
Linux Systems
oslo
waco
UNIX Systems
paris
Universal Age
UNIX Logs
UNIX OS
rx2620
server2
Windows Systems
ATHENS
BERLIN
BRUGE
CAIRO
Physical
TMS Infrastructure - REMOTE_WACO
oslo.itsc.austin.ibm.com:KUL
REMOTE_WACO
oslo.itsc.austin.ibm.com:LZ
waco.itsc.austin.ibm.com:LZ
rx2620:UA
rx2620.itsc.austin.ibm.com:KUX
rx2620ASFSdp:UAGENT00
Total: 7 Selected: 0
Last refreshed: 09/12/2007 04:56 PM
TMS Infrastructure - REMOTE_ATHENS
parisASFSdp:UAGENT00
paris:UA
REMOTE_ATHENS
Primary:ATHENS:NT
Primary:BERLIN:NT
paris.itsc.austin.ibm.com:KUL
paris.itsc.austin.ibm.com:KUX
Total: 7 Selected: 0
Last refreshed: 09/12/2007 04:55 PM
Hub Time: Wed, 09/12/2007 04:57 PM
Server Available
Managed System Status - cairo - SYSADMIN

Figure 3-2 Self-monitoring topology expanded

3.1.1 Considerations before installing the product

In this section, we discuss the things that you need to consider before starting the installation.

- Installation parameters.
- Required order of installation component products.
- Windows installation considerations
- Linux or UNIX Installation considerations
- Other considerations

Installation parameters

You will need the following information before starting the installation:

- Name of the monitoring server that will be installed or to which the agent will connect
- Host names of the systems that will be installed
- Port numbers (unless the default port numbers will be used)
- Whether the monitoring server being installed or being connected to is configured as a hub or remote monitoring server
- Whether you want to configure the hot standby feature or not

Required order of installation component products

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

- Hub Tivoli Enterprise Monitoring Server
- Remote monitoring server (if necessary)
- Tivoli Enterprise Management Agent Framework (although you can install a remote monitoring server on a machine which already has an agent)
- Tivoli Enterprise Portal Server
- Tivoli Enterprise Portal desktop client

> **Note:** These products must be installed on at least one computer before the agent can be properly configured.

Windows installation considerations

Before installing the IBM Tivoli Monitoring V6.2 components on Windows, you need to consider the items in the following sections.

User authority

To install IBM Tivoli Monitoring V6.2 on a Windows computer, you *must* have Administrator privileges on that computer. You also need to run the IBM Tivoli Monitoring V6.2 components as a user with Administrator privileges.

Installation using a Citrix client

When using a Citrix client to access the IBM Tivoli Monitoring V6.2 installation program for Windows through Microsoft Windows Terminal Services, you need to manually change Terminal Services to install mode before running the installation. To change the Terminal Services to install mode, run the command **`change user /install`** before starting the installation. After installation, run the command **`change user /execute`** to return Terminal Services to normal mode.

Linux or UNIX Installation considerations

The following sections provide information about issues specific to Linux and UNIX installations.

Changes in the behavior of the autostart scripts

The behavior of the autostart scripts generated by the installation of fix packs on UNIX platforms is different depending on the fix pack level:

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

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

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

or

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

Where:

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

N: An integer specific to each installation on a system.

ITM_Install_Home: The full path to the IBM Tivoli Monitoring V6.2 installation directory.

product_code: The two-character code for this application. Refer to *IBM Tivoli Monitoring Version 6.2.0 Installation and Setup Guide,* GC32-9407 for a list of the component codes.

instance: The instance name required to start this application.

PLAT: The platform directory where the application is installed.

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

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

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

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

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

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

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

Note: Please note the following considerations for changes to the autostart scripts:

- Any changes made directly to the autostart script (ITMAgentsN or rc.itmN, depending on the platform) will not be preserved and will be overwritten the next time that you configure an application, or install or upgrade an application.
- Any changes made to the AutoRun.sh script will not be preserved and will be overwritten the next time you apply higher maintenance.

Create an IBM Tivoli account for installing and maintenance

If security guidelines prevent you from using the root account in certain environments, you can create to create an IBM Tivoli account for installing and maintaining the installation directory.

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

Here are some of the guidelines for creating an IBM Tivoli account for installation and maintenance:

- You can install the IBM Tivoli Monitoring V6.2 software as the root user, but you do not have to. If you do not do the installation as a root user, you must follow the steps outlined in “Changing the file permissions for agents on a Linux or UNIX server” on page 110 after you install any monitoring agent.
- Use the same user to install all components.
- If you are using NFS or a local file system, establish your installation directory according to the guidelines used in your environment.
- Consider using the Korn shell for your IBM Tivoli account; however, you can use any shell that is shipped with the UNIX operating system.

Note: IBM Tivoli products do not support third-party vendor shells such as BASH (Bourne Again SHell) and TCSH (TC-Shell).

File descriptor (maxfiles) limit

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

```
ulimit -a
```

The nofiles parameter is the number of file descriptors available to a process. For the monitoring server process (kdsmain), the .nofiles. parameter should be set larger than the maximum number of agents that will be connecting to the monitoring server. If the monitoring server is unable to get file descriptors when needed, unexpected behavior can occur, including program failures. Consider increasing the value to 1000 file descriptors or more. There are other user limit parameters that control how much data, stack, and memory are available to a process. For large environments, consider increasing these memory-related user limit parameters for the monitoring server (kdsmain) process. Configuring the user limit parameters usually requires root access, and involves changing system startup files that are operating system specific. Consult the operating system manuals for information about how to configure the user limit parameters.

Other considerations

This section describes some non-specific operating system considerations.

Host name for TCP/IP network services

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

Use of fully qualified path names

Because of the wide variety of UNIX operating systems and possible user environments, use fully qualified path names when entering a directory during the installation process (do not use pattern-matching characters). IBM scripts use the Korn shell. When a new process or shell is invoked, use of symbolic links, environmental variables, or aliases can potentially cause unexpected results.

Multiple Network Interface Cards

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

Installing into a Network File System (NFS) environment

IBM supports installing IBM Tivoli Monitoring V6.2 in NFS environments. Using NFS, you can concentrate your software and data in a specific location, minimizing maintenance, administrative overhead, and disk space. Although using NFS to support multiple hosts simplifies the maintenance of installed IBM Tivoli products, its use can impact performance. If you are installing into an NFS environment, consider the administrative savings to the possible impact on the performance of your network. Consider the number of hosts that share a single installation directory, as well as the effects of network congestion and file system performance on the overall response time of your IBM Tivoli products. NFS also has some trade-offs in how you manage your environment. While you can have your entire IBM Tivoli Monitoring V6.2 in one place, there might be additional configuration required to define the use of specific products or processes in your installation directory, like how the product will work with the same configuration.

3.2 Installing and configuring IBM Tivoli Monitoring V6.2

The following section describes the IBM Tivoli Monitoring V6.2 installation and configuration process.

Table 3-1 provides an overview of the steps required to install IBM Tivoli Monitoring V6.2.

Table 3-1 Installation steps

Steps	References
Install the hub Tivoli Enterprise Monitoring Server.	3.2.1, “Installing/configuring the hub Tivoli Enterprise Monitoring Server” on page 56
Install any remote monitoring servers.	3.2.2, “Installing and configuring the remote monitoring server” on page 81
Install the Tivoli Enterprise Portal Server.	3.2.3, “Installing the Tivoli Enterprise Portal Server” on page 89
Install monitoring agents.	3.2.4, “Installing the monitoring agents” on page 101

Steps	References
Install the portal desktop client (optional).	3.2.5, “Installing the Tivoli Enterprise Portal desktop client” on page 111

Before you begin, take note of the following information concerning the installation procedures in this chapter:

- The installation procedures provide information for installing a single component (such as the monitoring server) on one computer. If you want to install multiple components (such as the monitoring server and the portal server) on the same computer and you want to install them simultaneously, the actual steps might vary. Refer to the *IBM Tivoli Monitoring Version 6.2.0 Installation and Setup Guide,* GC32-9407 for further information.
- The following sections contain Windows, Linux, and UNIX procedures for installing the various components. Use the procedure that best applies to your environment layout. For example, you can install a monitoring server on UNIX, a portal server on Linux, and a portal desktop client on Windows.
- If your site uses the IP.PIPE protocol for communications, be aware of the following limitations:
  - There can be at most 16 IP.PIPE processes per host.
  - IP.PIPE uses one, and only one, physical port per process. Port numbers are allocated using a well-known port allocation algorithm. The first process for a host is assigned port 1918, which is the default.
  - KDC_PORTS is not supported for IP.PIPE.

  If you need to have more than 16 processes per host, use IP.UDP (User Datagram Protocol) for connections between IBM Tivoli Monitoring V6.2 components.

3.2.1 Installing/configuring the hub Tivoli Enterprise Monitoring Server

We will start by installing the hub Tivoli Enterprise Monitoring Server in Windows and UNIX Systems in our test environment.

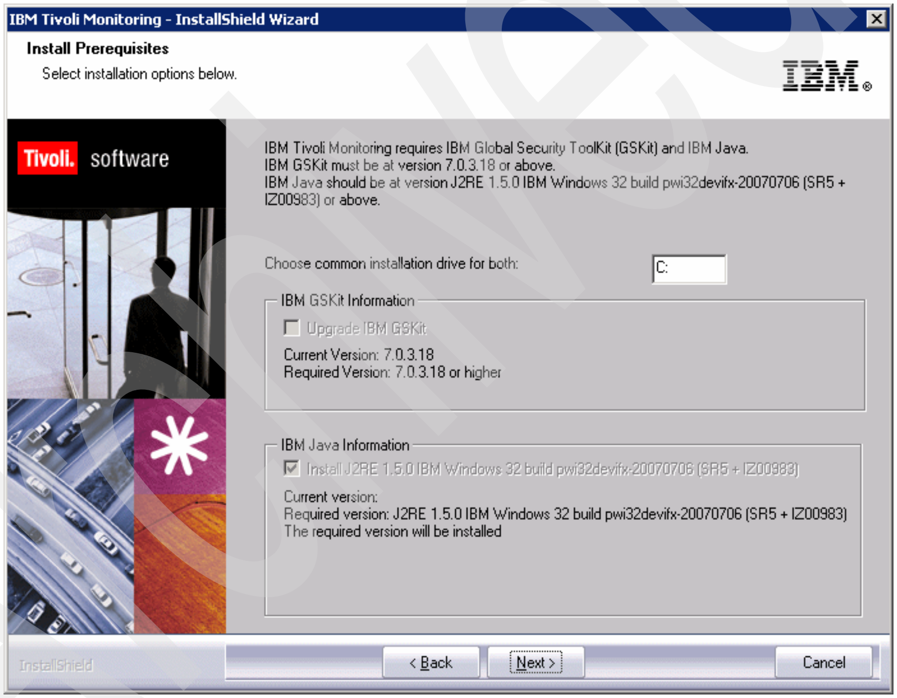
Installing the hub monitoring server on a Windows system

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

1. Launch the installation wizard by double-clicking the setup.exe file in the \WINDOWS subdirectory 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. In the Install Prerequisites window, read the information about the required levels of IBM Global Security Toolkit (GSKit) and IBM Java. The check box for each prerequisite is cleared if the correct level of the software is already installed (Figure 3-3). Otherwise, the check box is selected to indicated that the software is to be installed.


IBM Tivoli Monitoring - InstallShield Wizard
Install Prerequisites
Select installation options below.
IBM
Tivoli. software
InstallShield
< Back
Next >
Cancel

IBM Tivoli Monitoring requires IBM Global Security ToolKit (GSKit) and IBM Java.
IBM GSKit must be at version 7.0.3.18 or above.
IBM Java should be at version J2RE 1.5.0 IBM Windows 32 build pwi32devifx-20070706 (SR5 + IZ00983) or above.

Choose common installation drive for both: C:

IBM GSKit Information
□ Upgrade IBM GSKit
Current Version: 7.0.3.18
Required Version: 7.0.3.18 or higher

IBM Java Information
☑ Install J2RE 1.5.0 IBM Windows 32 build pwi32devifx-20070706 (SR5 + IZ00983)
Current version:
Required version: J2RE 1.5.0 IBM Windows 32 build pwi32devifx-20070706 (SR5 + IZ00983)
The required version will be installed

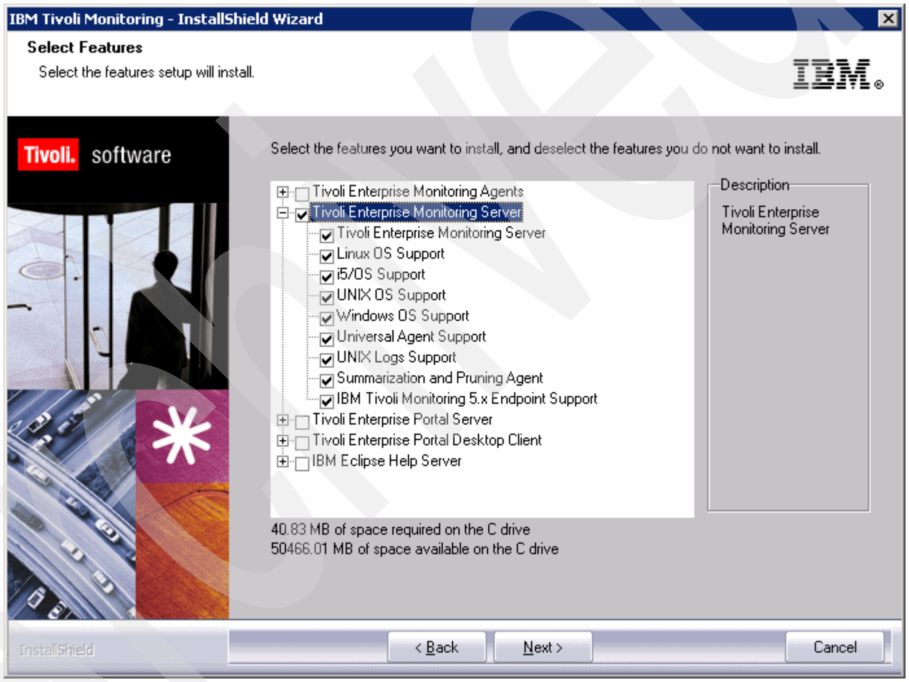
Figure 3-3 Install Prerequisites

4. Click **Next**. The prerequisite software is installed if necessary.
5. Click **Accept** to accept the license agreement.
6. Choose the directory where you want to install the product. The default directory is C:\IBM\ITM. Click **Next**.

7. Type a 32-character encryption key. You can use the default key. Click **Next** and then click **OK** to confirm the encryption key.

> **Note:**
>
> - Do not use the “=”, “,”, or “l” 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.

8. In the Select Features window, select the check box for **Tivoli Enterprise Monitoring Server (**Figure 3-4).



IBM Tivoli Monitoring - InstallShield Wizard

Select Features

Select the features setup will install.

Select the features you want to install, and deselect the features you do not want to install.

- □ Tivoli Enterprise Monitoring Agents
- ☑ Tivoli Enterprise Monitoring Server
  - ☑ Tivoli Enterprise Monitoring Server
  - ☑ Linux OS Support
  - ☑ i5/OS Support
  - ☑ UNIX OS Support
  - ☑ Windows OS Support
  - ☑ Universal Agent Support
  - ☑ UNIX Logs Support
  - ☑ Summarization and Pruning Agent
  - ☑ IBM Tivoli Monitoring 5.x Endpoint Support
- □ Tivoli Enterprise Portal Server
- □ Tivoli Enterprise Portal Desktop Client
- □ IBM Eclipse Help Server

Description

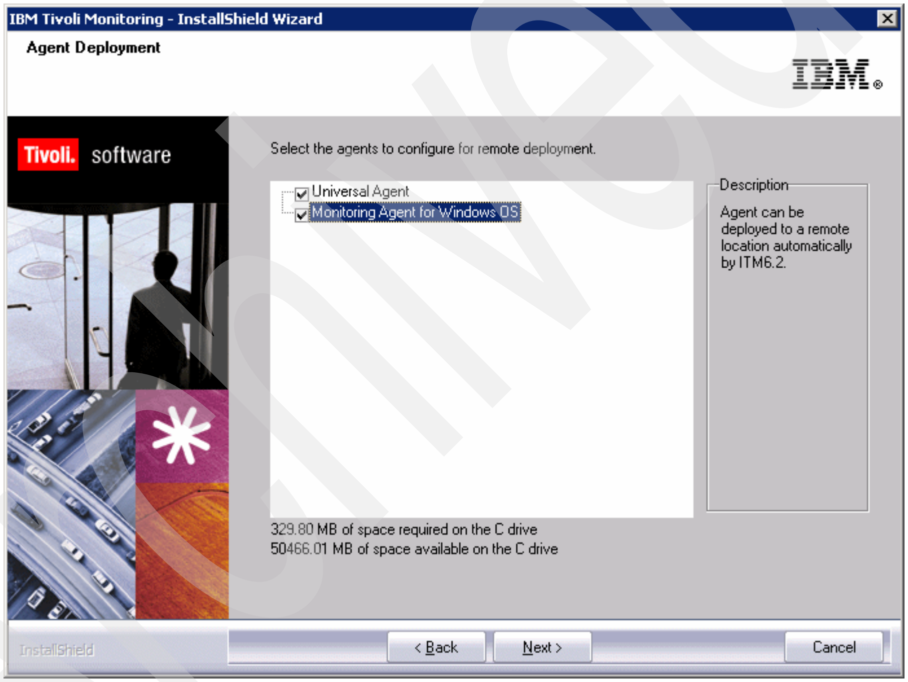
Tivoli Enterprise Monitoring Server

40.83 MB of space required on the C drive
50466.01 MB of space available on the C drive

Figure 3-4 Selecting features to install

> **Note:** When you select the **Tivoli Enterprise Monitoring Server** check box, all of the check boxes in the attached subtree are automatically selected. The support check boxes in the subtree are for installing application support files for base monitoring agents to the monitoring server. (The base monitoring agents are included with the base IBM Tivoli Monitoring V6.2 installation package.) It is best to leave all of the support check boxes selected so you do not need to re-configure application support as new agent types are added to your environment.

9. Click **Next** to display the Agent Deployment window (Figure 3-5). The agent depot contains agents that you can deploy to remote computers.



IBM Tivoli Monitoring - InstallShield Wizard

Agent Deployment

Select the agents to configure for remote deployment.

☑ Universal Agent
☑ Monitoring Agent for Windows OS

Description

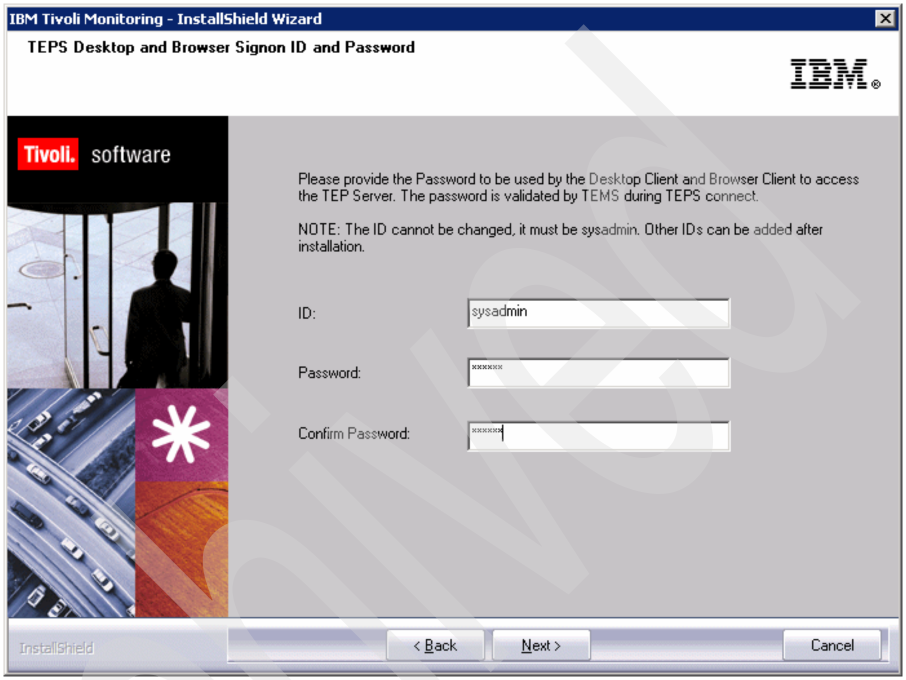
Agent can be deployed to a remote location automatically by ITM6.2.

329.80 MB of space required on the C drive
50466.01 MB of space available on the C drive

Figure 3-5 Agent remote deployment depot

10. If no IBM Tivoli Monitoring V6.2 component has been previously installed on this computer, a window is displayed for you to select a program folder for the Windows Start menu. Select a program folder and click **Next**. The default program folder name is IBM Tivoli Monitoring.

11. If the TEPS Desktop and Browser Signon ID and Password window is displayed (Figure 3-6), enter and confirm the password to be used for logging on to the Tivoli Enterprise Portal. The default logon user ID, sysadmin, cannot be changed on this window.


IBM Tivoli Monitoring - InstallShield Wizard
TEPS Desktop and Browser Signon ID and Password
IBM
Tivoli. software
InstallShield
< Back
Next >
Cancel

Please provide the Password to be used by the Desktop Client and Browser Client to access the TEP Server. The password is validated by TEMS during TEPS connect.

NOTE: The ID cannot be changed, it must be sysadmin. Other IDs can be added after installation.

ID: sysadmin

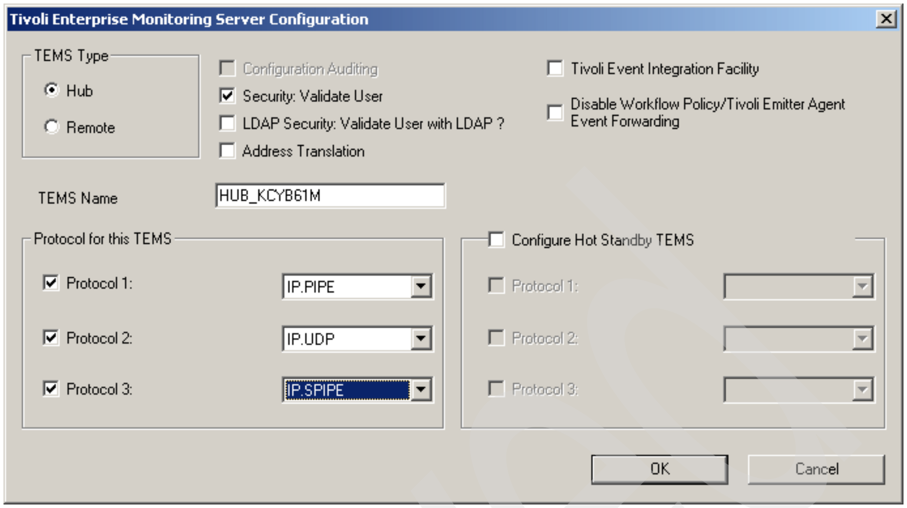
Password: ******

Confirm Password: ******

Figure 3-6 TEPS Desktop and Browser Signon ID and Password

> **Note:** This password is required only when Security: Validate Users is enabled on the hub monitoring server. This window is not displayed if the sysadmin user ID has already been defined in the operating system.

12. Review the installation summary details. The summary identifies the components you are installing. Click **Next** to begin the installation. After the components are installed, a configuration window (called the Setup Type window) is displayed.
13. Click **Next** to start configuring all selected components.
14. Configure the Tivoli Enterprise Monitoring Server (Figure 3-7 on page 61).



Tivoli Enterprise Monitoring Server Configuration

TEMS Type
● Hub
○ Remote

□ Configuration Auditing
☑ Security: Validate User
□ LDAP Security: Validate User with LDAP ?
□ Address Translation

□ Tivoli Event Integration Facility
□ Disable Workflow Policy/Tivoli Emitter Agent Event Forwarding

TEMS Name: HUB_KCYB61M

Protocol for this TEMS
☑ Protocol 1: IP.PIPE
☑ Protocol 2: IP.UDP
☑ Protocol 3: IP.SPIPE

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

Figure 3-7 Tivoli Enterprise Monitoring Server Configuration

a. Select the type of monitoring server you are configuring: Hub or Remote. For this procedure, select **Hub**.

b. Verify that the name of this monitoring server is correct in the TEMS Name field. If it is not, change it. The default name is *HUB_host_name*, for example, HUB_itmserv16.

c. Identify the communications protocol for the monitoring server. You have four choices: IP.UDP, IP.PIPE, IP.SPIPE, or SNA. You can specify up to three methods for communication. If the method you identify as Protocol 1 fails, Protocol 2 is used as a backup. If Protocol 2 fails, Protocol 3 is used as a backup.

> **Note:** Do not select any of the other options on this window (for example, **Address Translation**, **Tivoli Event Integration Facility**, or the option to configure **Hot Standby**). You can configure these options after installation is complete.

d. Click **OK**.

e. Complete the following fields for the communications protocol for the monitoring server. Table 3-2 describes the communication protocols that can be used. This information is valid for all components in the IBM Tivoli Monitoring V6.2 environment.

Table 3-2 Communications protocol settings

Field	Description
IP.UDP Settings	
Host name or IP Address	The host name or IP address for the hub monitoring server.
Port # or Port Pools	The listening port for the hub monitoring server. The default port is 1918.
IP.PIPE Settings	
Host name or IP Address	The host name or IP address for the hub monitoring server.
Port # or Port Pools	The listening port for the hub monitoring server. The default port is 1918.
SNA Settings	
Network Name	The SNA network identifier for your location.
LU Name	The LU name for the monitoring server. This LU name corresponds to the Local LU Alias in your SNA communications software.
LU 6.2 LOGMODE	The name of the LU6.2 LOGMODE. The default value is CANCTDCS.
TP Name	The transaction program name for the monitoring server.

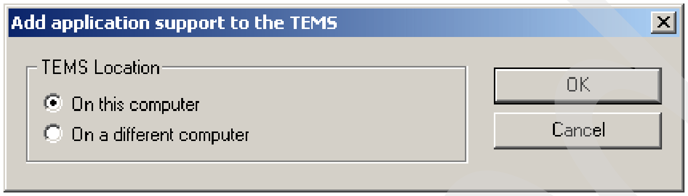
f. If you are certain that you have typed the values for all of these fields with *exactly* the correct case (upper and lower cases), you can select **Use case as typed**. However, because IBM Tivoli Monitoring V6.2 is case-sensitive, consider selecting **Convert to upper case** to reduce the chance of user error.

g. Click **OK** to continue.

15. If you selected **Tivoli Event Integration Facility**, provide the host name and port number for the Tivoli Enterprise Console event server or Netcool/OMNIbus Event Integration Facility (EIF) probe to which you want to forward events and click **OK**.

16. Enable application support on the monitoring server. In step 8 on page 58, we selected the base monitoring agents for which we wanted to install application support files on the monitoring server. In this step, we activate the application support through a process known as seeding the monitoring server. We can seed **On this computer** or **On a different computer**.

    a. Select **On this computer** and click **OK** (Figure 3-8).



Add application support to the TEMS

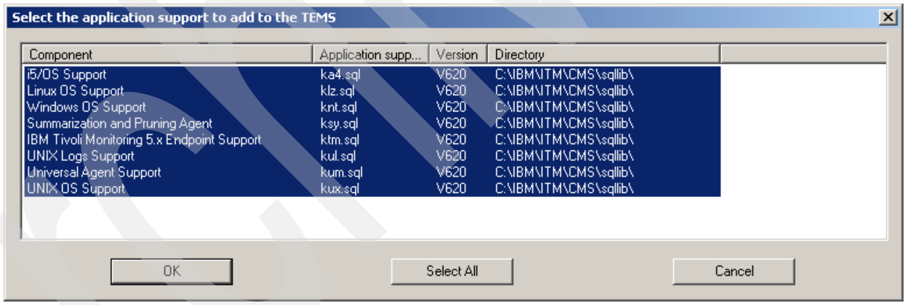
TEMS Location

● On this computer

○ On a different computer

Figure 3-8 Adding application support

    b. Click **OK** on the Select the application support to add to the TEMS window (Figure 3-9). This window lists the monitoring agents that you selected in step 8 on page 58. Click **OK** to begin seeding the monitoring server (using the SQL files listed on this window). This process can take up to 20 minutes.

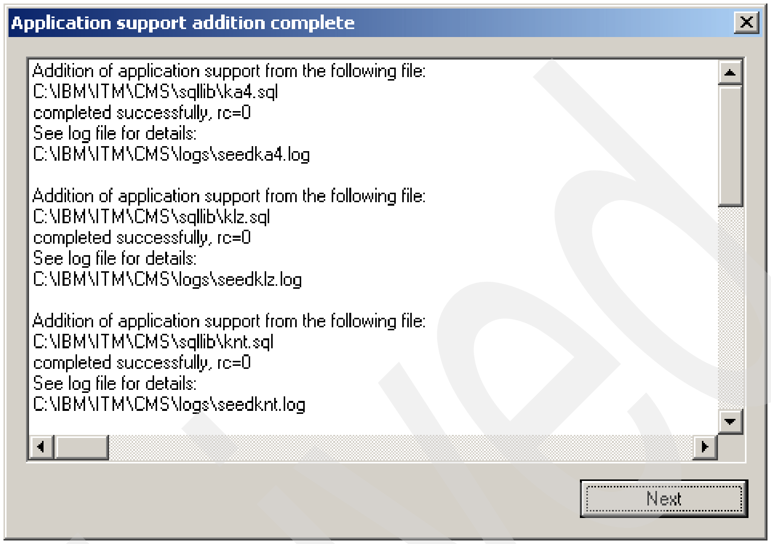


Select the application support to add to the TEMS

Component	Application supp...	Version	Directory
i5/OS Support	ka4.sql	V620	C:\IBM\ITM\CMS\sqllib\
Linux OS Support	klz.sql	V620	C:\IBM\ITM\CMS\sqllib\
Windows OS Support	knt.sql	V620	C:\IBM\ITM\CMS\sqllib\
Summarization and Pruning Agent	ksy.sql	V620	C:\IBM\ITM\CMS\sqllib\
IBM Tivoli Monitoring 5.x Endpoint Support	ktm.sql	V620	C:\IBM\ITM\CMS\sqllib\
UNIX Logs Support	kul.sql	V620	C:\IBM\ITM\CMS\sqllib\
Universal Agent Support	kum.sql	V620	C:\IBM\ITM\CMS\sqllib\
UNIX OS Support	kux.sql	V620	C:\IBM\ITM\CMS\sqllib\

Figure 3-9 Adding application support

c. Click **Next** on the message that provides results for the process of adding application support (Figure 3-10). A return code of 0 (rc: 0) indicates that the process has succeeded.



```
Addition of application support from the following file:
C:\IBM\ITM\CMS\sqllib\ka4.sql
completed successfully, rc=0
See log file for details:
C:\IBM\ITM\CMS\logs\seedka4.log

Addition of application support from the following file:
C:\IBM\ITM\CMS\sqllib\klz.sql
completed successfully, rc=0
See log file for details:
C:\IBM\ITM\CMS\logs\seedklz.log

Addition of application support from the following file:
C:\IBM\ITM\CMS\sqllib\knt.sql
completed successfully, rc=0
See log file for details:
C:\IBM\ITM\CMS\logs\seedknt.log
```

Figure 3-10 Application support results

17. Configure the communication between any IBM Tivoli Monitoring V6.2 component and the hub monitoring server:

    a. Specify the default values for IBM Tivoli Monitoring V6.2 components to use when they communicate with the monitoring server.

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

        ii. Identify the type of protocol that the agents use to communicate with the hub monitoring server. You have four choices: IP.UDP, IP.PIPE, IP.SPIPE, or SNA. You can specify up to three methods for communication. If the method you identify as Protocol 1 fails, Protocol 2 is used as a backup. If Protocol 2 fails, Protocol 3 is used as a backup.

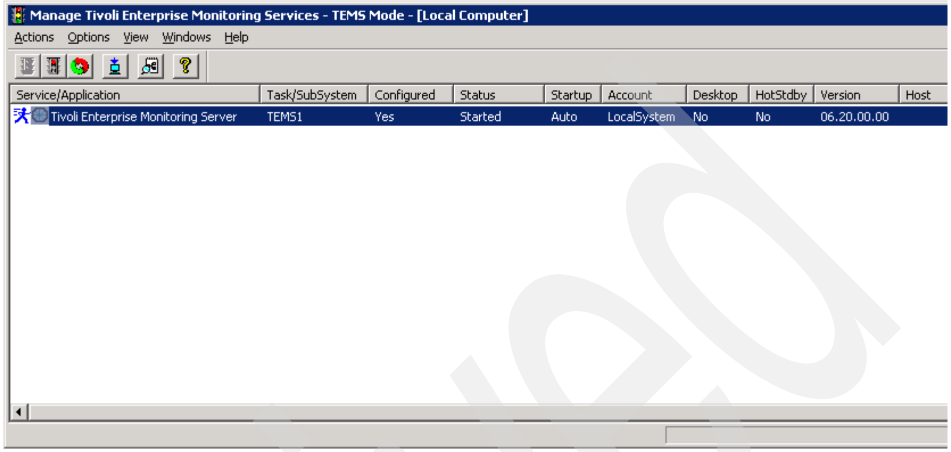
    b. Click **OK**.

    c. Complete the communication protocol fields for the monitoring server. See Table 3-2 on page 62 for definitions of these fields. Click **OK**.

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

19. Click **Finish** on the Maintenance Complete window if you are updating an existing installation.

The Manage Tivoli Monitoring Services utility is opened, as shown in Figure 3-11. (This might take a few minutes.) Now we can start, stop, and configure IBM Tivoli Monitoring V6.2 components with this utility.


Manage Tivoli Enterprise Monitoring Services - TEMS Mode - [Local Computer]
Actions
Options
View
Windows
Help

Service/Application	Task/SubSystem	Configured	Status	Startup	Account	Desktop	HotStdby	Version	Host
Tivoli Enterprise Monitoring Server	TEMS1	Yes	Started	Auto	LocalSystem	No	No	06.20.00.00	

Figure 3-11 Manage Tivoli Monitoring Services

Installing the hub monitoring server on a Linux or UNIX server

Before starting our hub installation, you need to check some prerequisites mentioned in 2.2.4, “Supported operating systems” on page 30. In our setup, first we checked the AIX XC C/C++ version (Example 3-1), which should be at 8.0.0.4 version.

Example 3-1 Verifying the xlc version

```
[root@server2][/]-> lslpp -l |grep -i xlc
  xlC.aix50.rte             6.0.0.13  COMMITTED  C Set ++ Runtime for
AIX 5.0
  xlC.cpp                    6.0.0.0  COMMITTED  C for AIX Preprocessor
  xlC.msg.en_US.cpp          6.0.0.0  COMMITTED  C for AIX Preprocessor
  xlC.msg.en_US.rte          6.0.0.0  COMMITTED  C Set ++ Runtime
  xlC.rte                    6.0.0.0  COMMITTED  C Set ++ Runtime
```

Because we did not have the correct version, we downloaded the package from `http://www-1.ibm.com/support/docview.wss?uid=swg1IY84212` and performed the following steps to install it:

1. Uncompress and untar the package into a directory.
2. Run **`inutoc .`** to create the .toc file.

3. Run the following command to update the xlC filesets:

```
/usr/lib/instl/sm_inst installp_cmd -a -d '.' -f '_update_all' '-c'
'-N' '-g' '-X'
```

4. After finishing the installation, we can check the new version, as shown in Example 3-2.

Example 3-2 Verifying the new version

```
[root@server2][/appo/xlc_8008]-> lslpp -l |grep -i xlc
  xlC.aix50.rte              8.0.0.8  COMMITTED  C Set ++ Runtime
for AIX 5.0
  xlC.cpp                    6.0.0.0  COMMITTED  C for AIX
Preprocessor
  xlC.msg.en_US.cpp          6.0.0.0  COMMITTED  C for AIX
Preprocessor
  xlC.msg.en_US.rte          8.0.0.8  COMMITTED  C Set ++ Runtime
  xlC.rte                    8.0.0.8  COMMITTED  C Set ++ Runtime
```

Now that the xLC is updated, we will use the following steps to install and configure the hub monitoring server on a Linux or UNIX computer.

> **Note:** GSKit *must* be installed from a user ID with root or administrator authority. If you are running the installer program interactively as non-root, the installer will prompt you for the root password. If you do not supply the root password when prompted or supply an invalid password, then GSKit must be installed manually from a user ID with root or administrator authority when the installation has completed. If you perform the installation using a silent installation as non-root, the prompt for the root password is bypassed, and GSKit must be installed manually from a user ID with root or administrator authority after the silent installation has completed.

1. In the directory where you have extracted the installation files, run the command **./install.sh**.
2. When prompted for the IBM Tivoli Monitoring V6.2 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.

Example 3-3 Running install.sh

```
[itmuser@server2][/home/itmuser]-> cd /appo/itm62
[itmuser@server2][/appo/itm62]-> install.sh
INSTALL

Enter the name of the IBM Tivoli Monitoring directory
```

```
[ default = /opt/IBM/ITM ]:

ITM home directory "/opt/IBM/ITM" already exists.
OK to use it [ 1-yes, 2-no; "1" is default ]?  1
```

3. If the directory you specified does not exist, you are asked whether to create it. Type 1 to create this directory.
4. The output shown in Example 3-4 is displayed. Type 1 to start the installation and press Enter. The user license agreement display is displayed. Press Enter to read through the agreement.

Example 3-4 Output of install.sh

```
Select one of the following:

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

Please enter a valid number:  1

Initializing ...
install.sh warning: unarchive of "/appo/itm62/unix/jraix526.tar" may
have failed, continuing ...
International Program License Agreement

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

Press Enter to continue viewing the license agreement, or
enter "1" to accept the agreement, "2" to decline it, "3"
to print it, "4" to read non-IBM terms, or "99" to go back
to the previous screen.
```

5. Type 1 to accept the agreement (Example 3-4 on page 67) and press Enter.
6. Type a 32-character encryption key and press Enter. If you want to use the default key, press Enter without typing any characters.

> **Note:**
>
> - Do not use the “=”, “,”, or “|” 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.

Example 3-5 GSKit install process from install.sh

```
lslpp: 0504-132  Fileset gskta.rte not installed.
lslpp: 0504-132  Fileset gskta.rte not installed.
Preparing to install the IBM Global Security Kit (GSkit)

+-------------------------------------------------------------------+
                    Pre-installation Verification...
+-------------------------------------------------------------------+
Verifying selections...done
Verifying requisites...done
Results...

SUCCESSES
---------
  Filesets listed in this section passed pre-installation
verification and will be installed.

  Selected Filesets
  -----------------
  gskjt.rte 7.0.3.18  # AIX Certificate and SSL Java...
  gskta.rte 7.0.3.18  # AIX Certificate and SSL Base...

  << End of Success Section >>

FILESET STATISTICS
------------------
    2  Selected to be installed, of which:
        2  Passed pre-installation verification
  ----
    2  Total to be installed

+-------------------------------------------------------------------+
                         Installing Software...
+------------------------------------------------------------------+

installp:  APPLYING software for:
        gskjt.rte 7.0.3.18

. . . . . << Copyright notice for gskjt >> . . . . . . .
 Licensed Materials - Property of IBM

 999999999
   (C) Copyright International Business Machines Corp. 1996, 2002,
2003.
   (C) Copyright Netscape Communications Corporation.  1995.
   (C) Copyright RSA Laboratories, a division of RSA Data Security,
Inc. 1991.

 All rights reserved.
 US Government Users Restricted Rights - Use, duplication or
disclosure restricted by GSA ADP Schedule Contract with IBM Corp.
. . . . . << End of copyright notice for gskjt >>. . . .

Filesets processed:  1 of 2  (Total time:  2 secs).

installp:  APPLYING software for:
        gskta.rte 7.0.3.18

. . . . . << Copyright notice for gskta >> . . . . . . .
 Licensed Materials - Property of IBM

 999999999
   (C) Copyright International Business Machines Corp. 1996, 2002,
2003.
   (C) Copyright Netscape Communications Corporation.  1995.
   (C) Copyright RSA Laboratories, a division of RSA Data Security,
Inc. 1991.

 All rights reserved.
 US Government Users Restricted Rights - Use, duplication or
disclosure restricted by GSA ADP Schedule Contract with IBM Corp.
. . . . . << End of copyright notice for gskta >>. . . .

--- postinstall ---
Linking suitable library according to the machine
Finished processing all filesets.  (Total time:  6 secs).
```

```
+-------------------------------------------------------------------+
                                Summaries:
+-------------------------------------------------------------------+
Installation Summary
--------------------
Name        Level           Part        Event       Result
---------------------------------------------------------------------
gskjt.rte   7.0.3.18        USR         APPLY       SUCCESS
gskta.rte   7.0.3.18        USR         APPLY       SUCCESS
+-------------------------------------------------------------------+
                    Pre-installation Verification...
+-------------------------------------------------------------------+
Verifying selections...done
Verifying requisites...done
Results...

SUCCESSES
---------
  Filesets listed in this section passed pre-installation
verification and will be installed.

  Selected Filesets
  -----------------
  gskjs.rte 7.0.3.18  # AIX Certificate and SSL Java...
  gsksa.rte 7.0.3.18  # AIX Certificate and SSL Base...

  << End of Success Section >>

FILESET STATISTICS
------------------
    2  Selected to be installed, of which:
        2  Passed pre-installation verification
  ----
    2  Total to be installed
+-------------------------------------------------------------------+
                         Installing Software...
+-------------------------------------------------------------------+
installp:  APPLYING software for:
        gsksa.rte 7.0.3.18

. . . . . << Copyright notice for gsksa >> . . . . . . .
 Licensed Materials - Property of IBM

 999999999
```

```
   (C) Copyright International Business Machines Corp. 1996, 2002,
2003.
   (C) Copyright Netscape Communications Corporation.  1995.
   (C) Copyright RSA Laboratories, a division of RSA Data Security,
Inc. 1991.

 All rights reserved.
 US Government Users Restricted Rights - Use, duplication or
disclosure restricted by GSA ADP Schedule Contract with IBM Corp.
. . . . . << End of copyright notice for gsksa >>. . . .

Filesets processed:  1 of 2  (Total time:  4 secs).

installp:  APPLYING software for:
        gskjs.rte 7.0.3.18

. . . . . << Copyright notice for gskjs >> . . . . . . .
 Licensed Materials - Property of IBM

 999999999
   (C) Copyright International Business Machines Corp. 1996, 2002,
2003.
   (C) Copyright Netscape Communications Corporation.  1995.
   (C) Copyright RSA Laboratories, a division of RSA Data Security,
Inc. 1991.

 All rights reserved.
 US Government Users Restricted Rights - Use, duplication or
disclosure restricted by GSA ADP Schedule Contract with IBM Corp.
. . . . . << End of copyright notice for gskjs >>. . . .

sysck: 3001-036 WARNING:  File
        /bin/gsk7jk
        is also owned by fileset gskjt.rte.
Finished processing all filesets.  (Total time:  5 secs).
+-----------------------------------------------------------------------------+
                                Summaries:
+-----------------------------------------------------------------------------+
Installation Summary
--------------------
Name        Level           Part        Event       Result
-----------------------------------------------------------------------------
gsksa.rte   7.0.3.18        USR         APPLY       SUCCESS
gskjs.rte   7.0.3.18        USR         APPLY       SUCCESS
```

```
Enter a 32-character encryption key, or just press Enter to use the
default
        Default = IBMTivoliMonitoringEncryptionKey
....+....1....+....2....+....3..

GSkit encryption key has been set.
Key File directory: /opt/IBM/ITM/keyfiles
```

7. Type the number for the operating system on which you are installing the monitoring server. The default value is your current operating system. Press Enter.
8. Type 1 to confirm the operating system and press Enter. A numbered list of available components is displayed.
9. Type the number that corresponds to the Tivoli Enterprise Monitoring Server option. Press Enter.
10. Type 1 to confirm the installation. The installation begins (Example 3-6).

Example 3-6 Installation begins

```
Product packages are available in /appo/itm62/unix

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

 1) AIX R5.2 (32 bit)
 2) AIX R5.2 (64 bit)
 3) AIX R5.3 (32 bit)
 4) AIX R5.3 (64 bit)
 5) Tivoli Enterprise Portal Browser Client support
 6) Tivoli Enterprise Portal Server support
 7) Tivoli Enterprise Monitoring Server support

Type the number for the OS or component support category you want,
or type "q" to quit selection
[ number "4" or "AIX R5.3 (64 bit)" is default ]:

You selected number "4" or "AIX R5.3 (64 bit)"

Is the operating system or component support correct [ 1=Yes, 2=No ;
default is "1" ] ? y

The following products are available for installation:

 1) Monitoring Agent for UNIX Logs  V06.20.00.00
 2) Monitoring Agent for UNIX OS  V06.20.00.00
 3) Summarization and Pruning Agent  V06.20.00.00
 4) Tivoli Enterprise Monitoring Server  V06.20.00.00
 5) Tivoli Enterprise Portal Server  V06.20.00.00
 6) Tivoli Enterprise Services User Interface  V06.20.00.00
 7) Universal Agent  V06.20.00.00
 8) Warehouse Proxy  V06.20.00.00
 9) 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

The following products will be installed:

  Tivoli Enterprise Monitoring Server  V06.20.00.00

Are your selections correct [ 1=Yes, 2=No ; default is "1" ] ?

 ... installing "Tivoli Enterprise Monitoring Server  V06.20.00.00
for AIX R5.3 (64 bit)"; please wait.

 => installed "Tivoli Enterprise Monitoring Server  V06.20.00.00 for
AIX R5.3 (64 bit)".
... Initializing component Tivoli Enterprise Monitoring Server
V06.20.00.00 for AIX R5.3 (64 bit).
```

11. When prompted, type a name for your monitoring server. Do not use the fully qualified host name (Example 3-7). Press Enter.

Example 3-7   Install process finishing

```
Please enter TEMS name [ TEMS is default ]: HUB_TEMS
... creating config file
"/opt/IBM/ITM/config/server2_ms_HUB_TEMS.config"
... creating file "/opt/IBM/ITM/tables/HUB_TEMS/glb_site.txt."
... updating "/opt/IBM/ITM/config/kbbenv"
... verifying Hot Standby.
... Tivoli Enterprise Monitoring Server  V06.20.00.00 for AIX R5.3
(64 bit) initialized.
```

```
Do you want to install additional products or product support
packages [ 1=Yes, 2=No ; default is "2" ] ?
... postprocessing; please wait.
... finished postprocessing.
Installation step complete.

As a reminder, you should install product support on each of your
TEM servers for any agents you have just installed.
This is done via the "/opt/IBM/ITM/bin/itmcmd support" command on
your TEM servers.

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

12. After all of the components are installed, you are asked whether you want to install components for a different operating system or not (Example 3-7 on page 73). Type 2 and press Enter.

The installation is complete. The next step is to configure your monitoring server.

Hub monitoring server configuration on a Linux or UNIX server

This installation is different than the Windows installation in that we have to perform some configuration steps in order to start the hub monitoring 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 V6.2).
2. Run the following command:

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

3. Press Enter to indicate that this is a hub monitoring server (indicated by the *LOCAL default).
4. Press Enter to accept the default host name for the monitoring server. This should be the host name for your computer. If it is not, type the correct host name and then press Enter.
5. Enter the type of protocol to use for communication with the monitoring server. You have four choices: IP, IP.PIPE, IP.SPIPE, or SNA. Press Enter to use the default communications protocol (IP.PIPE).
6. If you want to set up a backup protocol, enter that protocol and press Enter. If you do not want to use backup protocol, press Enter without specifying a protocol. In our case, we configured two protocols, as shown in Example 3-8 on page 75.

Example 3-8 Configuring hub monitoring server

```
[root@server2][/appo/itm62]-> itmcmd config -S -t HUB_TEMS
Configuring TEMS...

Hub or Remote [1=*LOCAL, 2=*REMOTE] (Default is: 1):
TEMS hostname (Default is: server2):

Network Protocol 1 [ip, sna, ip.pipe or ip.spipe] (Default is:
ip.pipe):

     Now choose the next protocol number from one of these:
     - ip
     - sna
     - ip.spipe
     - 0 for none
Network Protocol 2 (Default is: 0): ip

     Now choose the next protocol number from one of these:
     - sna
     - ip.spipe
     - 0 for none
Network Protocol 3(Default is: 0): ip.spipe
IP Port Number (Default is: 1918):
IP.PIPE Port Number (Default is: 1918):
Enter name of KDC_PARTITION (Default is: null):
Enter path and name of KDC_PARTITIONFILE (Default is:
/opt/IBM/ITM/tables/HUB_TEMS/partition.txt):
IP.SPIPE Port Number (Default is: 3660):
```

7. Depending on the type of protocol you specified, provide the information shown in Table 3-3 when prompted.

Table 3-3 UNIX monitoring server protocols and values

Protocol	Value	Definition
IP.UDP	IP Port Number	The port number for the monitoring server. The default is 1918.
SNA	Net Name	The SNA network identifier for your location.
	LU Name	The LU name for the monitoring server. This LU name corresponds to the Local LU Alias in your SNA communications software.
	Log Mode	The name of the LU6.2 LOGMODE. The default value is .CANCTDCS.

Protocol	Value	Definition
IP.PIPE	IP.PIPE Port Number	The port number for the monitoring server. The default is 1918.
IP.SPIPE	IP.SPIPE Port Number	The port number for the monitoring server. The default is 3660.

8. Press Enter to *not* specify the name of the KDC_PARTITION. You can configure the partition file at a later time; for further information about firewall configuration, you can refer to *IBM Tivoli Monitoring Version 6.2.0 Installation and Setup Guide,* GC32-9407 or Chapter 4, “Firewall considerations”, of *IBM Tivoli Monitoring: Implementation and Performance Optimization for Large Scale Environments*, SG24-7443.
9. Press Enter when prompted for the path and name of the KDC_PARTITION.
10. If you want to use Configuration Auditing, press Enter. If you do not want to use this feature, type 2 and press Enter.
11. Press Enter to accept the default setting for the Hot Standby feature (none).

> **Note:** The Hot Standby feature, also referred to as the Fault Tolerant Option (FTO) provided by the Tivoli Monitoring platform, allows a standby hub monitoring server to be configured that can take over operations of the hub monitoring server in case it becomes unavailable. This mechanism specifically addresses the availability of the hub monitoring server, as opposed to the clustering solution, which can address a number of other Tivoli Monitoring components as well. Refer to Chapter 10, “IBM Tivoli Monitoring resiliency and high availability” of *IBM Tivoli Monitoring: Implementation and Performance Optimization for Large Scale Environments*, SG24-7443 for more information about Hot Standby and cluster solutions in IBM Tivoli Monitoring.

12. Press Enter to accept the default for the Optional Primary Network Name (none).
13. Press Enter for the default Security: Validate User setting (NO).

> **Note:** You can configure the Security: Validate User after finishing the configuration. If you want to configure this setting, you need to create a sysadmin account for the Linux/UNIX box where the hub monitoring server is installed. When the security is enabled, even though they log on to the portal server, users attempting to use the Tivoli Enterprise Portal application will be authenticated at the hub monitoring server.

14. If you want to forward situation events to either IBM Tivoli Enterprise Console (TEC) or the IBM Tivoli Netcool/OMNIbus console, type 1 and press Enter to enable the Tivoli Event Integration Facility. Complete the following additional steps:

    a. For EIF Server, type the host name of the TEC event server or the host name of the Netcool/OMNIbus EIF probe and press Enter.

    b. For EIF Port, type the EIF reception port number for the TEC event server or the Netcool/OMNIbus EIF probe and press Enter.

15. To disable Workflow Policy/Tivoli Emitter Agent event forwarding, type 1 and press Enter. Otherwise, press Enter to accept the default (2=NO).

16. Type s to accept the default SOAP configuration and exit the configuration.

> **Note:** You can configure any SOAP information at a later time.
>
> IBM provides numerous SOAP methods with IBM Tivoli Monitoring Web services. These methods enable you to dynamically query and control IBM Tivoli Monitoring environments. Using IBM SOAP methods, you can:
>
> - Stop or start policies and situations.
> - Forward AF/Remote trapped messages and display them on a Universal Message console.
> - Retrieve attribute data that you can display in charts or reports.
> - Open and close events.
> - Make real-time requests for data.
> - Issue SOAP requests as system commands in Tivoli Enterprise Portal.
>
> You can also use this product to test a request to ensure that it works properly. You can then create a policy that submits multiple requests for processing. You can also generate daily operation summaries and store retrieved data in the Tivoli Data Warehouse.
>
> Please consult *IBM Tivoli Monitoring Version 6.2.0 Installation and Setup Guide,* GC32-9407 for more information.

Example 3-9 shows the final steps to finish the configuration.

Example 3-9 Finishing hub monitoring server configuration

```
Configuration Auditing? [1=YES, 2=NO] (Default is: 1):
Hot Standby TEMS hostname or type 0 for "none" (Default is: 0):
Enter Optional Primary Network Name or type 0 for "none" :(Default
is: 0):
Security: Validate User ? [1=YES, 2=NO] (Default is: 2):
Tivoli Event Integration Facility? [1=YES, 2=NO] (Default is: 2):
Disable Workflow Policy/Tivoli Emitter Agent Event Forwarding?
[1=YES, 2=NO] (Default is: 2):
 ... Writing to database file for ms.

Hubs
##      CMS_Name
1       ip.pipe:HUB_TEMS[1918]

1)Add, 2)Remove ##, 3)Modify Hub ##, 4)UserAccess ##, 5)Cancel,
6)Save/exit: 6
... creating config file
"/opt/IBM/ITM/config/server2_ms_HUB_TEMS.config"
... creating file "/opt/IBM/ITM/tables/HUB_TEMS/glb_site.txt."
... updating "/opt/IBM/ITM/config/kbbenv"
... verifying Hot Standby.
TEMS configuration completed...
[root@server2][/appo/itm62]-> itmcmd server start HUB_TEMS
cinfo Starting TEMS...
TEMS started...
```

The monitoring server is now configured. We can check that the installation has completed by running **cinfo**, as shown in Example 3-10.

Example 3-10 Checking installation

```
[root@server2][/appo/itm62]-> cinfo  -r

*********** Thu Sep  6 16:01:39 CDT 2007 ******************
User: root Groups: system bin sys security cron audit lp
hostname : server2      Installer Lvl:06.20.00.00
CandleHome: /opt/IBM/ITM
***********************************************************
Host     Prod  PID     Owner  Start     ID        ..Status
server2  ms    250018  root   16:01:01  HUB_TEMS  ...running
[root@server2][/appo/itm62]-> cinfo -i
```

```
*********** Thu Sep  6 16:02:02 CDT 2007 ******************
User: root Groups: system bin sys security cron audit lp
hostname : server2      Installer Lvl:06.20.00.00
CandleHome: /opt/IBM/ITM
***********************************************************
...Product inventory

a4      Monitoring Agent for i5/OS
         tms     Version: 06.20.00.00

ax      IBM Tivoli Monitoring Shared Libraries
         aix523  Version: 06.20.00.00
         aix526  Version: 06.20.00.00

jr      Tivoli Enterprise-supplied JRE
         aix523  Version: 05.00.00.00
         aix526  Version: 05.00.00.00

lz      Monitoring Agent for Linux OS
         tms     Version: 06.20.00.00

ms      Tivoli Enterprise Monitoring Server
         aix523  Version: 06.20.00.00

nt      Monitoring Agent for Windows OS
         tms     Version: 06.20.00.00

sh      Tivoli Enterprise Monitoring SOAP Server
         aix523  Version: 06.20.00.00

sy      Summarization and Pruning Agent
         tms     Version: 06.20.00.00

tm      Monitoring Agent for IBM Tivoli Monitoring 5.x Endpoint
         tms     Version: 06.20.00.00

ui      Tivoli Enterprise Services User Interface
         aix523  Version: 06.20.00.00
         aix526  Version: 06.20.00.00

ul      Monitoring Agent for UNIX Logs
         tms     Version: 06.20.00.00

um      Universal Agent
         tms     Version: 06.20.00.00
```

```
ux      Monitoring Agent for UNIX OS
          tms     Version: 06.20.00.00
```

Enabling application support on a Linux or UNIX server

When we installed the IBM Tivoli Monitoring V6.2 components on Linux or UNIX boxes, the application support was installed (see Example 3-10 on page 78) for the base agents, more specifically, the agents that come with the installation media. Now we have to enable this application support for:

- Monitoring servers (hub and remote)
- Portal server
- Portal desktop clients

> **Note:** The process of enabling support is also referred to as *activating* or *adding application support*, and in the case of the monitoring server, as *seeding the monitoring server*.

Use the following procedure to add application support for base monitoring agents to a monitoring server (see Example 3-11).

1. Start the monitoring server by running the following command:

   ```
   ./itmcmd server start tems_name
   ```

2. . Run the following command to add the application support:

   ```
   ./itmcmd support -t tems_name pc
   ```

   Where pc is the product code.

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
   ```

Example 3-11 Adding application support

```
[root@server2][/appo/itm62]-> itmcmd support -t HUB_TEMS nt ux um ul lz
Multi-product support installation: nt
Copying cat and attr data...
Product support installation started...
Info: Seeding with /opt/IBM/ITM/tables/cicatrsq/SQLLIB/knt.sql
Product support installation completed...
Multi-product support installation: ux
Copying cat and attr data...
```

```
Product support installation started...
Info: Seeding with /opt/IBM/ITM/tables/cicatrsq/SQLLIB/kux.sql
Product support installation completed...
Multi-product support installation: um
Copying cat and attr data...
Product support installation started...
Info: Seeding with /opt/IBM/ITM/tables/cicatrsq/SQLLIB/kum.sql
Product support installation completed...
Multi-product support installation: ul
Copying cat and attr data...
Product support installation started...
Info: Seeding with /opt/IBM/ITM/tables/cicatrsq/SQLLIB/kul.sql
Product support installation completed...
Multi-product support installation: lz
Copying cat and attr data...
Product support installation started...
Info: Seeding with /opt/IBM/ITM/tables/cicatrsq/SQLLIB/klz.sql
Product support installation completed...
Multi-product support installation completed

[root@server2][/appo/itm62]-> itmcmd server stop HUB_TEMS;itmcmd server
start HUB_TEMS
```

3.2.2 Installing and configuring the remote monitoring server

After installing the hub monitoring server, we can now install the remote monitoring servers. The following section describes the steps to install on Windows and Linux/UNIX servers.

Installing a remote monitoring server on a Windows server

Use the following steps to perform the installation on a Windows server:

1. Launch the installation wizard by double-clicking the **`setup.exe`** file in the \WINDOWS subdirectory 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.

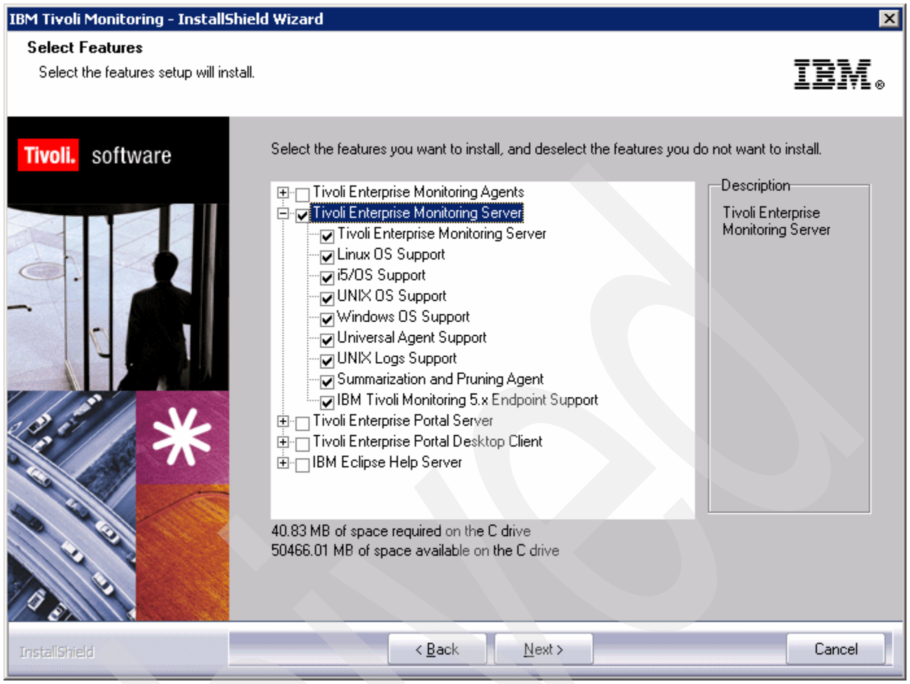
Note: If you have another IBM Tivoli Monitoring V6.2 component already installed on this computer, select **Modify** on the Welcome window to indicate that you are updating an existing installation. Click **OK** on the message telling you about preselected items.

3. In the Install Prerequisites window, read the information about the required levels of IBM Global Security Toolkit (GSKit) and IBM Java. The check box for each prerequisite is cleared if the correct level of the software is already installed. Otherwise, the check box is selected to indicated that the software is to be installed.
4. Click **Next**. The prerequisite software is installed if necessary.
5. Click **Accept** to accept the license agreement.
6. Choose the directory where you want to install the product. The default directory is C:\IBM\ITM. Click **Next**.
7. Type a 32-character encryption key. You can use the default key. Click **Next** and then click **OK** to confirm the encryption key.

Note:

- Do not use the “=”, “,”, or “|” 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.

8. On the Select Features window, select the check box for **Tivoli Enterprise Monitoring Server**. Notice that the others boxes are selected automatically (Figure 3-12 on page 83). This will install application support files for base monitoring agents to the remote monitoring server.



Select Features

Select the features setup will install.

Select the features you want to install, and deselect the features you do not want to install.

- ⊞ □ Tivoli Enterprise Monitoring Agents
- ⊟ ☑ Tivoli Enterprise Monitoring Server
  - ☑ Tivoli Enterprise Monitoring Server
  - ☑ Linux OS Support
  - ☑ i5/OS Support
  - ☑ UNIX OS Support
  - ☑ Windows OS Support
  - ☑ Universal Agent Support
  - ☑ UNIX Logs Support
  - ☑ Summarization and Pruning Agent
  - ☑ IBM Tivoli Monitoring 5.x Endpoint Support
- ⊞ □ Tivoli Enterprise Portal Server
- ⊞ □ Tivoli Enterprise Portal Desktop Client
- ⊞ □ IBM Eclipse Help Server

Description

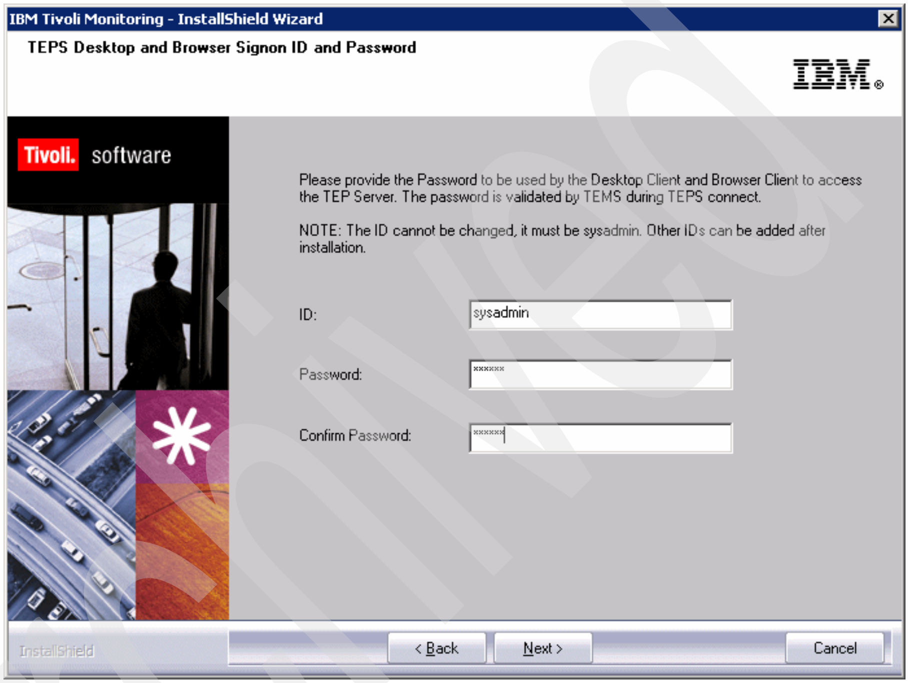
Tivoli Enterprise Monitoring Server

40.83 MB of space required on the C drive
50466.01 MB of space available on the C drive

Figure 3-12 Selecting application support

9. If you want to install any agents on this remote monitoring server, expand **Tivoli Enterprise Monitoring Agents** and select the agents you want to install.
10. Click **Next** to display the Agent Deployment window. Select the agents. This procedure will add the agent bundles to the agent depot. (You can add agents to the agent depot at a later time by updating your installation.) Click **Next**.
11. If *no* IBM Tivoli Monitoring V6.2 component has been previously installed on this computer, a window is displayed for you to select a program folder for the Windows Start menu. Select a program folder and click **Next**. The default program folder name is IBM Tivoli Monitoring.

12. If the TEPS Desktop and Browser Signon ID and Password window (Figure 3-13) is displayed, enter and confirm the password to be used for logging on to the Tivoli Enterprise Portal. The default logon user ID, sysadmin, *cannot be changed on this window*. The logon password must match the password that you specified for sysadmin when you configured the hub monitoring server. This window is not displayed if the sysadmin user ID has already been defined in the operating system.



IBM Tivoli Monitoring - InstallShield Wizard

TEPS Desktop and Browser Signon ID and Password

Please provide the Password to be used by the Desktop Client and Browser Client to access the TEP Server. The password is validated by TEMS during TEPS connect.

NOTE: The ID cannot be changed, it must be sysadmin. Other IDs can be added after installation.

ID: sysadmin

Password: ******

Confirm Password: ******

Figure 3-13 Portal server Desktop and Browser Signon ID and Password

13. Review the installation summary details. The summary identifies the components you are installing. Click **Next** to begin the installation. After the components are installed, a configuration window (called the Setup Type window) is displayed.

14. Clear the check boxes for any components that have already been installed and configured (at the current release level) on this computer, unless you want to modify the configuration. Click **Next** to start configuring all selected components.

15. Configure the Tivoli Enterprise Monitoring Server (Figure 3-14 on page 85):

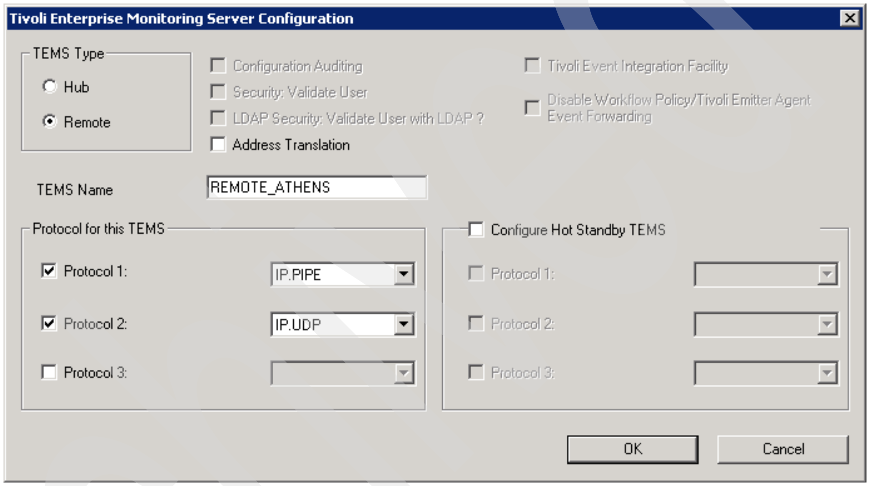
    a. Select the type of monitoring server you are configuring: hub or remote. For this procedure, select **Remote**.

b. Verify that the name of this monitoring server is correct in the TEMS Name field. If it is not, change it. The default name is REMOTE_host_name, for example, REMOTE_ATHENS.

c. Identify the communications protocol for the monitoring server. You have four choices: IP.UDP, IP.PIPE, IP.SPIPE, or SNA. You can specify up to three methods for communication.

d. Click **OK**.

e. Complete the fields shown in Figure 3-14 for the communications protocol for the monitoring server. Use Table 3-2 on page 62 as reference.



Tivoli Enterprise Monitoring Server Configuration

TEMS Type
○ Hub
● Remote

□ Configuration Auditing
□ Security: Validate User
□ LDAP Security: Validate User with LDAP ?
□ Address Translation
□ Tivoli Event Integration Facility
□ Disable Workflow Policy/Tivoli Emitter Agent Event Forwarding

TEMS Name: REMOTE_ATHENS

Protocol for this TEMS
☑ Protocol 1: IP.PIPE
☑ Protocol 2: IP.UDP
□ Protocol 3:

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

Figure 3-14 Tivoli Enterprise Monitoring Server configuration window

f. If you are certain that you have typed the values for all of these fields with exactly the correct casing (upper and lower cases), you can select **Use case** as typed. However, because IBM Tivoli Monitoring V6.2 is case-sensitive, consider selecting **Convert to upper case** to reduce the chance of user error.

g. Click **OK** to continue.

The next configuration step is to seed the monitoring server.

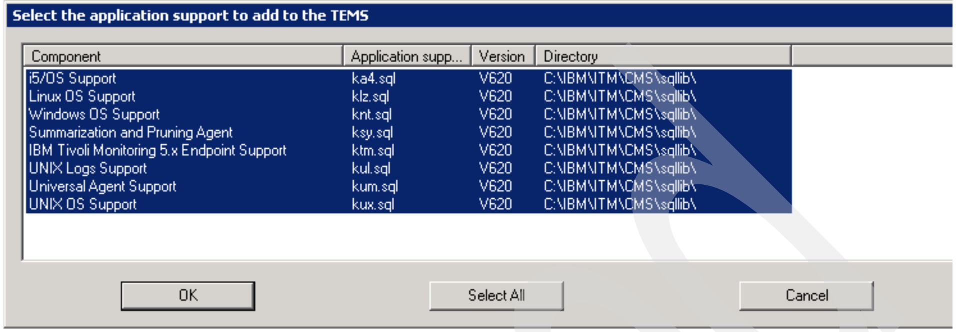
16. Specify the location of the monitoring server to which to add application support. You have two choices:

a. Specify the location of the monitoring server to which to add application support. You have two choices:

- On this computer
- On a different computer

Select **On this computer** and click **OK**.

b. Click **OK** on the Select the application support to add to the TEMS window as shown in Figure 3-15.



Select the application support to add to the TEMS

Component	Application supp...	Version	Directory
i5/OS Support	ka4.sql	V620	C:\IBM\ITM\CMS\sqllib\
Linux OS Support	klz.sql	V620	C:\IBM\ITM\CMS\sqllib\
Windows OS Support	knt.sql	V620	C:\IBM\ITM\CMS\sqllib\
Summarization and Pruning Agent	ksy.sql	V620	C:\IBM\ITM\CMS\sqllib\
IBM Tivoli Monitoring 5.x Endpoint Support	ktm.sql	V620	C:\IBM\ITM\CMS\sqllib\
UNIX Logs Support	kul.sql	V620	C:\IBM\ITM\CMS\sqllib\
Universal Agent Support	kum.sql	V620	C:\IBM\ITM\CMS\sqllib\
UNIX OS Support	kux.sql	V620	C:\IBM\ITM\CMS\sqllib\

Figure 3-15 Adding application support

c. Click **Next** on the message that provides results for the process of adding application support. A return code of 0 (rc: 0) indicates that the process succeeded.

17. Configure the communication between any IBM Tivoli Monitoring V6.2 component and the monitoring server.

a. Specify the default values for IBM Tivoli Monitoring V6.2 components to use when they communicate with the monitoring server.

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

ii. Identify the type of protocol that the agents use to communicate with the hub monitoring server. Click **OK**.

b. Complete the communication protocol fields for the monitoring server.

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

19. Click **Finish** on the Maintenance Complete window, if you are updating an existing installation.

Installing a remote monitoring server on a Linux or UNIX server

To install a remote monitoring server, we use the same procedure as installing a hub monitoring server; the only difference occurs while configuring it. Table 3-4 on page 87 shows the steps for installing, configuring, and adding application support.

Table 3-4   Steps for installing a remote monitoring server on a Linux/UNIX server

Steps	Where to find information
Install the remote monitoring server. Use the same instructions as for installing the hub monitoring server.	"Installing the hub monitoring server on a Linux or UNIX server" on page 65
Configure the remote monitoring server.	"Configuring the remote monitoring server" on page 87
Add application support to the remote monitoring server. Use the same instructions as for adding application support to the hub monitoring server.	"Enabling application support on a Linux or UNIX server" on page 80

Note: IBM Tivoli Monitoring V6.2 does not support multiple monitoring servers (hub or remote) on the same computer.

Configuring the remote monitoring server

Use the following steps to configure the remote monitoring server:

1. At the command line, change to the /opt/IBM/ITM/bin directory (or the directory where you installed IBM Tivoli Monitoring V6.2).
2. Run the following command:

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

3. Type `remote` to indicate that this is remote hub monitoring server.
4. Press Enter to accept the default host name for the monitoring server. This should be the host name for your computer. If it is not, type the correct host name and then press Enter.
5. Enter the type of protocol to use for communication with the monitoring server. You have four choices: IP, IP.PIPE, IP.SPIPE, or SNA. Press Enter to use the default communications protocol (IP.PIPE).
6. If you want to set up a backup protocol, enter that protocol and press Enter. If you do not want to use a backup protocol, press Enter without specifying a protocol. In our case, we configured two protocols.
7. Depending on the type of protocol you specified, provide the correct information according to the information in Table 3-3 on page 75.
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, press Enter. If you do not want to use this feature, type n and press Enter.

11. Press Enter for the default Security Validation, it will accept no as the default.

    Example 3-12 shows the remote monitoring server configuration.

Example 3-12 Remote monitoring server configuration

```
[root@waco /]# itmcmd config -S -t REMOTE_WACO
Configuring TEMS...

Hub or Remote [1=*LOCAL, 2=*REMOTE] (Default is: 1): 2
Hub TEMS hostname (Default is: waco): server2

Network Protocol 1 [ip, sna, ip.pipe or ip.spipe] (Default is:
ip.pipe):

   Now choose the next protocol number from one of these:
     - ip
     - sna
     - ip.spipe
    - 0 for none
Network Protocol 2 (Default is: 0): ip

   Now choose the next protocol number from one of these:
     - sna
     - ip.spipe
    - 0 for none
Network Protocol 3(Default is: 0): ip.spipe
IP Port Number (Default is: 1918):
IP.PIPE Port Number (Default is: 1918):
Enter name of KDC_PARTITION (Default is: null):
Enter path and name of KDC_PARTITIONFILE (Default is:
/opt/IBM/ITM/tables/REMOTE_WACO/partition.txt):
IP.SPIPE Port Number (Default is: 3660):

Configuration Auditing? [1=YES, 2=NO] (Default is: 1):
Enter Optional Primary Network Name or type 0 for "none" :(Default
is: 0):

... Writing to database file for ms.

Hubs
##      CMS_Name
1       ip.pipe:REMOTE_WACO[1918]
```

```
1)Add, 2)Remove ##, 3)Modify Hub ##, 4)UserAccess ##, 5)Cancel,
6)Save/exit: 6
... creating config file
"/opt/IBM/ITM/config/waco_ms_REMOTE_WACO.config"
... creating file "/opt/IBM/ITM/tables/REMOTE_WACO/glb_site.txt."
... updating "/opt/IBM/ITM/config/kbbenv"
... verifying Hot Standby.
TEMS configuration completed...
```

After the configuration is finished, a configuration file is generated in the install_dir/config directory using the format <*host_name*>_ms_<*tems_name*>.config.

3.2.3 Installing the Tivoli Enterprise Portal Server

This section describes the steps for installing and configuring Tivoli Enterprise Portal Server on Windows, AIX, or Linux servers.

> **Note:** Tivoli Enterprise Portal Server requires a database to store information; please refer to 2.2.5, “Supported databases for Tivoli Enterprise Portal Server and Tivoli Data Warehouse” on page 37.

Installing the portal server on Windows server

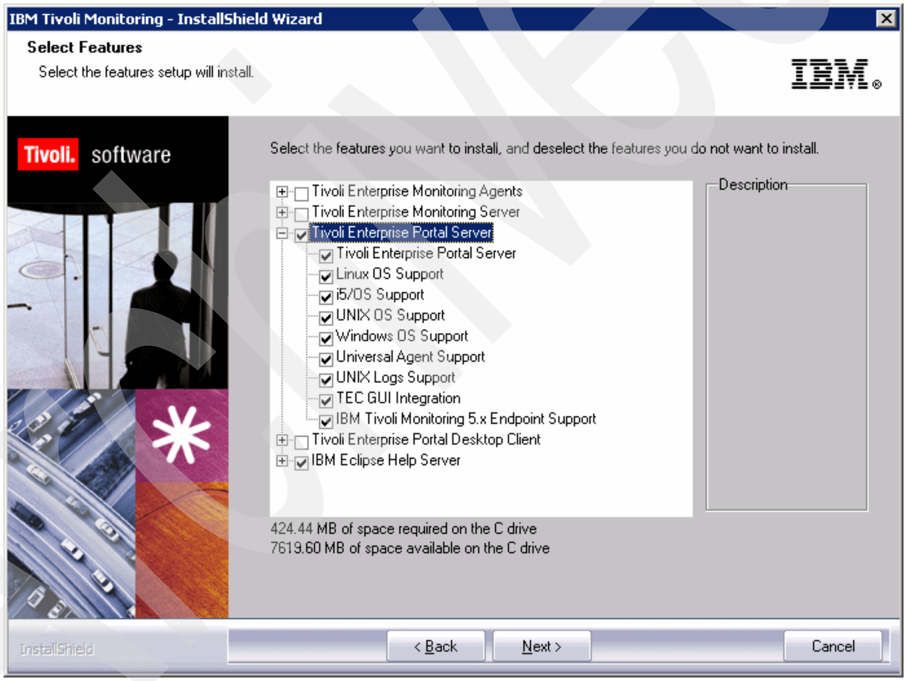
The installation procedure for a portal server on Windows includes steps for configuring the connection between the portal server and the following components:

- The hub monitoring server
- The portal server database
- The Tivoli Data Warehouse database

Complete the following steps to install the Tivoli Enterprise Portal Server and portal client on a Windows computer:

1. Launch the installation wizard by double-clicking the setup.exe file in the \WINDOWS subdirectory of the installation media.
2. Click **Next** in the Welcome window.
3. In the Install Prerequisites window, read the information about the required levels of IBM Global Security Toolkit (GSKit) and IBM Java.
4. Click **Next**. The prerequisite software is installed if necessary.
5. Read and accept the software license agreement by clicking **Accept**.

6. If you do not have an RDBMS (IBM DB2 or Microsoft SQL Server) installed on this computer, a message regarding potentially missing required software is displayed. Stop the installation, install the RDBMS, and begin the installation again.
7. Specify the directory where you want to install the portal server software and accompanying files. The default location is C:\IBM\ITM. Click **Next**.
8. Type an encryption key to use. This key should be the same as what was used during the installation of the hub monitoring server to which this portal server will connect. Click **Next** and then **OK** to confirm the encryption key.
9. In the Select Features window (Figure 3-16), select Tivoli Enterprise Portal Server from the list of components to install. Remember to leave the components under Tivoli Enterprise Portal Server selected; the support check boxes in the subtree are for installing application support files.



IBM Tivoli Monitoring - InstallShield Wizard

Select Features

Select the features setup will install.

Select the features you want to install, and deselect the features you do not want to install.

- □ Tivoli Enterprise Monitoring Agents
- □ Tivoli Enterprise Monitoring Server
- ☑ Tivoli Enterprise Portal Server
  - ☑ Tivoli Enterprise Portal Server
  - ☑ Linux OS Support
  - ☑ i5/OS Support
  - ☑ UNIX OS Support
  - ☑ Windows OS Support
  - ☑ Universal Agent Support
  - ☑ UNIX Logs Support
  - ☑ TEC GUI Integration
  - ☑ IBM Tivoli Monitoring 5.x Endpoint Support
- □ Tivoli Enterprise Portal Desktop Client
- ☑ IBM Eclipse Help Server

424.44 MB of space required on the C drive
7619.60 MB of space available on the C drive

Figure 3-16 Selecting features to install

> **Note:** The IBM Eclipse Help Server is automatically selected when you select the portal server.

10. *Optionally* select the following additional components to install:

   a. If you want to view events on the IBM Tivoli Enterprise Console event server through the Tivoli Enterprise Portal, expand **Tivoli Enterprise Portal Server** and ensure that **TEC GUI Integration** is selected.

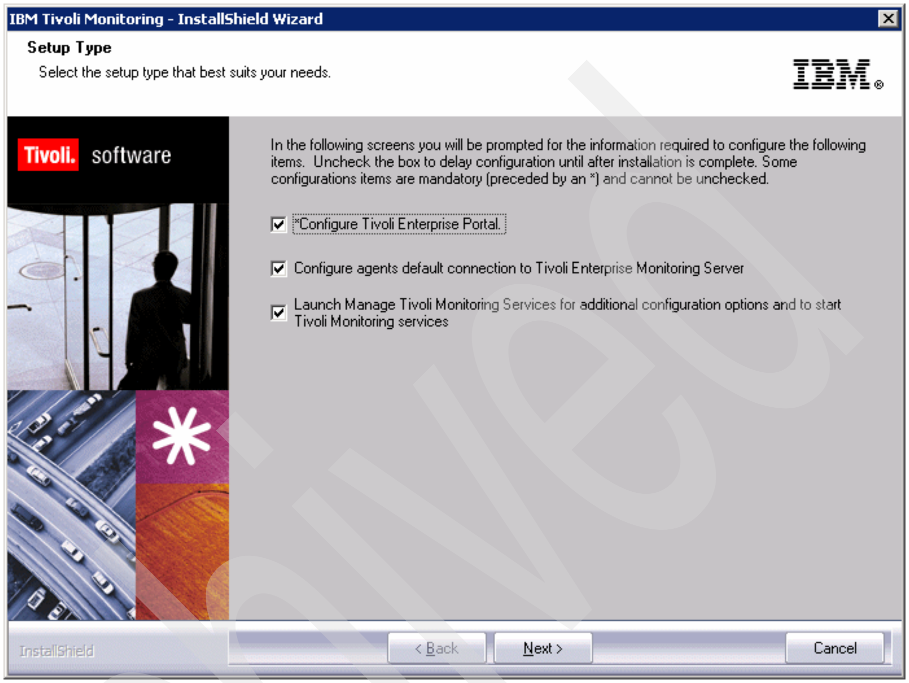
   b. If you want to install a portal desktop client on this computer, select **Tivoli Enterprise Portal Desktop Client**. When you select the Tivoli Enterprise Portal Desktop Client check box, all of the check boxes in the attached subtree are automatically selected. These check boxes are for installing application support files for base monitoring agents to the portal desktop client. Leave these check boxes selected as you did for the portal server in Step 9 on page 90.

11. Click **Next**.

12. If no IBM Tivoli Monitoring V6.2 component has been previously installed on this computer, a window is displayed for you to select a program folder for the Windows Start menu. Select a program folder and click **Next**. The default program folder name is IBM Tivoli Monitoring.

13. Review the installation summary details. The summary identifies what you are installing and where you chose to install it. Click **Next** to start the installation. After installation is complete, a configuration window (called the Setup Type window) is displayed.

14. Clear the check boxes for any components that have already been installed and configured (at the current release level) on this computer (Figure 3-17), unless you want to modify the configuration.



Setup Type

Select the setup type that best suits your needs.

In the following screens you will be prompted for the information required to configure the following items. Uncheck the box to delay configuration until after installation is complete. Some configurations items are mandatory (preceded by an *) and cannot be unchecked.

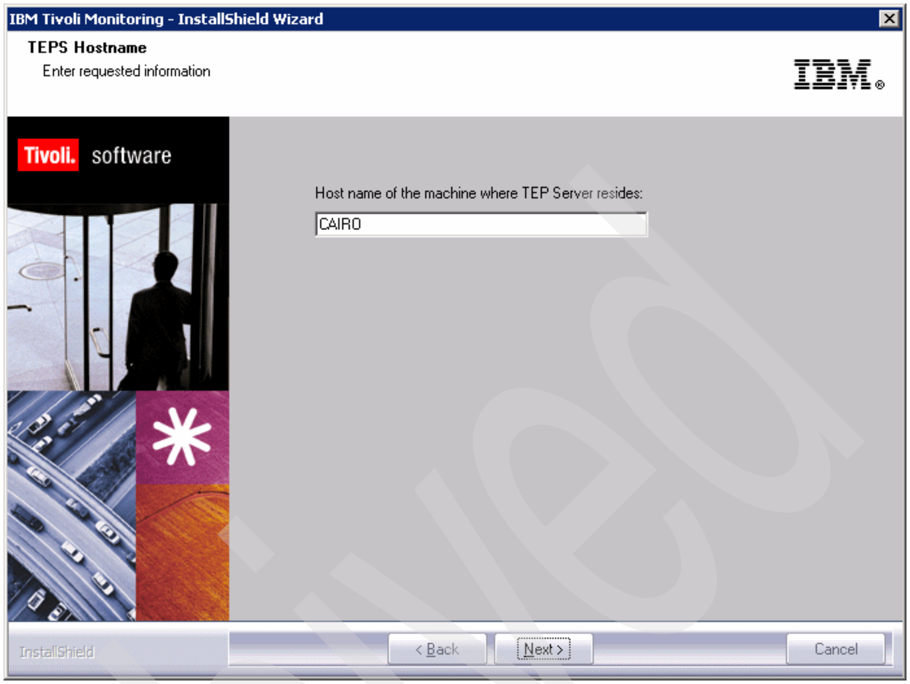
☑ *Configure Tivoli Enterprise Portal.

☑ Configure agents default connection to Tivoli Enterprise Monitoring Server

☑ Launch Manage Tivoli Monitoring Services for additional configuration options and to start Tivoli Monitoring services

Figure 3-17 Selecting components to configure

15. Type the host name of the computer where you are installing the portal server (Figure 3-18 on page 93). (The host name of this computer is displayed by default.) Click **Next**.



IBM Tivoli Monitoring - InstallShield Wizard

TEPS Hostname

Enter requested information

Host name of the machine where TEP Server resides: CAIRO

Figure 3-18 TEPS host name

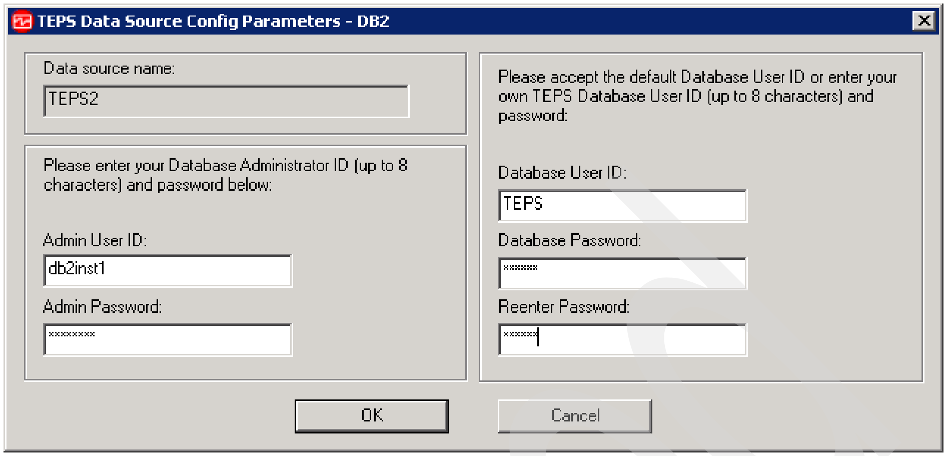
16. If more than one RDBMS product is installed on this computer, a window is displayed for you to choose the RDBMS product you want to use. Choose IBM DB2 or SQL Server and click **Next**.

17. A window is displayed for you (Figure 3-19 on page 94) to configure the connection between the portal server and the portal server database (TEPS database). The installation program uses the information in this window to automatically perform the following tasks:

    – Create the portal server database.

    – Create a database user for the portal server to use to access the database.

    – Configure the ODBC connection between the portal server and the database.



TEPS Data Source Config Parameters - DB2

Data source name: TEPS2

Please enter your Database Administrator ID (up to 8 characters) and password below:

Admin User ID: db2inst1

Admin Password: ********

Please accept the default Database User ID or enter your own TEPS Database User ID (up to 8 characters) and password:

Database User ID: TEPS

Database Password: ******

Reenter Password: ******

Figure 3-19   Configuration window for the portal server database using DB2

Use the information shown in Table 3-5 to complete the TEPS data source config parameters step.

Table 3-5   Configuration information for the portal server database

Field	DB2 default	MS SQL default	Description
Admin User ID	db2inst1	sa	The database administrator ID.
Admin Password	(no default)	(no default)	The password for the database administrator ID.
Database User ID	TEPS	cnps	The login name of the database user that portal server will use to access the database.
Database Password	(no default)	(no default)	The password for the database login user. If your environment requires complex passwords (passwords that require both alpha and numeric characters), specify a password that complies with these requirements.
Reenter password	(no default)	(no default)	

18. Click **OK** to complete the fields.

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

20. Click **Next** to accept the default Tivoli Data Warehouse user ID and password.

> **Note:** This is the warehouse user ID. The same ID and password must be used by all components connecting to the Tivoli Data Warehouse, including the Tivoli Enterprise Portal Server, Warehouse Proxy Agents, and the Summarization and Pruning Agent.

21. Configure the connection between the portal server and the hub Tivoli Enterprise Monitoring Server:

    a. Select the communications protocol that the monitoring server uses from the **Protocol** drop-down list. You can also specify whether the connection between the portal server and the hub monitoring server passes through a firewall. Click **OK**.

    b. Enter the host name or IP address and the port number for the hub monitoring server. Click **OK**.

22. A message is displayed asking if you want to re-configure the warehouse connection for the portal server. In our case, we will perform this step following the instructions in 3.4, “Tivoli Data Warehouse” on page 122.

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

Installing and configuring a portal server on a Linux or AIX server

This section describes the procedures to install and configure Tivoli Enterprise Portal Server and portal client on a Linux or AIX Server.

Before we perform the installation, we need to know some information about the user account used for the installation:

- Run these installation and configuration procedures as either the root user or as the DB2 administrator. If you are configuring the Tivoli Enterprise Portal Server using the DB2 administrator ID, then:
  - The configuration ID must be the same as the ID used to install the TEPS.
  - The configuration ID must be the same as the ID specified during the configuration dialog for the DB2 Admin ID.
  - The configuration ID must have the proper DB2 authority or rights to attach to the DB2 Instance Name specified during the configuration dialog.

  - The ID specified during the configuration dialog for the DB2 User ID must be an already existing ID. You may not allow the configuration dialog to attempt to create the user. For the GUI dialog, ensure that the check box for **Create the user** is unchecked. For the CLI dialog, ensure that the response for Create New User is NO. After you have installed and configured the portal server, you can use a different user to run the portal server, as long as that user has access to the binaries used by the portal server.

- GSKit *must* be installed from a user ID with root or administrator authority. If you are running the installer program interactively as non-root, the installer will prompt you for the root password. If you do not supply the root password when prompted or supply an invalid password, then GSKit must be installed manually from a user ID with root or administrator authority when the installation has completed. If you perform the installation using a silent installation as non-root, the prompt for the root password is bypassed, and GSKit must be installed manually from a user ID with root or administrator authority after the silent installation has completed.

In contrast to a Windows installation, installing Tivoli Enterprise Portal Server on Linux or AIX is performed in three steps, which are described in Table 3-6.

Table 3-6 Steps for installing a portal server on a Linux or AIX computer

Steps	Where to find information
Install the portal server.	“Installing the portal server on Linux or AIX” on page 96
Configure the portal server.	“Configuring the portal server on Linux or AIX” on page 98
Start the portal server	“Starting the portal server” on page 101

Installing the portal server on Linux or AIX

Complete the following steps to install the portal server:

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

   ```
   ./install.sh
   ```

2. When prompted for the IBM Tivoli Monitoring V6.2 home directory, press Enter to accept the default (/opt/IBM/ITM) or type the full path to a different directory.
3. If the installation directory does not already exist, you are asked if you want to create it. Type **y** to create this directory and press Enter.

4. The following prompt is displayed:

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

   Type 1 to start the installation and display the software license agreement.

5. Press Enter to read through the agreement.
6. Type 1 to accept the agreement and press Enter.
7. Enter a 32-character encryption key or press Enter to accept the default key. This key should be the one used during the installation of the monitoring server to which this portal server will connect. A numbered list of available operating systems is displayed.
8. Type the number for the operating system on which you are installing the portal server. The default value is your current operating system. Press Enter.
9. Type 1 to confirm the operating system and press Enter. A numbered list of products available for installation is displayed.
10. Type the number for Tivoli Enterprise Portal Server and press Enter. A message is displayed indicating that the Tivoli Enterprise Portal Server is about to be installed.

    > **Note:** The IBM Eclipse Help Server is automatically installed when you install the Tivoli Enterprise Portal.

11. Type 1 to confirm the installation. The installation begins.
12. After the Tivoli Enterprise Portal Server is installed, you are asked whether you want to install additional products or product support packages. Type 1 and press Enter. The installer presents a numbered list of products and application support packages.
13. Install the required application support packages.When you entered 1 in the preceding step, the installer presents a numbered list of items, including the following application support packages:

    ```
    Tivoli Enterprise Portal Browser Client support
    Tivoli Enterprise Portal Server support
    ```

> **Note:** The Tivoli Enterprise Portal Browser Client support package is portal server code that supports the browser clients. You must install the browser client support package on the computer where you install the portal server if you want to connect to it using a browser client.

Complete the following steps to install the portal server and browser client support packages for the base monitoring agents:

a. Type the number that corresponds to Tivoli Enterprise Portal Browser Client support and press Enter. A numbered list of base monitoring agents is displayed.

b. Type the numbers that correspond to the base monitoring agents for which you want to install the application support package, or type the number that corresponds to All of the above. Type the numbers on the same line separated by spaces or commas (,). Press Enter. It is best to select all of the base monitoring agents (All of the above) so you do not need to re-configure application support as new agent types are added to your environment.

c. Type 1 to confirm the installation and press Enter. The installation begins.

d. After the support package is installed, you are asked whether you want to install additional products or product support packages. Enter 1 and repeat the preceding steps for the Tivoli Enterprise Portal Server support package.

> **Note:** This step installs the application support files. However, you must enable the application support by configuring the portal server. The next two sections show you how to configure the portal server.

14. After you are finished installing the portal server and browser client packages, you are asked whether you want to install additional products or product support packages. Type 2 and press Enter.

Configuring the portal server on Linux or AIX

This section describes the steps to configure the portal server using the command-line procedure. For information how to configure a portal server using a GUI, refer to *IBM Tivoli Monitoring Version 6.2.0 Installation and Setup Guide,* GC32-9407. This configuration will perform the following tasks:

- Automatically enables application support on the portal server for the base monitoring agents.

- Includes steps for configuring the connection between the portal server and the following components:
  - The hub monitoring server
  - The portal server database
  - The Tivoli Data Warehouse database

> **Note:** Since we did not set up Tivoli Data Warehouse, we complete this procedure but accept the defaults at the prompts for configuring the connection to the data warehouse. We re-configure the connection in 3.4, “Tivoli Data Warehouse” on page 122.

Complete the following steps to configure the Tivoli Enterprise Portal Server from the command line on Linux or AIX:

1. Log on to the computer where the Tivoli Enterprise Portal Server is installed.
2. At the command line, change to the ITMinstall_dir/bin directory, where ITMinstall_dir is the directory where you installed the product.
3. Run the following command to start configuring the Tivoli Enterprise Portal Server:

   ```
   ./itmcmd config -A cq
   ```

   where cq is the product code for the portal server.
4. Edit the ITM Connector settings:
   a. Press Enter to accept the default for the following prompt:

      ```
      Edit 'ITM Connector' settings? [ 1=Yes, 2=No ] (default is: 1):
      ```

   b. Press Enter to enable the connector.

   c. Press Enter to accept the default name of ITM1 or type your preferred name and press Enter. This is the name that is to be displayed in the common event console for this connector.

   d. Press Enter to accept the default number of events (100) that are to be available in the common event console for this connector, or type the number of events you would like to see displayed and press Enter.

   e. Type 2 and press Enter to display only active events in the Common Event Console for this connector. Type 1 and press Enter to view both active and closed events. By default, only active events are displayed.

   f. Type 2 and press Enter to skip defining data for extra columns in the Common Event Console. When you define a Tivoli Enterprise Console or Tivoli Netcool/OMNIbus connector, you can define the information that is to be mapped to each of these customizable columns. See the *IBM Tivoli Monitoring Version 6.2.0 Administrator's Guide,* SC32-9408 for information about configuring these connectors.

5. Press Enter when you are asked if the agent connects to a monitoring server. (Although the prompt refers to an agent, this command is used to configure the portal server.)
6. Configure the connection between the portal server and the hub monitoring server:

   a. Type the host name for the hub monitoring server and press Enter.

   b. Type the protocol that the hub monitoring server uses to communicate with the portal server. You have four choices: IP.UDP, SNA, IP.PIPE, or IP.SPIPE.

   c. If you want to set up a backup protocol, enter that protocol and press Enter. If you do not want to use backup protocol, press Enter without specifying a protocol.

   d. Depending on the type of protocol you specified, provide information according to the information shown in Table 3-3 on page 75.

   e. Press Enter when you are asked if you want to configure the connection to a secondary monitoring server. The default value is none.

   f. Press Enter to accept the default for the Optional Primary Network Name (none).

   g. Press Enter to accept the default setting for SSL between the portal server and clients (N).

   > **Note:** By default, Secure Sockets Layer (SSL) is disabled. If you want enable it, type 1 and press Enter.

7. Configure the connection between the portal server and the portal server database:

   a. Type the DB2 instance name. The default value is db2inst1. Press Enter.

   b. Type the DB2 administrator ID. The default is db2inst1. Press Enter.

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

   c. Type the password for the DB2 administrator ID and press Enter.

   d. Confirm the password for the DB2 administrator ID by typing it again. Press Enter.

   e. Type the name of the portal server database. The default is TEPS. Press Enter.

   f. Type the login name of the database user that the portal server will use to access the database. The default is *itmuser*. Press Enter.

   g. Type the password for the database user and press Enter.

   h. Confirm the password for the database user by typing it again. Press Enter.

   i. You are asked if it is okay to create the DB2 login user if it does not exist. Type 1 and press Enter.

8. You are asked if you are using DB2 or Oracle for the Tivoli Data Warehouse. Enter D for DB2, J for Oracle JDBC™. DB2 is the default.
9. Since we are configuring the connection between the portal server and a DB2 warehouse database later, we do the following to finalize our installation:

   a. Press Enter to accept the DB2 default (even if you are going to create the Tivoli Data Warehouse using Oracle).

   b. Press Enter at all remaining prompts to accept the defaults.

You will see a message telling you that InstallPresentation is running, and then a message telling you that the installation has completed.

Starting the portal server

From the bin directory of /opt/IBM/ITM (or where you installed IBM Tivoli Monitoring V6.2), run the following command to start the portal server:

```
./itmcmd agent start cq
```

3.2.4 Installing the monitoring agents

This section describes how to install distributed monitoring agents. A distributed monitoring agent is one that is installed on a distributed (not z/OS) operating system. We also show an example of agent remote deployment.

To install a distributed monitoring agent, use the appropriate installation media:

- Use the IBM Tivoli Monitoring V6.2 base product CDs to install the monitoring agents in the following list. These are the same product CDs that you use to install the monitoring servers, portal server, and portal desktop clients. The monitoring agents included on these CDs are called base monitoring agents:
  - ITM 5.x Endpoint
  - Linux OS
  - UNIX Logs
  - UNIX OS
  - Universal Agent
  - Warehouse Proxy
  - Warehouse Summarization and Pruning
  - Windows OS

  There are several IBM Tivoli Monitoring V6.2 base product CDs, organized according to operating system. To install a monitoring agent, use the product CD appropriate to the operating system. For example, install a Linux OS monitoring agent from the IBM Tivoli Monitoring base CD for Linux.
- Use the agent product CDs to install distributed monitoring agents that are delivered separately from the IBM Tivoli Monitoring base installation package. For example, use the IBM Tivoli Monitoring for Databases product CDs to install a monitoring agent for DB2 or Oracle. Depending on the agent that you are installing, there might be additional configuration steps required. See the agent documentation for more information.

All monitoring agents require that agent-specific application support be installed on the monitoring servers, portal server, and portal desktop clients.

The following sections provide instructions for installing a monitoring agent:

- “Installing a monitoring agent on a Windows server” on page 102
- “Installing a monitoring agent on Linux or UNIX server” on page 108

Installing a monitoring agent on a Windows server

Use the following steps to install a distributed monitoring agent on a Windows computer:

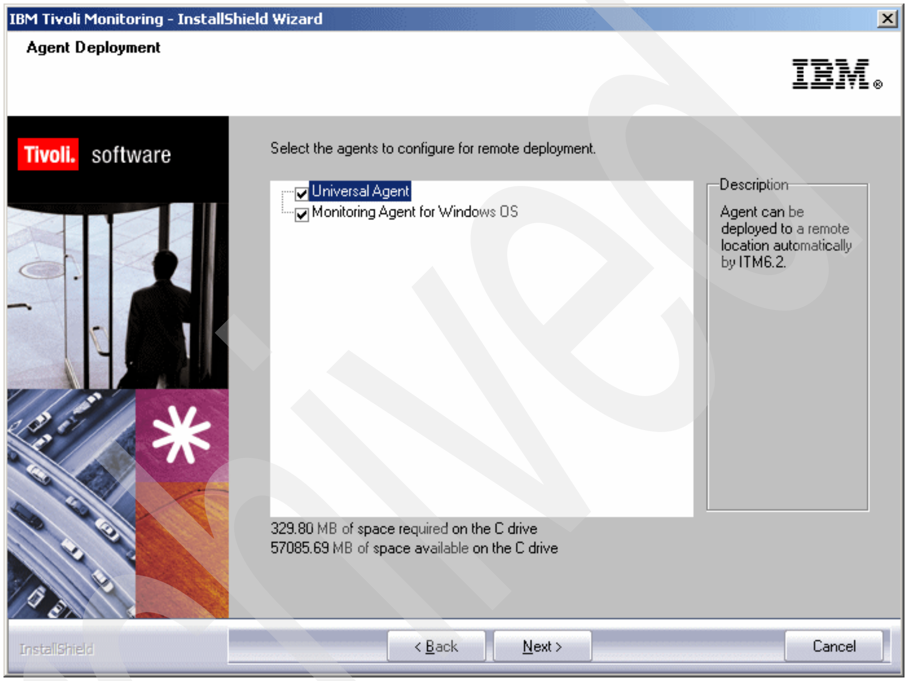
1. Launch the installation wizard by double-clicking the setup.exe file in the \WINDOWS subdirectory on the installation media. Use either an IBM Tivoli Monitoring V6.2 base product CD for Windows or a distributed agent product CD for Windows.

2. Click **Next** on the Welcome window.

> **Note:** If you have another IBM Tivoli Monitoring V6.2 component already installed on this computer, select **Modify** on the Welcome window to indicate that you are updating an existing installation. Click **OK** on the message telling you about preselected items. Then skip to Step 9.

3. On the Install Prerequisites window, read the information about the required levels of IBM Global Security Toolkit (GSKit) and IBM Java.
4. Click **Next**. The prerequisite software is installed if necessary.
5. Read and accept the software license agreement by clicking **Accept**.
6. If you do not have a database (DB2 or MS SQL) installed on this computer, a message regarding potentially missing software is displayed. You do *not* need a database to install a management agent on this computer, so you can click **Next** and ignore this message.
7. Choose the directory where you want to install the product. Click **Next**.
8. Type a 32-character encryption key. This key should be the same as the key that was used during the installation of the monitoring server to which this monitoring agent connects. Click **Next** and then click **OK** to confirm the encryption key.
9. On the Select Features window, expand **Tivoli Enterprise Monitoring Agents**.
10. Select the names of the agents that you want to install and click **Next**.

11. If a monitoring server is not installed on this computer, go to Step 12. If you are installing monitoring agents on a computer that already has a monitoring server installed, the Agent Deployment window is displayed (Figure 3-20). Select the agents, if any, that you want to add to the agent depot. (You can add agents to the agent depot at a later time by updating your installation.) Click **Next**.



IBM Tivoli Monitoring - InstallShield Wizard

Agent Deployment

Select the agents to configure for remote deployment.

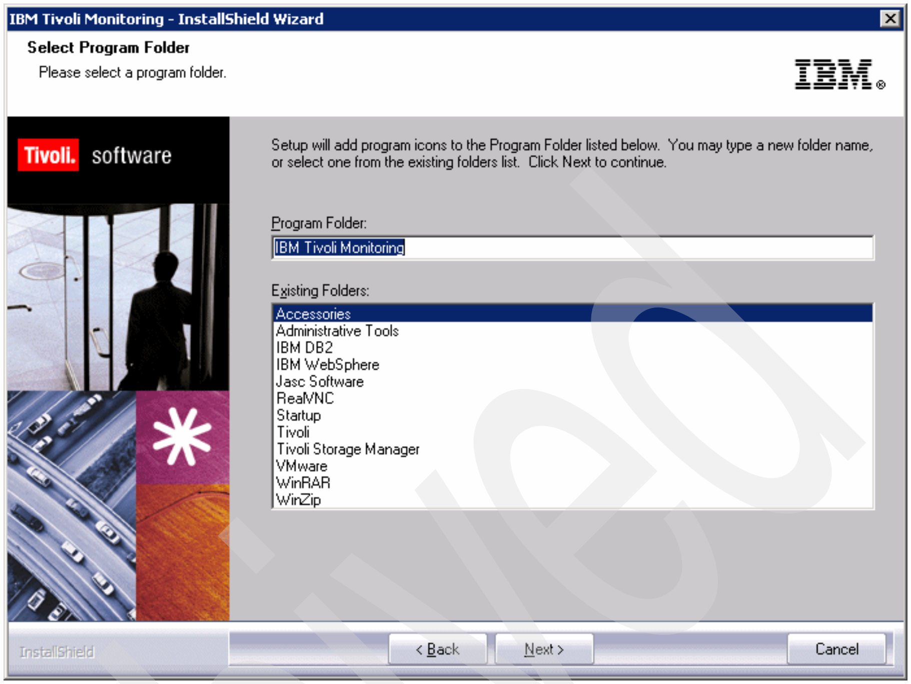
☑ Universal Agent
☑ Monitoring Agent for Windows OS

Description
Agent can be deployed to a remote location automatically by ITM6.2.

329.80 MB of space required on the C drive
57085.69 MB of space available on the C drive

Figure 3-20 Agent Deployment

12. This step applies only to agents that you install from the IBM Tivoli Monitoring installation image. If you are installing agents from an agent product installation image, go to Step 13 on page 105. If no IBM Tivoli Monitoring component has been previously installed on this computer, a window is displayed for you to select a program folder for the Windows Start menu. Select a program folder (Figure 3-21 on page 105) and click **Next**. The default program folder name is IBM Tivoli Monitoring.



IBM Tivoli Monitoring - InstallShield Wizard

Select Program Folder

Please select a program folder.

Setup will add program icons to the Program Folder listed below. You may type a new folder name, or select one from the existing folders list. Click Next to continue.

Program Folder:

IBM Tivoli Monitoring

Existing Folders:

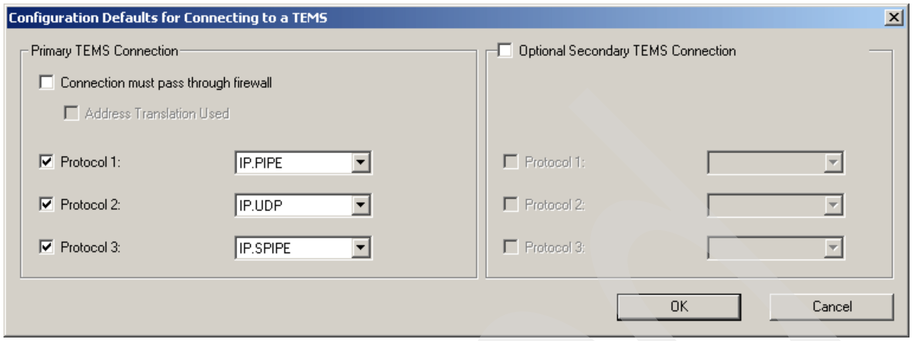
Accessories
Administrative Tools
IBM DB2
IBM WebSphere
Jasc Software
RealVNC
Startup
Tivoli
Tivoli Storage Manager
VMware
WinRAR
WinZip

Figure 3-21 Program folder

13. Review the installation summary details. The summary identifies what you are installing and where you chose to install it. Click **Next** to start the installation. After installation is complete, a configuration window (called the Setup Type window) is displayed.

14. Clear the check boxes for any components that have already been installed and configured (at the current release level) on this computer, unless you want to modify the configuration. (For example, clear the check box for the Tivoli Enterprise Monitoring Server if it has already been installed and configured on this computer.) Click **Next** to start configuring all selected components.

15. Define the communications between the monitoring agents and the monitoring server, as shown in Figure 3-22.



Configuration Defaults for Connecting to a TEMS

Primary TEMS Connection

□ Connection must pass through firewall

□ Address Translation Used

☑ Protocol 1: IP.PIPE

☑ Protocol 2: IP.UDP

☑ Protocol 3: IP.SPIPE

□ Optional Secondary TEMS Connection

□ Protocol 1:

□ Protocol 2:

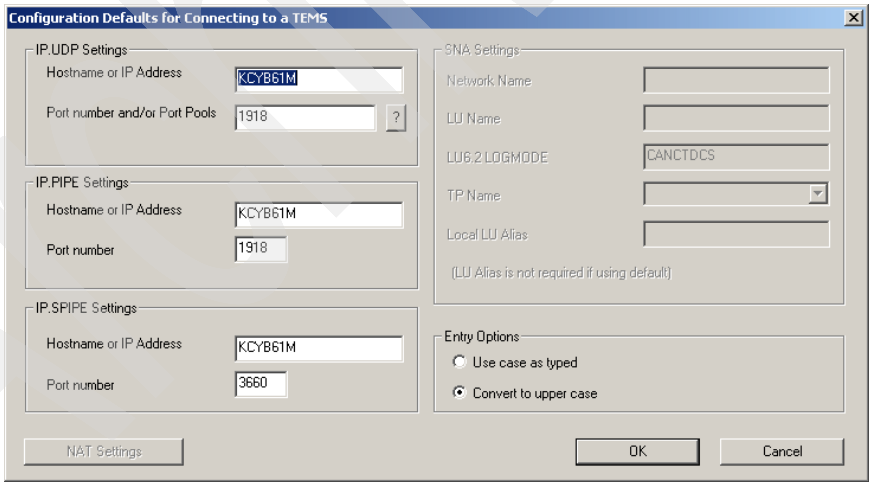
□ Protocol 3:

Figure 3-22 Communications configuration

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

b. Identify the type of protocol that the agents use to communicate with the monitoring server.

c. Click **OK**. A second configuration window is displayed.



Configuration Defaults for Connecting to a TEMS

IP.UDP Settings

Hostname or IP Address: KCYB61M

Port number and/or Port Pools: 1918 ?

IP.PIPE Settings

Hostname or IP Address: KCYB61M

Port number: 1918

IP.SPIPE Settings

Hostname or IP Address: KCYB61M

Port number: 3660

SNA Settings

Network Name:

LU Name:

LU6.2 LOGMODE: CANCTDCS

TP Name:

Local LU Alias:

(LU Alias is not required if using default)

Entry Options

○ Use case as typed

● Convert to upper case

Figure 3-23 Protocols configuration

d. Complete the fields for the communications protocol for the monitoring server. Use Table 3-2 on page 62 as a reference.

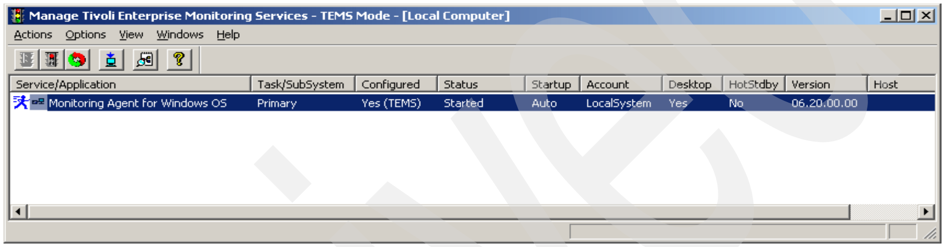
e. Click **OK** to exit the Configuration Defaults for Connecting to a TEMS window.

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

17. Click **Finish** on the Maintenance Complete window if you are updating an existing installation.

18. Open the Manage Tivoli Monitoring Services utility (if it does not open automatically) to see if the monitoring agents that you installed have been configured and started.

Note: If Yes is displayed in the Configured column, the agent has been configured and started during the installation process.



Manage Tivoli Enterprise Monitoring Services - TEMS Mode - [Local Computer]
Actions Options View Windows Help

Service/Application	Task/SubSystem	Configured	Status	Startup	Account	Desktop	HotStdby	Version	Host
Monitoring Agent for Windows OS	Primary	Yes (TEMS)	Started	Auto	LocalSystem	Yes	No	06.20.00.00	

Figure 3-24 Manage Tivoli Enterprise Monitoring Services

19. If the value in the Configured column is blank and Template is displayed in the Task/Subsystem column, right-click the Template agent and complete the following steps:

    a. Click **Configure Using Defaults**.

    b. Complete any windows requiring information by using the agent-specific configuration settings in the user's guide for your agent.

    Note: Do not enter non-ASCII characters on any of these windows. Entering characters from other character sets has unpredictable results.

    c. Repeat this step as necessary to create monitoring agent instances for each application instance you want to monitor.

Installing a monitoring agent on Linux or UNIX server

Like in Enterprise Server and Portal Server installation, we install Monitoring Agent using the steps described in Table 3-7.

Table 3-7 Steps for installing a monitoring agent on Linux or UNIX

Steps	Where to find information
Install the monitoring agent.	"Installing the monitoring agent on a Linux or UNIX server" on page 108
Configure the monitoring agent.	"Configuring the monitoring agent on a Linux or UNIX server" on page 109
Change the file permissions for files on the computer where you installed the agent.	"Changing the file permissions for agents on a Linux or UNIX server" on page 110
Start the monitoring agent.	"Starting the monitoring agents" on page 111

Installing the monitoring agent on a Linux or UNIX server

Use the following steps to install a monitoring agent on a Linux or UNIX computer:

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

   ```
   ./install.sh
   ```

2. When prompted for the IBM Tivoli Monitoring V6.2 home directory, press Enter to accept the default (/opt/IBM/ITM) or type the full path to a different directory.
3. If the installation directory does not already exist, you are asked if you want to create it. Type y to create this directory and press Enter.
4. The following prompt is displayed:

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

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

   Type 1 to start the installation and display the software license agreement.

5. Press Enter to read through the agreement.
6. Type 1 to accept the agreement and press Enter.
7. Enter a 32-character encryption key or press Enter to accept the default key. This key should be the one used during the installation of the monitoring server to which this portal server will connect. A numbered list of available operating systems is displayed.
8. Type the number for the operating system on which you are installing the monitoring agents. The default value is your current operating system. Press Enter.
9. Type 1 to confirm the operating system and press Enter. A numbered list of products available for installation is displayed.
10. Type the number that corresponds to the monitoring agent or agents that you want to install. If you want to install more than one agent, use a comma (,) or a space to separate the numbers for each agent. Press Enter.

    Note: Before you install the Warehouse Proxy agent or Summarization and Pruning agent, follow the instructions in 3.4, “Tivoli Data Warehouse” on page 122 to set up a Tivoli Data Warehouse solution.

11. Type 1 to confirm the installation. The installation begins.
12. After all of the components are installed, you are asked whether you want to install additional products or product support packages. Type 2 and press Enter**.**

Continue with “Configuring the monitoring agent on a Linux or UNIX server” on page 109; after configuring, we might need change permissions and finally start the agent.

Configuring the monitoring agent on a Linux or UNIX server

Use the following steps to configure your monitoring agent:

1. Run the following command:

   ```
   ./itmcmd config -A pc
   ```

   where pc is the product code for your agent. For the UNIX agent, use the product code ux; for Linux, use lz. See Appendix D, “IBM Tivoli Product Codes”, in *IBM Tivoli Monitoring Version 6.2.0 Installation and Setup Guide,* GC32-9407*,* for more information about agent product codes.
2. Press Enter when you are asked if the agent connects to a monitoring server.
3. Type the host name for the monitoring server.

4. Type the protocol that you want to use to communicate with the monitoring server. You have four choices: IP, SNA, IP.SPIPE, or IP.PIPE. Press Enter to accept the default protocol (IP.PIPE).
5. If you want to set up a backup protocol, enter that protocol and press Enter. If you do not want to use a backup protocol, press Enter without specifying a protocol.
6. Depending on the type of protocol you specified, use Table 3-3 on page 75 to provide the information needed.
7. Press Enter to not specify the name of the KDC_PARTITION.
8. Press Enter when you are asked if you want to configure the connection to a secondary monitoring server. The default value is no.
9. Press Enter to accept the default for the Optional Primary Network Name (none).

> **Note:** When we install the Warehouse Proxy agent, we need to complete the configuration using the Manage Tivoli Monitoring Services graphical user interface (GUI), which requires an X11 GUI interface. You can find more information about this topic in the *IBM Tivoli Monitoring Version 6.2.0 Installation and Setup Guide,* GC32-9407.

Changing the file permissions for agents on a Linux or UNIX server

If you used a non-root user to install a monitoring agent on a UNIX computer, the file permissions are initially set to a low level. Run the following procedure to change these file permissions:

1. Log in to the computer as root, or become the root user by running the **su** command.
2. Create a new group (such as "itmusers") to own all of the files in the IBM Tivoli Monitoring installation directory.

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

   ```
   groupadd itmusers
   ```

   For an AIX computer, run the following command:

   ```
   mkgroup itmusers
   ```

3. Run the following command to ensure that the CANDLEHOME environment variable correctly identifies IBM Tivoli Monitoring V6.2 installation directory:

   ```
   echo $CANDLEHOME
   ```

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

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

   ```
   cd $CANDLEHOME
   ```

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

   ```
   pwd
   ```

6. Run the following commands:

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

7. Run the following command to change the ownership of additional agent files:

   ```
   bin/SetPerm
   ```

8. If you want to run the agent as a particular user, add the user to the itmusers group. To do this, edit the /etc/group file and ensure that the user is in the list of users for the itmusers group.

   For example, if you want to run the agent as user test1, ensure that the following line is in the /etc/group file:

   ```
   itmusers:x:504:test1
   ```

9. Run the **su** command to switch to the user that you want to run the agent as or log in as that user.

Starting the monitoring agents

You can either start all agents running on a computer or start individual agents by using the product codes. To start all monitoring agents, run the following command:

```
./itmcmd agent start all
```

To start specific agents, run the following command:

```
./itmcmd agent start pc pc pc
```

where pc is the product code for the agent that you want to start.

3.2.5 Installing the Tivoli Enterprise Portal desktop client

There are two methods of deploying the desktop client. You can install the desktop client from the installation media and run and maintain it on the local system. You can also use IBM Web Start for Java to download and run the desktop client from the Tivoli Enterprise Portal Server.

This section describes how to install the desktop client from the installation media on Windows and Linux computers. When you install the desktop client from the installation media, you must also install support for all the applications that you will be using.

Installing the desktop client on Windows

Complete the following steps to install the Tivoli Enterprise Portal desktop client from the IBM Tivoli Monitoring installation media for Windows:

1. On the computer where you want to install the desktop client, start the installation wizard by launching the `setup.exe` file in the \WINDOWS subdirectory on the installation media.
2. Click **Next** on the Welcome window.

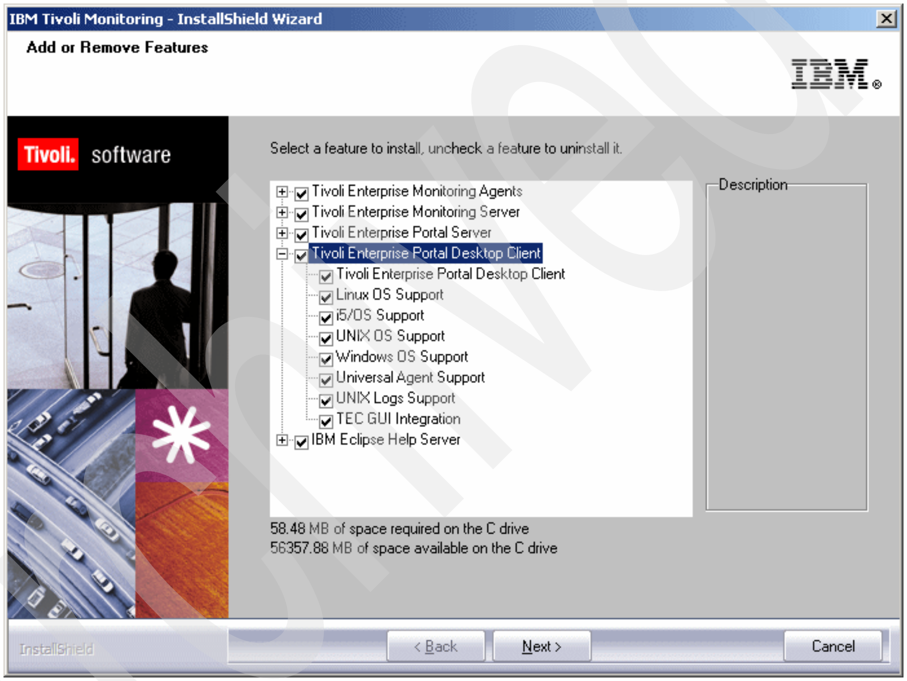
> **Note:** If you have another IBM Tivoli Monitoring component already installed on this computer, select **Modify** on the Welcome window to indicate that you are updating an existing installation. Click **OK** on the message telling you about preselected items. Then skip to Step 8.

3. In the Install Prerequisites window, read the information about the required levels of IBM Global Security Toolkit (GSKit) and IBM Java.
4. Click **Next**. The prerequisite software is installed if necessary.
5. Read and accept the software license agreement by clicking **Accept**.
6. Specify the directory where you want to install the portal desktop client software and accompanying files. The default location is C:\IBM\ITM. Click **Next**.
7. Type an encryption key to use. This key should be the same as what was used during the installation of the hub monitoring server to which the client will connect. Click **Next** and then **OK** to confirm the encryption key.
8. In the Select Features window, select **Tivoli Enterprise Portal Desktop Client** from the list of components to install.

   When you select the Tivoli Enterprise Portal Desktop Client check box, all of the check boxes in the attached subtree are automatically selected. The support check boxes in the subtree are for installing application support files for base monitoring agents to the portal desktop client. (The base monitoring agents are included with the base IBM Tivoli Monitoring installation package.) It is best to leave all of the support check boxes selected so you do not need to re-configure application support as new agent types are added to your environment.

> **Note:** If you are updating an existing installation (you selected **Modify** on the Welcome window), all the check boxes on the Select Features window reflect your choices during the initial installation. Clearing a check box has the effect of uninstalling the component. Clear a check box only if you want to remove a component.

9. If you want to view IBM Tivoli Enterprise Console events through the Tivoli Enterprise Portal, expand **Tivoli Enterprise Portal Desktop Client** and ensure that TEC GUI Integration is selected (Figure 3-25).



IBM Tivoli Monitoring - InstallShield Wizard

Add or Remove Features

Select a feature to install, uncheck a feature to uninstall it.

- ☑ Tivoli Enterprise Monitoring Agents
- ☑ Tivoli Enterprise Monitoring Server
- ☑ Tivoli Enterprise Portal Server
- ☑ Tivoli Enterprise Portal Desktop Client
  - ☑ Tivoli Enterprise Portal Desktop Client
  - ☑ Linux OS Support
  - ☑ i5/OS Support
  - ☑ UNIX OS Support
  - ☑ Windows OS Support
  - ☑ Universal Agent Support
  - ☑ UNIX Logs Support
  - ☑ TEC GUI Integration
- ☑ IBM Eclipse Help Server

Description

58.48 MB of space required on the C drive
56357.88 MB of space available on the C drive

Figure 3-25 Add or remove features

10. Click **Next**.

11. If a monitoring server is not installed on this computer, go to Step 12. If you are installing the desktop client on a computer that already has a monitoring server installed, the Agent Deployment window is displayed. The Agent Deployment window lists monitoring agents on this installation image that you can add to the agent depot. The agent depot contains agent bundles that you can deploy to remote computers. Click **Next**.

12. If no IBM Tivoli Monitoring component has been previously installed on this computer, a window is displayed for you to select a program folder for the Windows Start menu. Select a program folder and click **Next**. The default program folder name is IBM Tivoli Monitoring.
13. Review the installation summary details. The summary identifies what you are installing and where you chose to install it. Click **Next** to start the installation. After installation is complete, a configuration window (called the Setup Type window) is displayed.
14. Clear the check boxes for any components that have already been installed and configured (at the current release level) on this computer, unless you want to modify the configuration. (For example, clear the check box for the Tivoli Enterprise Monitoring Server if it has already been installed and configured on this computer.) Click **Next** to start configuring all selected components.
15. Type the host name of the portal server and click **OK**.
16. Click **Finish** to complete the installation.

Installing the desktop client on Linux

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

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

   ```
   ./install.sh
   ```

2. When prompted for the IBM Tivoli Monitoring home directory, press Enter to accept the default (/opt/IBM/ITM) or type the full path to a different directory.
3. If the installation directory does not already exist, you are asked if you want to create it. Type 1 to create this directory and press Enter.
4. The following prompt is displayed:

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

   Type 1 to start the installation and display the software license agreement.

5. Press Enter to read through the agreement.
6. Type 1 to accept the agreement and press Enter.

7. Type an 32-character encryption key to use and press Enter. This key should be the same key as that used during the installation of the portal server to which the client will connect. A numbered list of available operating systems is displayed.

8. Type the number for the operating system on which you are installing the desktop client. The default value is your current operating system. Press Enter.

9. Type 1 to confirm the operating system and press Enter. A numbered list of available components is displayed.

10. Type the number for Tivoli Enterprise Portal Desktop Client and press Enter. A message is displayed indicating that the Tivoli Enterprise Portal Desktop Client is about to be installed.

11. Type 1 to confirm the installation. The installation begins.

12. After the portal desktop client is installed, you are asked whether you want to install additional products or product support packages. Type 1 and press Enter. A numbered list is displayed, including the following application support package: Tivoli Enterprise Portal Desktop Client support.

13. Install the application support package for the portal desktop client. All monitoring agents require that application support files be installed on the monitoring servers (hub and remote), portal server, and portal desktop clients in your environment. Application support files contain the information required for agent-specific workspaces, helps, predefined situations, and other data. This step installs the application support files for base monitoring agents. The base monitoring agents are included with the base IBM Tivoli Monitoring installation package.

    a. Type the number that corresponds to Tivoli Enterprise Portal Desktop Client support and press Enter. A numbered list of base monitoring agents is displayed.

    b. Type the numbers of the base monitoring agents for which you want to install application support, or type the number that corresponds to All of the above. Type the numbers on the same line separated by spaces or commas. Press Enter. It is best to select all of the base monitoring agents (All of the above) so you do not need to re-configure application support as new agent types are added to your environment.

    c. Type 1 to confirm the installation and press Enter.

       The installation begins.

> **Note:** This step installs the application support files. However, you must enable the application support by configuring the portal desktop client. The next sections shows you how to configure the portal desktop client.

14. After application support for the monitoring agents is installed, you are asked whether you want to install additional products or product support packages. Type 2 and press Enter.

The next step is to configure the desktop client.

Configuring the desktop client on Linux

Complete the following steps to configure the desktop client if you installed the client from the IBM Tivoli Monitoring installation media. You do not need to complete this procedure if you obtained the desktop client by using IBM Web Start for Java to download it from the Tivoli Enterprise Portal Server.

1. At the command line, go to /opt/IBM/ITM/bin directory (or the /bin subdirectory where you installed the product).
2. Run the following command:

   ```
   ./itmcmd config -A cj
   ```

3. Press Enter to use the default instance name.
4. Type the host name for the portal server and press Enter.
5. Press Enter when you are asked if you want to use HTTP Proxy support. The default value is no.
6. Start the desktop client:

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

3.3 Remote agent deployment

Note: Remote deployment of agents is covered in detail in Chapter 7, “Deploying IBM Tivoli Monitoring agents in a large scale environment” in *IBM Tivoli Monitoring: Implementation and Performance Optimization for Large Scale Environments*, SG24-7443. Please refer to this book for more information about this topic.

IBM Tivoli Monitoring provides the ability to deploy monitoring agents from a central location: the monitoring server. We can deploy the OS agent using **`tacmd createNode`** or non OS agent using **`tacmd addSystem`**.

Before we deploy the agent, we need populate the agent depot, which is an installation directory on the monitoring server with agents and maintenance packages images.

Any agent installation image with prerequisites is called a *bundle*. When we add a bundle to the agent depot, we need to add the bundle that supports the operating system that we want to deploy.

Table 3-8 describes the steps required to set up and manage remote agent deployment.

Table 3-8 Remote agent deployment steps

Steps	Where to find information
Populate the agent deploy depot with installable agent images.	3.3.1, "Populating the agent depot for OS agents" on page 117
Deploy an OS agent.	3.3.2, "Deploying OS agents" on page 119
Deploy a non-OS agent.	3.3.3, "Deploying non-OS agents" on page 121

3.3.1 Populating the agent depot for OS agents

There are two methods to populate the agent depot:

- "Populating the agent depot from the installation image" on page 117
- "Populating the agent depot with the tacmd addBundles command" on page 119

Populating the agent depot from the installation image

This section describes how to populate the agent depot on Windows, Linux, and UNIX using the installation image.

Populating the agent depot during installation on Windows

The procedure to populate the agent depot from the Windows installation image differs based on the installation image (base IBM Tivoli Monitoring or application agent) that you are using. Use the procedure below that applies to the image you are using:

1. Launch the installation wizard by double-clicking the setup.exe file in the \Windows subdirectory of the installation image.
2. Select **Modify** on the Welcome window and click **Next**.
3. Click **OK** for the warning message regarding existing components on this computer.
4. Click **OK** on the Add or Remove Features window without making any changes. (Do not clear any selected items because this removes them from the computer.)

5. On the Agent Deployment window, select the agents that you want to add to the depot and click **Next**.
6. Review the installation summary and click **Next** to begin the installation. After the agents are added to the agent depot, a configuration window (called the Setup Type window) is displayed.
7. Clear all selected components. You have already configured all components on this computer and do not need to reconfigure any now. Click **Next**.
8. Click **Finish** to complete the installation.
9. Click **Finish** in the Maintenance Complete window.

Populating the agent depot during installation on Linux or UNIX

Use the following steps to populate the agent depot from the Linux or UNIX installation image:

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

   ```
   ./install.sh
   ```

2. When prompted for the IBM Tivoli Monitoring home directory, press Enter to accept the default (/opt/IBM/ITM). If you want to use a different installation directory, type the full path to that directory and press Enter.
3. If the directory you specified does not exist, you are asked whether to create it. Type y to create this directory.
4. The following prompt is displayed. Select one of the following:

   ```
   1) Install products to the local host.
   2) Install products to depot for remote deployment (requires TEMS).
   3) Install TEMS support for remote seeding
   4) Exit install.
   Please enter a valid number:
   ```

   Type 2 to start the installation and press Enter. The end user license agreement is displayed. Press Enter to read through the agreement.
5. Type 1 to accept the agreement and press Enter.
6. Type the number that corresponds to the agent or agents that you want to add to the agent depot and press Enter. If you are going to add more than one agent, use a comma (,) to separate the numbers. To select all available agents, type all. You can select multiple agents with consecutive corresponding numbers by typing the first and last numbers for the agents, separated by a hyphen (-).
7. When you have specified all the agents that you want to add to the agent depot, type E and press Enter to exit.

Populating the agent depot with the tacmd addBundles command

To populate the agent depot using the **tacmd addBundles** command, run the following command:

```
tacmd addBundles [-i IMAGE_PATH] [-t PRODUCT_CODE] [-p
OPERATING_SYSTEM] [-v VERSION] [-n] [-f]
```

For the full syntax, including parameter descriptions, refer to *IBM Tivoli Monitoring Version 6.2.0 Command Reference,* SC23-6045.

3.3.2 Deploying OS agents

> **Note:** Remote deployment of agents is covered in detail in Chapter 7, "Deploying IBM Tivoli Monitoring agents in a large scale environment", in *IBM Tivoli Monitoring: Implementation and Performance Optimization for Large Scale Environments*, SG24-7443. You can refer to this document for more information.

You can install the OS agent locally or remotely using the **tacmd createNode** command. The **tacmd createNode** command creates a directory on the target computer called the *node*. This is the directory into which not only the OS agent is installed, but where any non-OS agents are deployed. The **tacmd createNode** command uses one of the following protocols to connect to the computers on which you want to install the OS agent:

- Server Message Block (SMB), used primarily for Windows servers
- Secure Shell (SSH), used primarily by UNIX servers, but also available on Windows

  > **Note:** Only SSH version 2 is supported.

- Remote Execution (REXEC), used primarily by UNIX servers, but not very secure
- Remote Shell (RSH), used primarily by UNIX servers, but not very secure

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

Requirements for the tacmd createNode command

Before you can use the **`tacmd createNode`** command to deploy OS agents, ensure that the following is true:

- The user ID that you are going to use during the deployment has administrative privileges on the target computer.
- Any computer to which you want to deploy the OS agent must have a supported protocol installed.
- Security in your environment should be configured to permit createNode to pass through the firewall, using the protocol that you specify in the command parameters.
- On Windows computers:
  - SMB requires that the default, hidden, and administrative shares are available on the drive being accessed and on the drive that hosts the System temporary directory.
  - SMB signing is not supported when connecting using SMB. The computer to which you are deploying an OS agent cannot require SMB signing. For Windows XP, disable Simple File Sharing. Simple File Sharing requires that all users authenticate with guest privileges. This is not supported for createNode.
  - For Windows XP computers with Service Pack 2, disable the Internet Connection Firewall.
  - For Windows XP computers, set Network Access Sharing and Security to **Classic - local users authenticate as themselves**.
  - For all Windows computers, enable remote registry administration. (This is enabled by default.)
- On UNIX systems, if you are using the RSH protocol, run the **`tacmd createNode`** command as root on the monitoring server.
- If you are deploying the OS agent to a UNIX or Linux computer, that computer must have either the ksh or bash shell.
- If you are using SSH V2 (for either Windows or UNIX), configure SSH on the target computers to permit the use of password authentication.

> **Note:** If you are using private key authentication in your environment, you do not need to set SSH to permit password authentication.

Using the tacmd createNode command

To deploy an OS agent using the **`tacmd createNode`** command, run the following command:

```
tacmd createNode [-h HOST_NAME] [{smb|ssh|rexec|rsh}://]HOST[:PORT]]
[-u USERNAME] [-w PASSWORD][-o NAME=VALUE ...] [-d NODEDIR] [-i
IMAGE_PATH] [-p NAME=VALUE ...] [-f]
```

Before we install the OS agent from the command line using **`tacmd createNode`**, we need to check the agent install packages depot. Use **`tacmd listBundles`** to check the depot.

Example 3-13 shows an example of UNIX agent remote deployment.

Example 3-13 Remote agent deployment

```
[root@server2][/]-> tacmd createnode -h paris -u root -p
PROTOCOL=IP.PIPE PROTOCOL2=IP.UDP SERVER=athens
KUICCN001I Initializing required services...
KUICCN005I Enter the password for root.

KUICCN039I Attempting to connect to host paris ...
KUICCN050I Distributing file 13 of 69 (28 MB / 157.1 MB)...

[root@server2][/]-> tacmd createnode -h paris -u root -p
PROTOCOL=IP.PIPE PROTOCOL2=IP.UDP SERVER=athens
KUICCN001I Initializing required services...
KUICCN005I Enter the password for root.

KUICCN039I Attempting to connect to host paris ...
KUICCN050I Distributing file 69 of 69 (156.8 MB / 157 MB)...
KUICCN002I Beginning the installation and configuration process...

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

3.3.3 Deploying non-OS agents

You can deploy non-OS agents through the Tivoli Enterprise Portal or from the command line.

Before starting the deployment, the following steps have to completed:

- The agent depot should be populated with the agent bundles for the agents to be deployed.

- You must have already installed or deployed an OS agent on the computer where you are now deploying the non-OS agent.

> **Note:** The deployment and configuration of agents varies depending on the specific agent. The following procedures provide generic deployment information. For the exact values required for your agent, see the configuration information in the user’s guide for the agent.

Deploying through the portal

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

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

Deploying through the command line

Run the following command to deploy an agent from the command line:

```
tacmd addSystem -t pc [-n MANAGED-OS] [-p NAME=VALUE ...]
```

Refer to *IBM Tivoli Monitoring Version 6.2.0 Command Reference,* SC23-6045 for the full syntax of this command, including parameter descriptions.

3.4 Tivoli Data Warehouse

Tivoli Data Warehouse is the term used to describe the IBM Tivoli Monitoring V6.2 solution that includes Tivoli Enterprise Portal server, Tivoli Data Warehouse database, the Warehouse Proxy agent, and the Summarization and Pruning agent.

This section describes Tivoli Data Warehouse implementation using DB2 as part of the solution. Please refer to *IBM Tivoli Monitoring Version 6.2.0 Installation and Setup Guide,* GC32-9407 for more information about other database solutions.

Table 3-9 shows the Tivoli Data Warehouse installation steps.

Table 3-9 Tivoli Data Warehouse installation steps

Steps	**Where to find information**
Supported components.	3.4.1, "Supported components" on page 124
Prerequisite installation.	3.4.2, "Prerequisite installation" on page 125
Create Tivoli Data Warehouse database.	3.4.3, "Create the Tivoli Data Warehouse database" on page 125
Install and configure Warehouse Proxy Agent.	3.4.4, "Install and configure a Warehouse Proxy agent" on page 129
Configure communications between the Tivoli Enterprise Portal and data warehouse.	3.4.5, "Tivoli Enterprise Portal/Tivoli Data Warehouse communication" on page 142
Install and configure Summarization and Pruning agent.	3.4.6, "Install and configure the Summarization and Pruning agent" on page 146

3.4.1 Supported components

Figure 3-26 presents the options for a Tivoli Data Warehouse solution using DB2 for the warehouse database. The diagram summarizes the supported operating system platforms for the various warehousing components, the supported database products, and the connections between components. For more specific information about supported operating systems and database products, including product names and versions, see Chapter 2, “IT environment” on page 25.

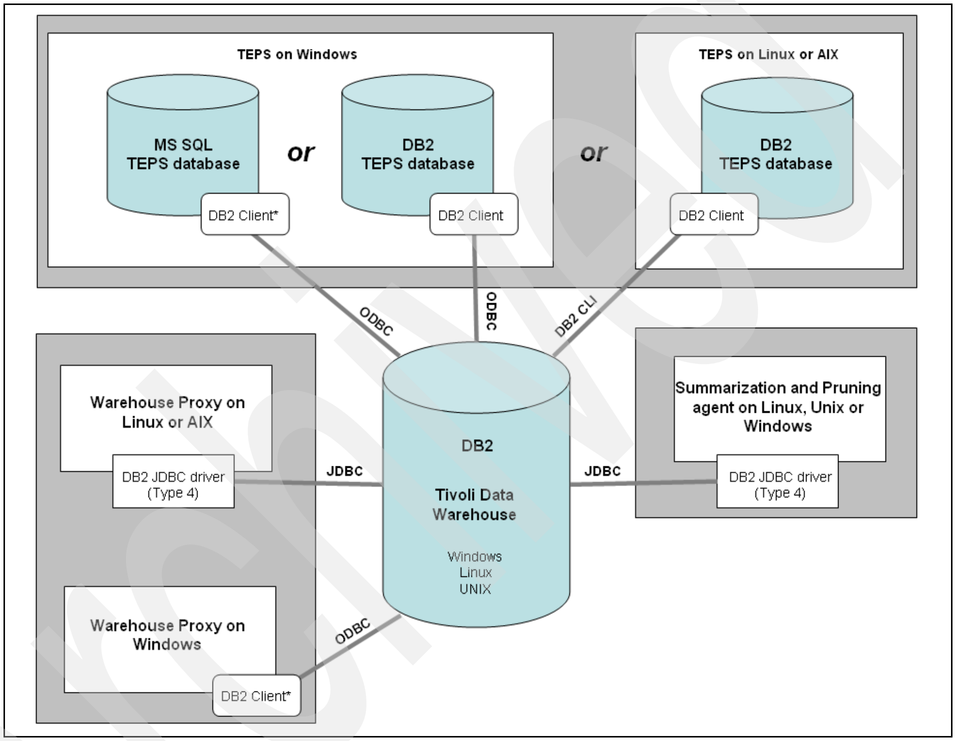


Figure 3-26 Tivoli Data Warehouse solution using DB2

Note: An asterisk (*) next to a database client indicates that you must manually install the client if it does not already exist.

3.4.2 Prerequisite installation

Before you implement your Tivoli Data Warehouse, we need the following components installed:

- The hub Tivoli Enterprise Monitoring Server.
- *(Optional)* One or more remote monitoring servers.
- The Tivoli Enterprise Portal Server, including the prerequisite RDBMS for the portal server database (DB2 or Microsoft SQL Server).
- An IBM DB2 server on the computer where you will create the Tivoli Data Warehouse database. (The Tivoli Data Warehouse database can be shared in a multi-hub installation or dedicated to a single hub).
- *(Optional)* A portal desktop client.
- *(Optional)* Monitoring agents, and the application support for the monitoring agents.

3.4.3 Create the Tivoli Data Warehouse database

This section provides guidelines for creating the Tivoli Data Warehouse database on DB2. For specific instructions on how to create a DB2 database, refer to the DB2 documentation or have a database administrator create the database for you.

Before you create the database, you need to estimate the size for the warehouse database. *IBM Tivoli Monitoring Version 6.2.0 Installation and Setup Guide,* GC32-9407 contains information about how to calculate the disk space needed.

Note: There are four important customizations that can affect the database size:

- Attribute groups to be selected for data collection
- How long the data will be kept (pruning settings)
- Number of agents
- Number of instances that an attribute group can have.

For detailed information about calculating the database size and also tips on how to optimize Tivoli Data Warehouse performance, refer to Chapter 4, “Planning historical data collection in large scale environments”, in *IBM Tivoli Monitoring: Implementation and Performance Optimization for Large Scale Environments*, SG24-7443.

Figure 3-27 shows our test environment Tivoli Data Warehouse solution using DB2. We installed Tivoli Data Warehouse on the same server as the portal server. For large scale production environments, you should install these on separate systems.

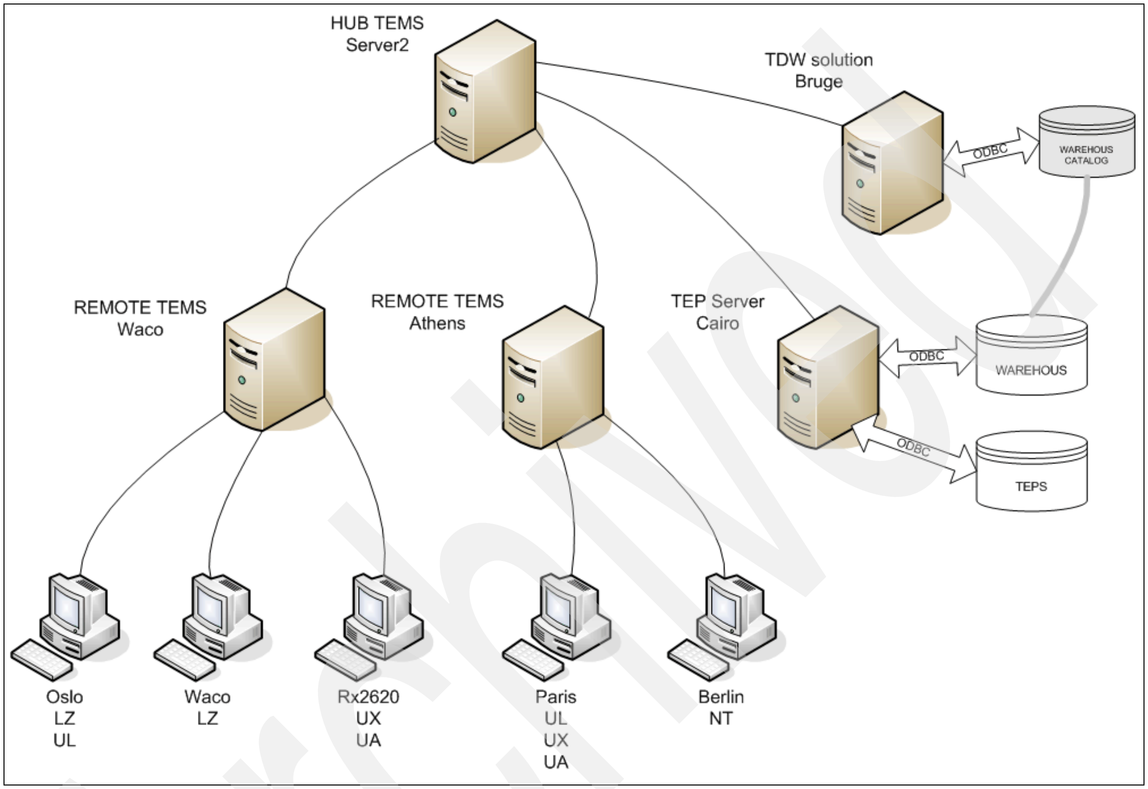


Figure 3-27 Tivoli Data Warehouse DB2 solution

Creating the warehouse database on DB2

Follow these guidelines to create a warehouse database using DB2:

- Create the database with UTF-8 encoding.
- Create a name for the warehouse database, and an operating system (OS) user account (user name and password) that the warehousing components (portal server, Warehouse Proxy agent, and Summarization and Pruning agent) can use to access the data warehouse. In these instructions, this user account is referred to as the warehouse user.
- Consider using the default values shown in Table 3-10 on page 127 for the warehouse name and warehouse user. The default values are used in the

configuration procedures for connecting the warehousing components to the warehouse database.

Table 3-10 Default values for Tivoli Data Warehouse parameters

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

- Give the warehouse user administrative authority to the database initially. After that, you can optionally limit the authority of the warehouse user to just the privileges required for interacting with the data warehouse. See the following sections for information about creating and limiting the authority of the warehouse user.
  - “Creating a warehouse user on Windows” on page 127
  - “Creating a warehouse user on Linux or UNIX” on page 128
  - “Limiting the authority of the warehouse user” on page 128
- For a Tivoli Data Warehouse on Linux or AIX, ensure that the DB2 server is configured for TCP/IP communications, as described in “Activating the DB2 listeners on a UNIX DB2 server” on page 129.

Creating a warehouse user on Windows

Complete the following steps on the computer where the warehouse database is installed to create a Windows OS user with Administrator authority:

1. Right-click the **My Computers** icon on the Windows desktop and click **Manage**.
2. In the navigation pane of the Computer Management window, expand **Local Users and Groups** by clicking on the plus sign (+).
3. Right-click the **Users folder** and click **New User**.
4. Type a user name and password in the **User Name** and **Password** fields. Confirm the password by typing it again in the **Confirm password** field.
5. Clear **User must change password at next logon**.
6. Click **Close**.
7. Click the **Groups** folder.
8. Double-click **Administrators** in the right pane of the window.
9. Click **Add** in the Administrator Properties window.

10. Locate the new user you created and select it.
11. Click **Add**.
12. Click **OK** and then **OK** again to close the Administrator Properties window.
13. Close the Computer Management window.

Creating a warehouse user on Linux or UNIX

Complete the following procedure on the computer where the warehouse database is installed to create a Linux or UNIX OS user with administrative authority to the warehouse:

- To create the user, follow the instructions in the documentation for the specific Linux or UNIX product and version that is installed on the computer where the warehouse database is located.
- To give this user administrative authority to the data warehouse, add the user to the DB2 SYSADM group. Run the following command to find the name of the DB2 SYSADM group:

  ```
  db2 get dbm cfg | grep SYSADM
  ```

Limiting the authority of the warehouse user

To limit the authority of the warehouse user, complete the following steps:

1. Connect to the data warehouse with db2admin privileges:

   ```
   db2 connect to WAREHOUS user db2admin using password
   ```

   where password is the password of the db2admin user.
2. Create a bufferpool of page size 8 K:

   ```
   db2 create bufferpool ITMBUF8K immediate size 250 pagesize 8k
   ```
3. Create a regular table space using the 8 K bufferpool:

   ```
   db2 create regular tablespace ITMREG8K pagesize 8K managed by system
   using ('itmreg8k') bufferpool ITMBUF8K
   ```
4. Create a system tablespace using the 8 K bufferpool:

   ```
   db2 create system temporary tablespace ITMSYS8K pagesize 8K managed
   by system using ('itmsys8k') bufferpool ITMBUF8k
   ```
5. Create a user tablespace using the 8 K Bufferpool:

   ```
   db2 create user temporary tablespace ITMUSER8K pagesize 8K managed
   by system using ('itmuser8k') bufferpool ITMBUF8k
   ```

6. Remove administrative privileges from the warehouse user (OS user) that you created when you created the warehouse database:
   - On Windows, remove the warehouse user from the Administrator group.
   - On Linux or UNIX, remove the warehouse user from the SYSADM group to which it was assigned.
7. Grant CONNECT and CREATETAB authorities to the warehouse user:

```
db2 "GRANT CONNECT ON DATABASE TO USER itmuser"
db2 "GRANT CREATETAB ON DATABASE TO USER itmuser"
```

Activating the DB2 listeners on a UNIX DB2 server

The TCP/IP listener processes on the DB2 server where the Tivoli Data Warehouse database is installed must be active in order to accept connections from a DB2 client or a JDBC Type 4 driver (DB2 UDB JDBC Universal Driver). On a Windows system, the DB2 listeners are automatically activated. Run the following commands on a UNIX system where the Tivoli Data Warehouse database is installed to activate the DB2 listeners:

```
db2set -i instance_name DB2COMM=tcpip
db2 update dbm cfg using SVCENAME port_number
db2stop
db2start
```

where instance_name is the name of the instance in which you created the warehouse database and port_number is the listening port for the instance. (The port number is specified in the file /etc/services.)

3.4.4 Install and configure a Warehouse Proxy agent

This section describes the steps to install and configure Warehouse Proxy agents in Windows, Linux, or AIX.

Installing a Warehouse Proxy agent

In order to populate a Tivoli Enterprise Data Warehouse database, we need to install a Warehouse Proxy agent. The installation process is similar to installing any other type of agent.

Table 3-11 shows you the steps for the agent installation process.

Table 3-11 Steps for installing a monitoring agent

Steps	Where to find information
Installing a monitoring agent on Windows	"Installing a monitoring agent on a Windows server" on page 102
Installing a monitoring agent on Linux or AIX	"Installing a monitoring agent on Linux or UNIX server" on page 108

Configuring communications on Windows

Besides installing the Warehouse Proxy agent, you need to establish the communication between the Tivoli Data Warehouse database and the Warehouse Proxy agent. The following steps describe the options to configure the communication

Installing a DB2 client

You need install a DB2 client on the computer where the Warehouse Proxy agent is installed if *both* of the following statements are true:

- The Warehouse Proxy is installed on Windows.
- The Warehouse Proxy needs to connect to a remote data warehouse.

Refer to the DB2 documentation for instructions on how to install a DB2 client.

After installing the DB2 client, you need catalog the remote data warehouse where the DB2 client was installed.

Cataloging a remote data warehouse

Perform this procedure on a computer where a DB2 client is installed to enable communication between the client and a remote DB2 server where the data warehouse is installed. For example, use this procedure to set up communication to a remote DB2 data warehouse server from:

- The DB2 client on the computer where the Tivoli Enterprise Portal Server is installed (on any platform).
- The DB2 client on a Windows computer where a Warehouse Proxy agent is installed.

Complete the following steps on the computer where the DB2 client is installed (the local computer):

1. Catalog the remote TCP/IP node where the warehouse database is installed:

   ```
   db2 catalog tcpip node <node_name> remote <host_name> server <port>
   db2 terminate
   ```

   Where:

   – <node_name> is an arbitrary name on the user's workstation used to identify the node.

   – <host_name> specifies the host name or IP address.

   – <port> is the default port for DB2 server is 60000.

2. Catalog the remote Tivoli Data Warehouse database:

   ```
   db2 catalog db <db_name> as <db_alias> at node <node_name>
   db2 terminate
   ```

   Where:

   – <db_name> is the name of the remote warehouse database.

   – <db_alias> is the nickname or alias used to identify the remote warehouse database on the local computer. The local alias for the warehouse database must match the name that you specify in the configuration procedure for the portal server, Warehouse Proxy agent, or Summarization and Pruning agent.

   – <node_name> is the name of the node where the warehouse database is located.

3. Test the connection to the remote warehouse database:

   ```
   db2 connect to <db_alias> user <user_name> using <user_password>
   ```

   Where:

   – <db_alias> is the nickname or alias used to identify the remote warehouse database on the local computer.

   – <user_name> and <user_password> are the user ID and password that the local DB2 client uses to access the warehouse database.

   These values must match the values that you specify in the configuration procedures for the portal server, Warehouse Proxy agent, or Summarization and Pruning agent.

The following examples describes the procedures to catalog a database. Example 3-14 shows a catalog of a node from the TEPS.

Example 3-14 Catalog a node from the TEPS

```
C:\>db2 catalog tcpip node bruge remote bruge server 50000
DB20000I  The CATALOG TCPIP NODE command completed successfully.
DB21056W  Directory changes may not be effective until the directory
cache is refreshed.
C:\>db2 terminate
DB20000I  The TERMINATE command completed successfully.
```

Example 3-15 shows a catalog of the warehouse from the TEPS.

Example 3-15 Catalog the warehouse from the TEPS

```
C:\>db2 catalog db warehous as warehous at node bruge
DB20000I  The CATALOG DATABASE command completed successfully.
DB21056W  Directory changes may not be effective until the directory
cache is refreshed.
C:\>db2 terminate
DB20000I  The TERMINATE command completed successfully.
```

Example 3-16 shows how to check that the node and the database have been created successfully.

Example 3-16 Checking the node

```
C:\>db2 list database directory
System Database Directory
Number of entries in the directory = 7

Database 1 entry:
Database alias                       = TEPS
 Database name                        = TEPS
 Database drive                       = C:\DB2
 Database release level               = a.00
 Comment                              =
 Directory entry type                 = Indirect
 Catalog database partition number    = 0
 Alternate server hostname            =
 Alternate server port number         =

Database 2 entry:
Database alias                       = WAREHOUS
 Database name                        = WAREHOUS
 Node name                            = BRUGE
 Database release level               = a.00
 Comment                              =
 Directory entry type                 = Remote
 Catalog database partition number    = -1
 Alternate server hostname            =
 Alternate server port number         =

C:\>db2 list node directory
Node Directory
Number of entries in the directory = 1
Node 1 entry:
Node name                      = BRUGE
 Comment                        =
 Directory entry type           = LOCAL
 Protocol                       = TCPIP
 Hostname                       = bruge
 Service name                   = 50000
```

Set the following system variable on the computer where the Warehouse Proxy agent is installed. Reboot the computer after setting the variable:

```
DB2CODEPAGE=1208
```

Set the environment variable whether or not the warehouse database is local or remote.

Configuring ODBC data source

A DB2 client on Windows requires an ODBC connection to the data warehouse, whether you have a remote database or local. For the Warehouse Proxy agent, you must configure the ODBC connection manually.

If the warehouse database is remote from the Warehouse Proxy agent, catalog the remote database before you configure the ODBC data source.

Complete the following procedure to set up an ODBC connection for a Warehouse Proxy agent on Windows to a local or remote Tivoli Data Warehouse.

1. On the computer where the Warehouse Proxy agent is installed, open the Control Panel.
2. Select **Administrative Tools** → **Data Sources (ODBC)**.
3. Click **Add** in the System DSN tab in the ODBC Data Source Administrator window.
4. Select **IBM DB2 ODBC DRIVER** from the list.

5. Click **Finish**.
6. In the ODBC DB2 Driver - Add window, perform the following steps:
   a. Enter ITM Warehouse in **Data source name**.
   b. Enter Warehous in **Database Alias**. If the Tivoli Data Warehouse is located on a remote computer, ensure that the database alias matches the alias that you used when cataloging the remote data warehouse. See "Cataloging a remote data warehouse" on page 130 for more details.
   c. Click **OK**.
7. Test the ODBC database connection before continuing:
   a. In the ODBC Data Source Administrator window, select **ITM Warehouse**.
   b. Click **Configure**.
   c. In the CLI/ODBC Settings - ITM Warehouse window, you see the data source name, ITM Warehouse.
   d. Enter ITMUser for the **User ID**.
   e. Type a password for the user in the **Password field**. The *default* password is itmpswd1.
   f. Click **Connect**.
   g. A Connection test successful message is displayed.
   h. Click **OK**.
   i. Click **OK** to close the window.

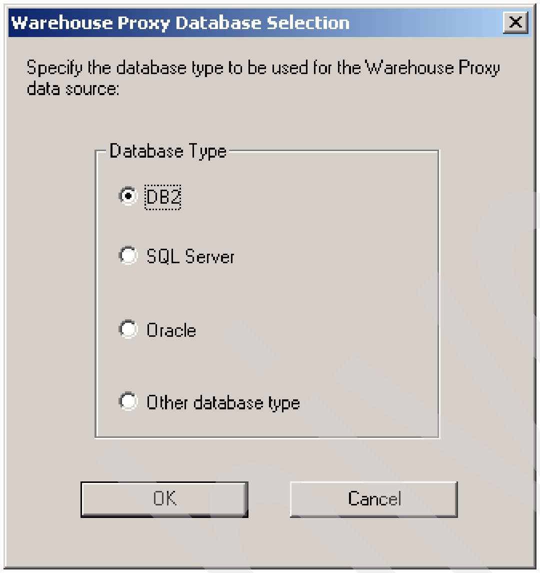
Configuring a Warehouse Proxy agent ODBC connection

Use this procedure to configure a Warehouse Proxy agent on Windows to connect to a DB2 data warehouse:

1. Log on to the Windows system where the Warehouse Proxy agent is installed and begin the configuration:
   a. Click **Start** → **Programs** → **IBM Tivoli Monitoring** → **Manage Tivoli Monitoring Services**. The Manage Tivoli Enterprise Monitoring Services window is displayed.
   b. Right-click **Warehouse Proxy** and click **Configure Using Defaults**. Click **Reconfigure** if the Warehouse Proxy is installed on the same computer as the portal server.
   c. Click **OK** on the message regarding connecting to a hub monitoring server.
2. The next two windows (entitled Warehouse Proxy: Agent Advanced Configuration) contain the settings for the connection between the Warehouse Proxy agent and the hub monitoring server. These settings were

specified when the Warehouse Proxy agent was installed. Click **OK** on each window to accept the settings.

3. Click **Yes** on the message asking if you want to configure the ODBC data source.
4. Select **DB2** from the list of databases and click **OK**. (See Figure 3-28).



Warehouse Proxy Database Selection

Specify the database type to be used for the Warehouse Proxy data source:

Database Type

● DB2

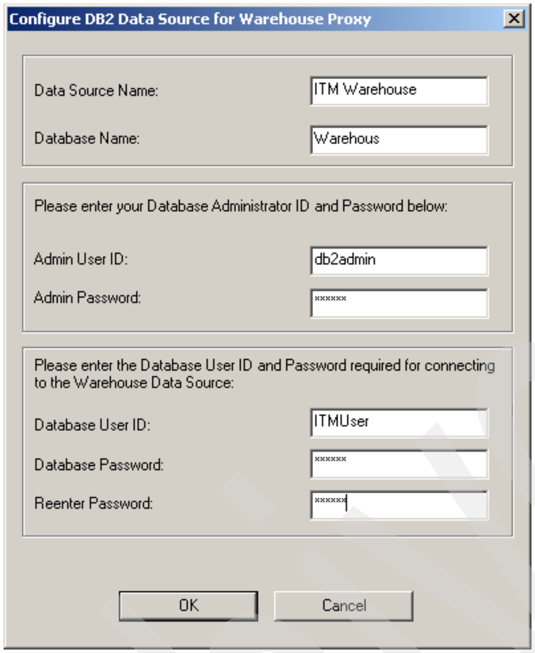
○ SQL Server

○ Oracle

○ Other database type

Figure 3-28 Warehouse Proxy Database Selection

The configuration window shown in Figure 3-29 is displayed.



Configure DB2 Data Source for Warehouse Proxy

Data Source Name: ITM Warehouse

Database Name: Warehous

Please enter your Database Administrator ID and Password below:

Admin User ID: db2admin

Admin Password: ******

Please enter the Database User ID and Password required for connecting to the Warehouse Data Source:

Database User ID: ITMUser

Database Password: ******

Reenter Password: ******

Figure 3-29 Configure DB2 Data Source for Warehouse Proxy window

5. Click **OK** to accept all default information in this window, or change one or more default values and then click **OK**. The fields on this window are described in Table 3-12.

Table 3-12 Configuring the information for the Tivoli Data Warehouse database on DB2

Field	**Default Value**	**Description**
Data Source Name	ITM Warehouse	The name of the data source.
Database Name	WAREHOUS	The name of the database. If the Warehouse Proxy agent is not installed on the same computer as the Tivoli Data Warehouse, this value must match the name of the database alias you used when cataloging the remote data warehouse.
Admin User ID	db2admin	The database administrator ID.

Field	Default Value	Description
Admin Password	(no default)	The password for the database administrator.
Database User ID	ITMUser	The name of the Windows OS user that the Warehouse Proxy agent will use to access the Tivoli Data Warehouse database.
Database Password	itmpswd1	The password for the Windows user. If your environment requires complex passwords (passwords that require both alpha and numeric characters), specify a password that complies with these requirements.
Reenter Password	itmpswd1	Confirm the password by entering it again.
Synchronize TEPS Warehouse Information	yes	This check box is used only if you are re-configuring a Warehouse Proxy agent that is installed on the same Windows computer as the portal server. If this check box is selected, any change that you make to the connection information in this window for the Warehouse Proxy is automatically applied to the portal server.

6. Click **OK**.

Configuring communications on Linux

This section describes how to configure the communication between data warehouse and the Warehouse Proxy agent on Linux.

If the data warehouse is located on a remote computer, you need to copy the DB2 UDB JDBC Universal Driver (Type 4 driver) JAR files, included with the DB2 product installation, to the local computer where the Warehouse Proxy agent is installed. You can copy the files to any directory on the local computer.

The Type 4 driver file names and locations are as follows:

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

where <db2installdir> is the directory where DB2 was installed.

The default DB2 Version 9 installation directory is as follows:

- On AIX: /usr/opt/db2_09_01
- On Linux: /opt/IBM/db2/V9.1

After copying the DB2 UDB JDBC Universal Driver (Type 4 driver), we need to configure it; see “Configuring a Warehouse Proxy agent JDBC connection” on page 138 to complete the configuration.

Configuring a Warehouse Proxy agent JDBC connection

Use this procedure to configure a Warehouse Proxy agent on Linux or AIX to connect to a DB2 Tivoli Data Warehouse on any operating system:

1. Log on to the computer where the Warehouse Proxy agent is installed and begin the configuration.

   > **Note:** An X11 GUI is required to configure the agent. Alternatively, you can run the following command to utilize an X terminal emulation program (such as Cygwin) that is running on another computer:
   >
   > ```
   > export DISPLAY=my_windows_pc_IP_addr:0.0
   > ```

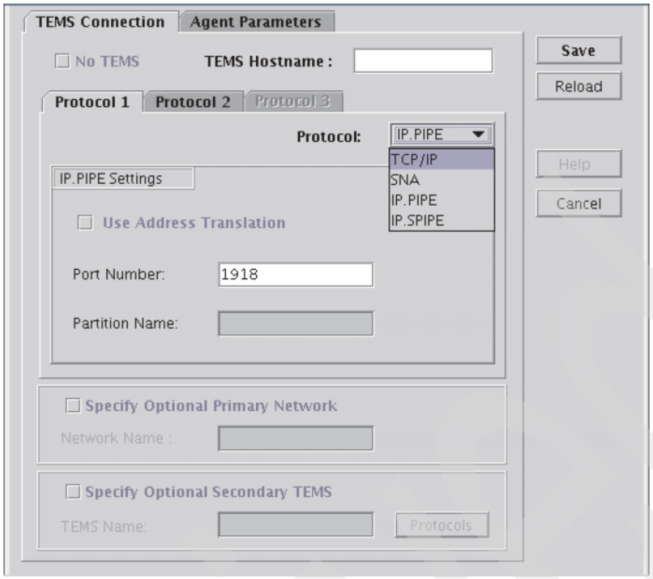
   a. Change to the install_dir/bin directory and run the following command:

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

      where install_dir is the installation directory for IBM Tivoli Monitoring.

      The default installation directory is opt/IBM/ITM. The Manage Tivoli Enterprise Monitoring Services window is displayed.

   b. Right-click **Warehouse Proxy** and click **Configure**. The Configure Warehouse Proxy window is displayed (Figure 3-30 on page 139).



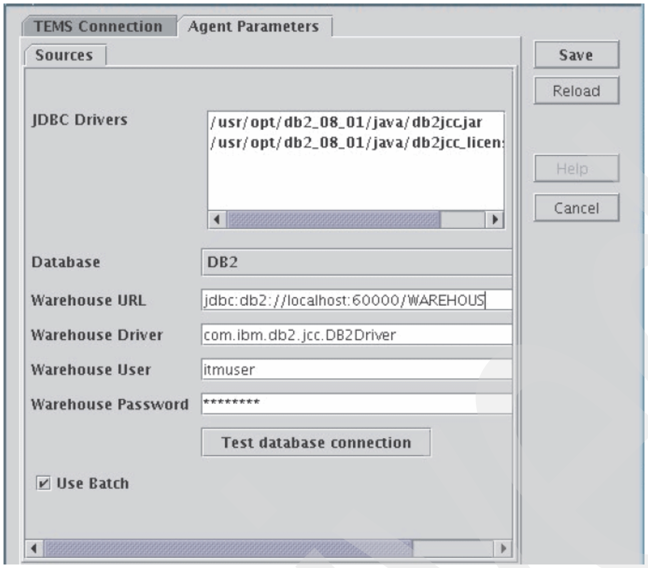
Protocol: IP.PIPE

Port Number: 1918

Figure 3-30 Configure Warehouse Proxy window (TEMS Connection tab)

2. On the **TEMS Connection tab**, review the settings for the connection between the Warehouse Proxy agent and the hub monitoring server. Correct the settings if necessary.

3. Click the **Agent Parameters** tab (Figure 3-31).



JDBC Drivers: /usr/opt/db2_08_01/java/db2jcc.jar
/usr/opt/db2_08_01/java/db2jcc_licen:

Database: DB2

Warehouse URL: jdbc:db2://localhost:60000/WAREHOUS

Warehouse Driver: com.ibm.db2.jcc.DB2Driver

Warehouse User: itmuser

Warehouse Password: ********

☑ Use Batch

Figure 3-31 Configure Warehouse Proxy window (Agent Parameters tab)

4. In the **Database** drop-down list, select **DB2**.
5. Add the names and directory locations of the JDBC driver JAR files to the **JDBC Drivers** list box:
   a. Use the scroll bar at the bottom of the window to display the Add and Delete buttons, which are located to the right of the JDBC Drivers list box.
   b. Click **Add** to display the file browser window. Navigate to the location of the driver files on this computer and select the following driver files:

      ```
      db2jcc.jar
      db2jcc_license_cu.jar
      ```

   c. Click **OK** to close the browser window and add the JDBC driver files to the list.

      If you need to delete an entry from the list, select the entry and click **Delete**.
6. Change the default value displayed in the Warehouse URL field if it is not correct. The default Tivoli Data Warehouse URL for IBM DB2 is as follows:

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

- If the Tivoli Data Warehouse is installed on a remote computer, specify the host name of the remote computer instead of localhost.

- Change the port number if it is different.
- If the name of the Tivoli Data Warehouse database is not WAREHOUS, replace WAREHOUS with the actual name.

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

   The DB2 JDBC driver name is as follows:

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

8. If necessary, change the entries in the Warehouse User and Warehouse Password fields to match the user name and password that were created for the Tivoli Data Warehouse. The default user name is itmuser and the default password is itmpswd1.
9. Check the **Use Batch** check box if you want the Warehouse Proxy agent to submit multiple execute statements to the Tivoli Data Warehouse database for processing as a batch.

   In some situations, such as crossing a network, sending multiple statements as a unit is more efficient than sending each statement separately. Batch processing is one of the features provided with the JDBC 2.0 API.

10. Click **Test database connection** to ensure you can communicate with the Tivoli Data Warehouse database.
11. Click **Save** to save your settings and close the window.

Starting the Warehouse Proxy

This section describes how to start the agent.

To start the agent in Windows, AIX, or Linux, open the Manage Tivoli Enterprise Services window, right-click **Warehouse Proxy**, and select **Start**.

For Linux or AIX, you can start Warehouse Proxy agent from the command line by running the following command from the bin directory of the IBM Tivoli Monitoring installation directory. The default installation directory is /opt/IBM/ITM:

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

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

3.4.5 Tivoli Enterprise Portal/Tivoli Data Warehouse communication

Complete the tasks described in Table 3-13, in the order listed, to configure communications between the portal server and the data warehouse.

Table 3-13 Configuring communications between portal server and DB2 data warehouse

Task	Procedure
(Portal server on Windows only) If the portal server database was created on Microsoft SQL Server, install a DB2 database client on the portal server. If the portal server database was created on DB2, the DB2 client already exists on the portal server.	Refer to the DB2 documentation for instructions on how to install a DB2 client.
On the computer where the portal server is installed, catalog the remote data warehouse. You must perform this step before configuring the portal server to connect to the data warehouse. Cataloging the remote data warehouse enables communications between the DB2 client on the portal server and the remote DB2 server where the data warehouse is located. Complete this task regardless of which platforms are used by the portal server or the data warehouse.	“Cataloging a remote data warehouse” on page 130.
Configure the portal server to connect to the data warehouse. The configuration procedure on Windows automatically configures an ODBC connection to the data warehouse.	For a portal server on Windows, see “Configuring a Windows portal server (ODBC connection)” on page 142. For a portal server on Linux or AIX, see “Configuring a Linux or AIX portal server (DB2 CLI connection)” on page 144.
Restart the portal server.	“Starting the Tivoli Enterprise Portal Server” on page 146.

Configuring a Windows portal server (ODBC connection)

The procedure described in this section uses the Manage Tivoli Enterprise Services window to configure an ODBC connection between a Windows portal server and the data warehouse. You do not need to configure the ODBC data source through the Control Panel in Windows.

Before starting this configuration, you need to catalog the remote warehouse database before you configure the Windows portal server to connect database.

See “Cataloging a remote data warehouse” on page 130 for more details. The ODBC connection does not work if the remote database has not been catalogued prior to performing this procedure.

Complete the following procedure to configure a portal server on Windows to connect to a DB2 data warehouse:

1. Log on to the Windows system where the portal server is installed and begin the configuration:

   a. Select **Start** → **Programs** → **IBM Tivoli Monitoring** → **Manage Tivoli Monitoring Services**.

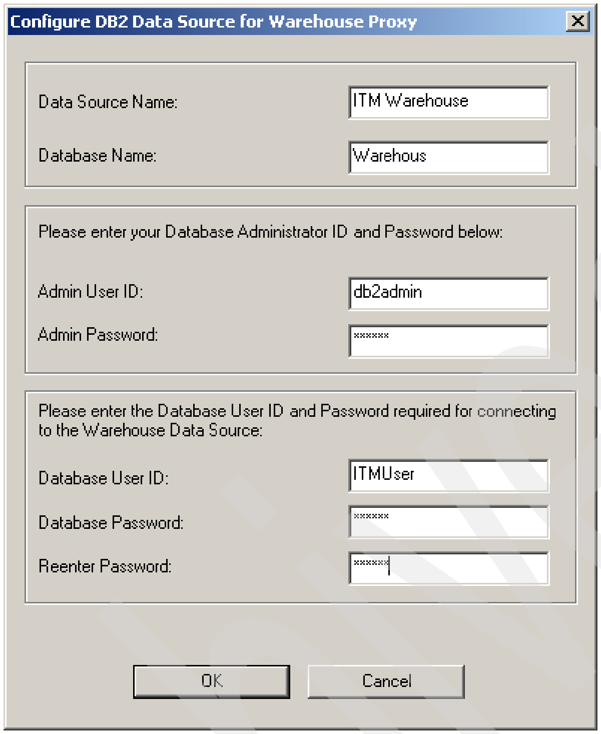
      The Manage Tivoli Enterprise Monitoring Services window is displayed.

   b. Right-click **Tivoli Enterprise Portal Server** and click **Reconfigure**.

2. The next two windows (entitled TEP Server Configuration) contain the settings for the connection between the portal server and the hub monitoring server. These settings were specified when the portal server was installed. Click **OK** on each window to accept the settings.

3. Click **Yes** on the message asking if you want to re-configure the warehouse information for the Tivoli Enterprise Portal Server.

4. Select **DB2** from the list of databases and click **OK**. Figure 3-32 is displayed.



Configure DB2 Data Source for Warehouse Proxy

Data Source Name: ITM Warehouse

Database Name: Warehous

Please enter your Database Administrator ID and Password below:

Admin User ID: db2admin

Admin Password: ******

Please enter the Database User ID and Password required for connecting to the Warehouse Data Source:

Database User ID: ITMUser

Database Password: ******

Reenter Password: ******

Figure 3-32 Configure DB2 Data Source for Warehouse Proxy window

5. Click **OK** to accept all the default information in this window, or change one or more default values and then click **OK**. The fields in this window are described in the Table 3-12 on page 136.

Configuring a Linux or AIX portal server (DB2 CLI connection)

Use this procedure to configure a portal server on Linux or AIX to connect to a DB2 Tivoli Data Warehouse on any operating system:

1. Log on to the computer where the Tivoli Enterprise Portal Server is installed and begin the configuration.

   a. . Change to the install_dir/bin directory and run the following command:

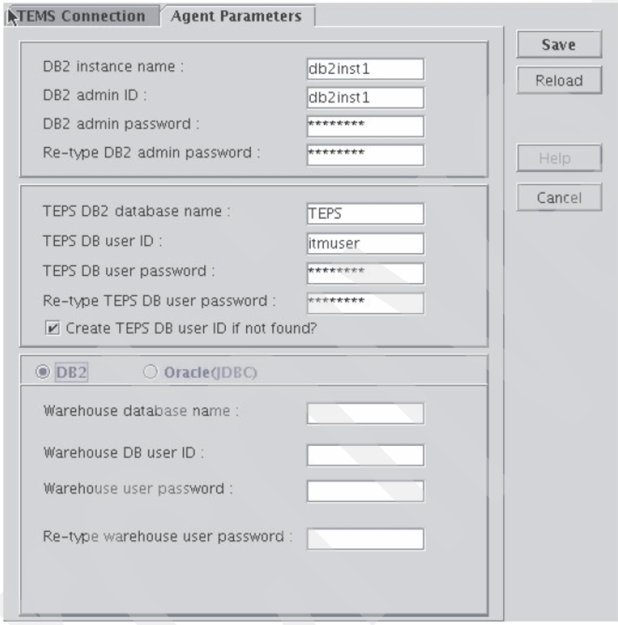
      ```
      ./itmcmd manage [-h install_dir]
      ```

      where install_dir is the installation directory for IBM Tivoli Monitoring. The default installation directory is opt/IBM/ITM.

      The Manage Tivoli Enterprise Monitoring Services window is displayed.

   b. Right-click **Tivoli Enterprise Portal Server** and click **Configure**. The Configure Tivoli Enterprise Portal Server window is displayed.

2. On the TEMS Connection tab, review the settings for the connection between the portal server and the hub monitoring server. These settings were specified when the portal server was installed.
3. Click the **Agent Parameters** tab.
4. Select the DB2 radio button. The fields for configuring the connection to a DB2 data warehouse are displayed at the bottom of the window.



DB2 instance name : db2inst1
DB2 admin ID : db2inst1
DB2 admin password : ********
Re-type DB2 admin password : ********

TEPS DB2 database name : TEPS
TEPS DB user ID : itmuser
TEPS DB user password : ********
Re-type TEPS DB user password : ********
☑ Create TEPS DB user ID if not found?

● DB2 ○ Oracle(JDBC)

Warehouse database name :
Warehouse DB user ID :
Warehouse user password :
Re-type warehouse user password :

Figure 3-33 Configuring the connection to a DB2 data warehouse

5. Enter information in the fields described in Table 3-14.

Table 3-14 Configuration information for TDW database on DB2

Field	Default value	Description
Warehouse database name	WAREHOUS	The name of the Tivoli Data Warehouse database.
Warehouse database user ID	itmuser	The login name of the database user that the portal server will use to access the Tivoli Data Warehouse database.

Field	Default value	Description
Warehouse user password	itmpswd1	The password for the database login user. If your environment requires complex passwords (passwords that require both alpha and numeric characters), specify a password that complies with these requirements.
Re-type warehouse user password	itmpswd1	Confirm the password by entering it again.

6. Confirm the password by entering it again.

Starting the Tivoli Enterprise Portal Server

This section describes how to start the Tivoli Enterprise Portal Server.

To start the portal server in Windows, AIX, or Linux, open the Manage Tivoli Enterprise Services window, right-click **Tivoli Enterprise Portal Server**, and select **Start**.

For Linux or AIX, you can start a Warehouse Proxy agent from the command line; run the following command from the bin directory of the IBM Tivoli Monitoring installation directory. The default installation directory is /opt/IBM/ITM:

```
./itmcmd agent start cq
```

where cq is the product code for the Tivoli Enterprise Portal Server.

3.4.6 Install and configure the Summarization and Pruning agent

This section describes the steps to install and configure the Summarization and Pruning agent on Windows, Linux, or AIX.

Install the Summarization and Pruning agent

If you want to aggregate and prune the size of the database, you need to use the Summarization and Pruning agent. The installation process is identical to the other agent installation. Table 3-15 on page 147 shows the steps for installing a monitoring agent.

Table 3-15 Steps for installing a monitoring agent

Steps	Where to find information
Installing monitoring agent on Windows	"Installing a monitoring agent on a Windows server" on page 102
Installing monitoring agent on Linux or AIX	"Installing a monitoring agent on Linux or UNIX server" on page 108

> **Note:** Complete the tasks described in Table 3-15, in the order listed, to install and configure the Summarization and Pruning agent.

Configuring communications

This section describes how to configure the communication between a data warehouse and the Summarization and Pruning agent.

If the data warehouse is located on a remote computer, you need to copy the DB2 UDB JDBC Universal Driver (Type 4 driver) JAR files, included with the DB2 product installation, to the local computer where the Summarization and Pruning agent is installed. You can copy the files to any directory on the local computer.

The Type 4 driver file names and locations are as follows:

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

where <db2installdir> is the directory where DB2 was installed.

The default DB2 Version 9 installation directory is as follows:

- On AIX: /usr/opt/db2_09_01
- On Linux: /opt/IBM/db2/V9.1
- On Windows: C:\Program Files\IBM\SQLLIB

After copying the DB2 UDB JDBC Universal Driver (Type 4 driver), we need to configure it; refer to "Configuring a Warehouse Proxy agent JDBC connection" on page 138 to complete the configuration.

JDBC connection for the Summarization and Pruning agent

Use this procedure to configure the Summarization and Pruning agent to connect to a Tivoli Data Warehouse database created on any of the supported database platforms and operating systems.

The procedure to configure JDBC is pretty much the same in regards to Windows with Linux and AIX agents. The steps below describes the procedure for the three platforms:

1. Log on to the computer where the Summarization and Pruning agent is installed and begin the configuration
2. Open the Manage Tivoli Enterprise Monitoring Services window:
   - On Windows, select **Start** → **Programs** → **IBM Tivoli Monitoring** → **Manage Tivoli Monitoring Services**.
   - On Linux or UNIX, change to the install_dir/bin directory and run the following command:

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

     where install_dir is the installation directory for IBM Tivoli Monitoring. The default installation directory is C:\IBM\ITM on Windows and /opt/IBM/ITM on Linux and UNIX
3. Right-click **Summarization and Pruning Agent**.
4. Click **Configure Using Defaults**.
   - On Windows, click **Configure Using Defaults**.
   - On Linux or UNIX, click **Configure**. I

   If you are reconfiguring, click **Reconfigure**.
5. Review the settings for the connection between the Summarization and Pruning agent and the hub Tivoli Enterprise Monitoring server. These settings were specified when the Summarization and Pruning agent was installed.

   On Windows, perform the following steps:

   a. On the Warehouse Summarization and Pruning Agent: Agent Advanced Configuration window, verify the communications protocol of the hub monitoring server in the **Protocol** drop-down list. Click **OK**.

   b. On the next window, verify the host name and port number of the hub monitoring server. Click **OK**.

   On Linux or UNIX, verify the following information in the TEMS Connection tab:

   - The host name of the hub monitoring server in the TEMS Hostname field. (If the field is not active, clear the **No TEMS** check box.)
   - The communications protocol that the hub monitoring server uses in the Protocol drop-down list.
     - If you select **IP.UDP**, **IP.PIPE**, or **IP.SPIPE**, enter the port number of the monitoring server in the Port Number field.

- If you select SNA, enter information in the Net Name, LU Name, and LOG Mode fields.

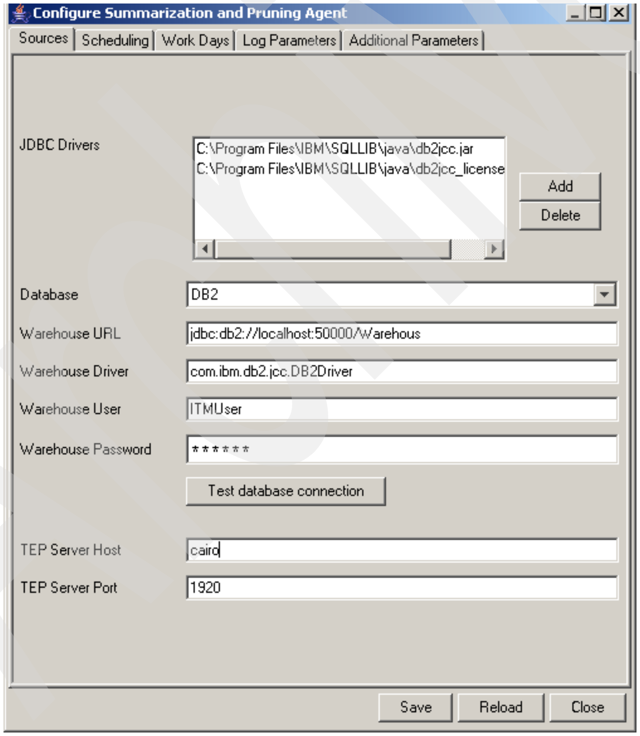
  For information about the different protocols available to the hub monitoring server on Linux or UNIX, and associated default values, see Table 3-3 on page 75.

6. When you are finished verifying or entering information about the hub monitoring server:

   – On Windows, click **Yes** on the message asking if you want to configure the Summarization and Pruning agent.

   – On Linux or UNIX, click the **Agent Parameters** tab. A multi-tabbed configuration window is displayed with the Sources tab at the front.

   Figure 7 on page 150 shows the configuration window for a Summarization and Pruning agent on Windows (with values displayed for a DB2 warehouse database). The configuration window for a Summarization and Pruning agent on Linux or UNIX is similar.



JDBC Drivers: C:\Program Files\IBM\SQLLIB\java\db2jcc.jar
C:\Program Files\IBM\SQLLIB\java\db2jcc_license

Database: DB2

Warehouse URL: jdbc:db2://localhost:50000/Warehous

Warehouse Driver: com.ibm.db2.jcc.DB2Driver

Warehouse User: ITMUser

Warehouse Password: ******

TEP Server Host: cairo

TEP Server Port: 1920

Figure 3-34 Sources tab of Configure Summarization and Pruning Agent window

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

   a. On Linux or UNIX, use the scroll bar at the bottom of the window to display the Add and Delete buttons, which are located to the right of the JDBC Drivers list box.

   b. Click **Add** to display the file browser window. Navigate to the location of the driver files on this computer and select the Type 4 driver files for your database platform. Refer to “Configuring communications” on page 147 for the files’ locations.

   c. Click **OK** to close the browser window and add the JDBC driver files to the list.

8. In the Database field, select **DB2** from the drop-down box. The default values for the database platform you selected are displayed in the other text fields on the Sources tab.

9. Change the default value displayed in the Warehouse URL field if it is not correct. The value for DB2 is:

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

   – If the Tivoli Data Warehouse is installed on a remote computer, specify the host name of the remote computer instead of localhost.

   – Change the port number if it is different.

   – If the name of the Tivoli Data Warehouse database is not WAREHOUS, replace WAREHOUS with the actual name.

10. Verify that the JDBC driver name for DB2 is set correctly; the correct value for DB2 is:

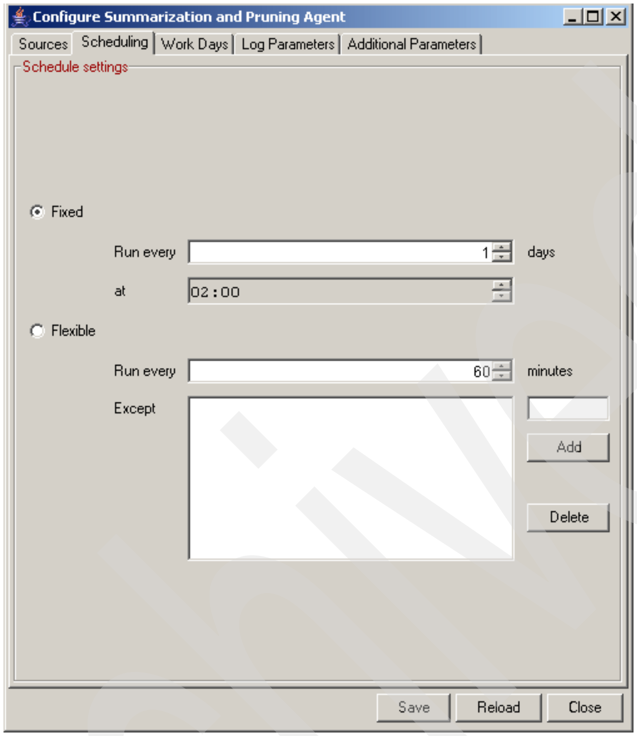
    ```
    com.ibm.db2.jcc.DB2Driver
    ```

11. If necessary, change the entries in the Warehouse User and Warehouse Password fields to match the user name and password that were created for the Tivoli Data Warehouse. The default user name is itmuser and the default password is itmpswd1.

12. In the TEP Server Host and TEP Server Port fields, enter the host name of the computer where the Tivoli Enterprise Portal Server is installed and the port number that it uses to communicate with the Tivoli Data Warehouse server.

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

14. Select the **Scheduling** tab to specify when you want summarization and pruning to take place. You can schedule it to run on a fixed schedule or on a flexible schedule (Figure 3-35):



Schedule settings

● Fixed

Run every 1 days

at 02:00

○ Flexible

Run every 60 minutes

Except

Figure 3-35 Scheduling tab for the Summarization and Pruning Agent

- Fixed
  - Schedule the Summarization and Pruning agent to run every x days.
  - Select the time of the day that you want the agent to run.

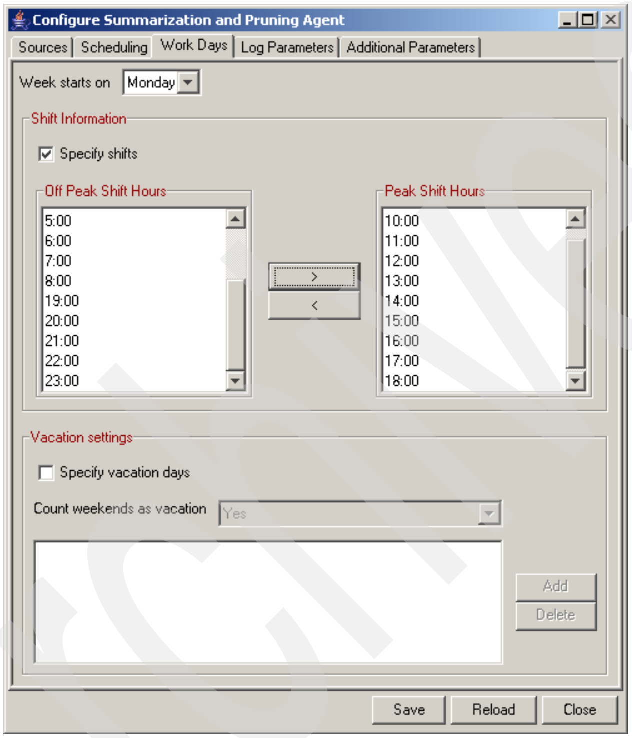
    Set the time to at least five minutes from the current time if you want it to run right away.
- Flexible
  - Schedule the Summarization and Pruning agent to run every x minutes.

- Optionally, specify the times when the agent should not run, using the format HH:MM-HH:MM, with multiple values separated by a comma. Click **Add** to add the text. For example, to block the agent from running between 00:00 and 01:59 and between 04:00 and 04:59, use:

  ```
  00:00-01:59,04:00-04:59
  ```

  Do not use the Add button unless you are adding a blackout period.

15. Specify shift and vacation settings in the Work Days tab (Figure 3-36).



Week starts on: Monday

☑ Specify shifts

Off Peak Shift Hours: 5:00, 6:00, 7:00, 8:00, 19:00, 20:00, 21:00, 22:00, 23:00

Peak Shift Hours: 10:00, 11:00, 12:00, 13:00, 14:00, 15:00, 16:00, 17:00, 18:00

□ Specify vacation days

Count weekends as vacation: Yes

Figure 3-36 Work Days tab of Summarization and Pruning Agent

When you enable and configure shifts, IBM Tivoli Monitoring produces three separate summarization reports:

- Summarization for peak shift hours
- Summarization for off-peak shift hours
- Summarization for all hours (peak and off-peak)

Similarly, when you enable and configure vacations, IBM Tivoli Monitoring produces three separate summarization reports:

- Summarization for vacation days
- Summarization for non-vacation days
- Summarization for all days (vacation and non-vacation)

Complete the following steps to enable shifts, vacations, or both:

- Select when the beginning of the week starts.

  To configure shifts:

  i. Select **Specify shifts** to enable shifts.

  ii. Optionally, change the default settings for peak and off peak hours by selecting and moving hours between the Peak Shift Hours box and the Off Peak Shift Hours box using the arrow buttons.

  Note: Changing the shift information after data has been summarized creates an inconsistency in the data. Data that was previously collected is not summarized again to account for the new shift values.

  To configure vacation settings:

  i. Select **Specify vacation days** to enable vacation days.

  ii. Select **Yes** in the drop-down list if you want to specify weekends as vacation days.

  iii. Select **Add** to add vacation days.

  iv. Select the vacation days you want to add from the calendar.

  On UNIX or Linux, right-click, instead of click, to select the month and year.

  The days you select are displayed in the list box.

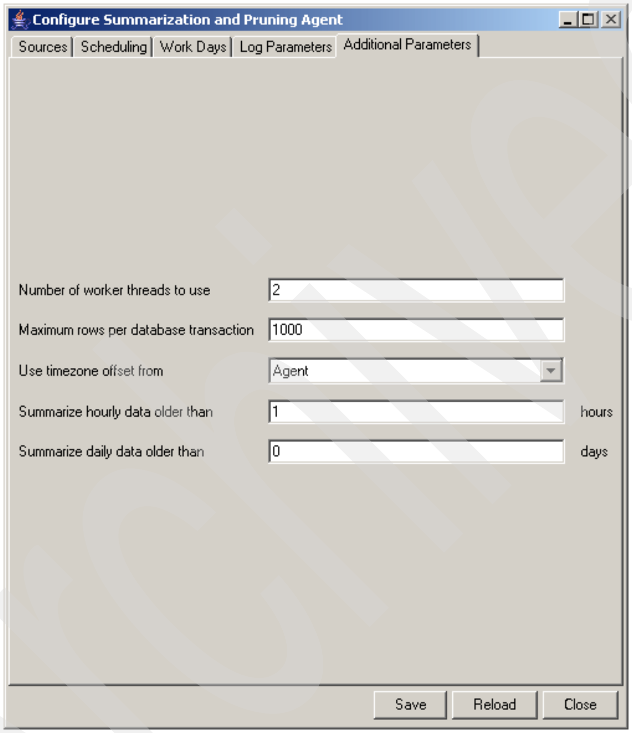
  If you want to delete any days you have previously chosen, select them and click **Delete**.

  Note: Add vacation days in the future. Adding vacation days in the past creates an inconsistency in the data. Data that was previously collected is not summarized again to account for vacation days.

16.Select the **Log Parameters** tab to set the intervals for log pruning:

- Select **Keep WAREHOUSEAGGREGLOG data for**, select the unit of time (day, month, or year), and the number of units for which data should be kept.
- Select **Keep WAREHOUSLOG data for**, select the unit of time (day, month, or year), and the number of units for which data should be kept.

17.Specify additional summarization and pruning settings in the **Additional Parameters** tab:



Number of worker threads to use: 2

Maximum rows per database transaction: 1000

Use timezone offset from: Agent

Summarize hourly data older than: 1 hours

Summarize daily data older than: 0 days

Figure 3-37 Additional Parameters tab of Summarization and Pruning Agent

a. Specify the number of additional threads you want to use for handling summarization and pruning processing. The number of threads should be 2 * N, where N is the number of processors where the Summarization and Pruning agent is running.

b. Specify the maximum rows that can be deleted in a single pruning transaction. Any positive integer is valid. The default is 1000. There is no value that indicates you want all rows deleted.

c. Indicate a time zone for historical data from the Use time zone offset from drop-down list. This field indicates which time zone to use when a user specifies a time period in a query for monitoring data.

   - Select Agent to use the time zone (or time zones) where the monitoring agents are located.
   - Select Warehouse to use the time zone where the Summarization and Pruning agent is located.

> **Note:**
>
> ► Skip this field if the Summarization and Pruning agent and the monitoring agents that collect data are all in the same time zone.
>
> ► If the Tivoli Data Warehouse and the Summarization and Pruning agent are in different time zones, the Warehouse choice indicates the time zone of the Summarization and Pruning agent, not the warehouse.

d. Specify the age of the data you want summarized in the Summarize hourly data older than and Summarize daily data older than fields. The default is 1 for hourly data and 0 for daily data.

18. Save your settings and close the window. Click **Save** to save your settings. On Windows, click **Close** to close the configuration window.

   – On Windows, click **Save** and then click **Close**.

   – On Linux or UNIX, click **Save** and then click **Cancel**.

Configure history collection

When you configure history collection, you specify settings for how often to collect, aggregate, and prune data for individual monitoring agents and attribute groups. Configure the history collection from the Tivoli Enterprise Portal. See the *IBM Tivoli Monitoring Version 6.2.0 Administrator's Guide,* SC32-9408 for instructions on how to configure history collection.

Starting the Summarization and Pruning agent

This section describes how to start the Summarization and Pruning agent.

To start the portal server in Windows, AIX, or Linux, open the Manage Tivoli Enterprise Services window, right-click **Summarization and Pruning agent**, and select **Start**.

For Linux or AIX, you can start the Warehouse Proxy agent from the command line by running the following command from the bin directory of the IBM Tivoli Monitoring installation directory. The default installation directory is /opt/IBM/ITM.

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

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

Part 2

Deployment

In this part, we discuss the deployment of IBM Tivoli Monitoring V6.2, including several case studies, such as migration from IBM Tivoli Monitoring V5, event management integration, and the Agent Builder.

4

Upgrading from IBM Tivoli Monitoring V5.1.2

This chapter details procedures for upgrading components of an IBM Tivoli Monitoring V5.1.2 environment into IBM Tivoli Monitoring V6.2 infrastructure.

The components of the two infrastructures and their comparison are outlined in this chapter. Installation procedures and the use of the IBM Tivoli Monitoring Migration Toolkit (migration toolkit) are detailed.

The following topics are described:

- "Upgrading from Tivoli Distributed Monitoring V3.7" on page 160
- "Environment used for this book" on page 160
- "Upgrading your IBM Tivoli Monitoring V5.1.2 environment" on page 163
- "IBM Tivoli Monitoring Migration Toolkit" on page 191
- "Migration toolkit internal flow" on page 275
- "Problem determination" on page 280
- "Migrating custom resource models" on page 283

4.1 Upgrading from Tivoli Distributed Monitoring V3.7

IBM Tivoli Monitoring V6.2 provides the IBM Tivoli Monitoring Upgrade Toolkit to upgrade the components of you Tivoli Distributed Monitoring V3.7 environment and migrate them to the new infrastructure.

The upgrade toolkit has been slightly modified to allow a direct migration to IBM Tivoli Monitoring V6.2, but the functions are exactly the same as the previous version.

Refer to Chapter 5, "Tivoli Distributed Monitoring V3.7 upgrade", in *Getting Started with IBM Tivoli Monitoring 6.1 on Distributed Environments*, SG24-7142 for more information. That chapter covers:

- Comparing Tivoli Distributed Monitoring to IBM Tivoli Monitoring V6.1
- Installing the Upgrade Tool components
- Using the Upgrade Tools
- Post-upgrade considerations

4.2 Environment used for this book

The environment installed for this part of the book consists of a Tivoli Management Framework architecture used as a framework for the IBM Tivoli Monitoring V5.1.2 infrastructure deployment. We used a single Tivoli Management Region (TMR) server with two gateways: one on the TMR server itself, and one on a separate managed node.

Figure 4-1 on page 161 shows the machine names that will be referred to in the next sections.

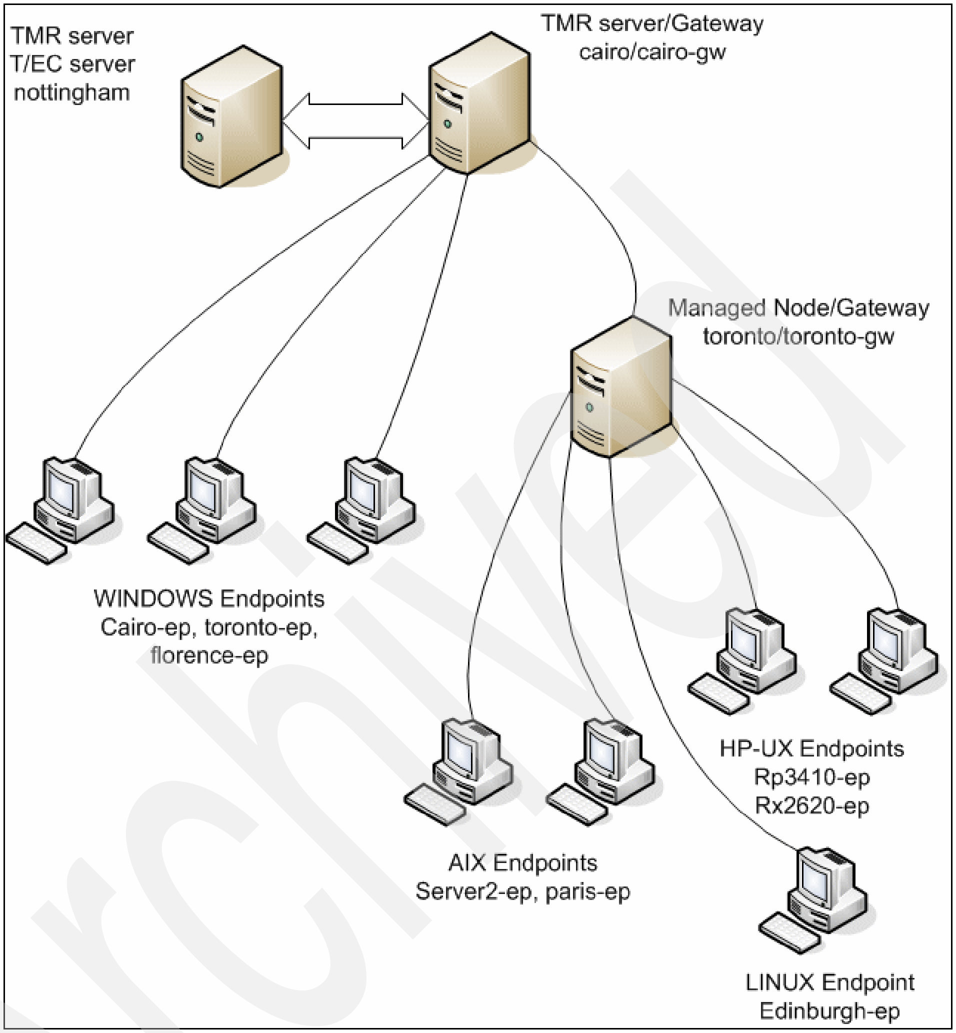


Figure 4-1 IBM Tivoli Monitoring V5.1.2 environment

The IBM Tivoli Monitoring V6.2 environment has been deployed in two stages:

- Manual installation of the infrastructure components: This stage consists of the installation of monitoring server, portal server, portal client, and any remote monitoring server in the mapped infrastructure
- Remote deployment of the managed systems using the migration toolkit: This stage consists of the remote deployment of the monitoring agents using the functionalities provided by the migration toolkit.

We will delve into the details of the above stages in 4.4, “IBM Tivoli Monitoring Migration Toolkit” on page 191.

Figure 4-2 shows the IBM Tivoli Monitoring V6.2 machines we used in this project.

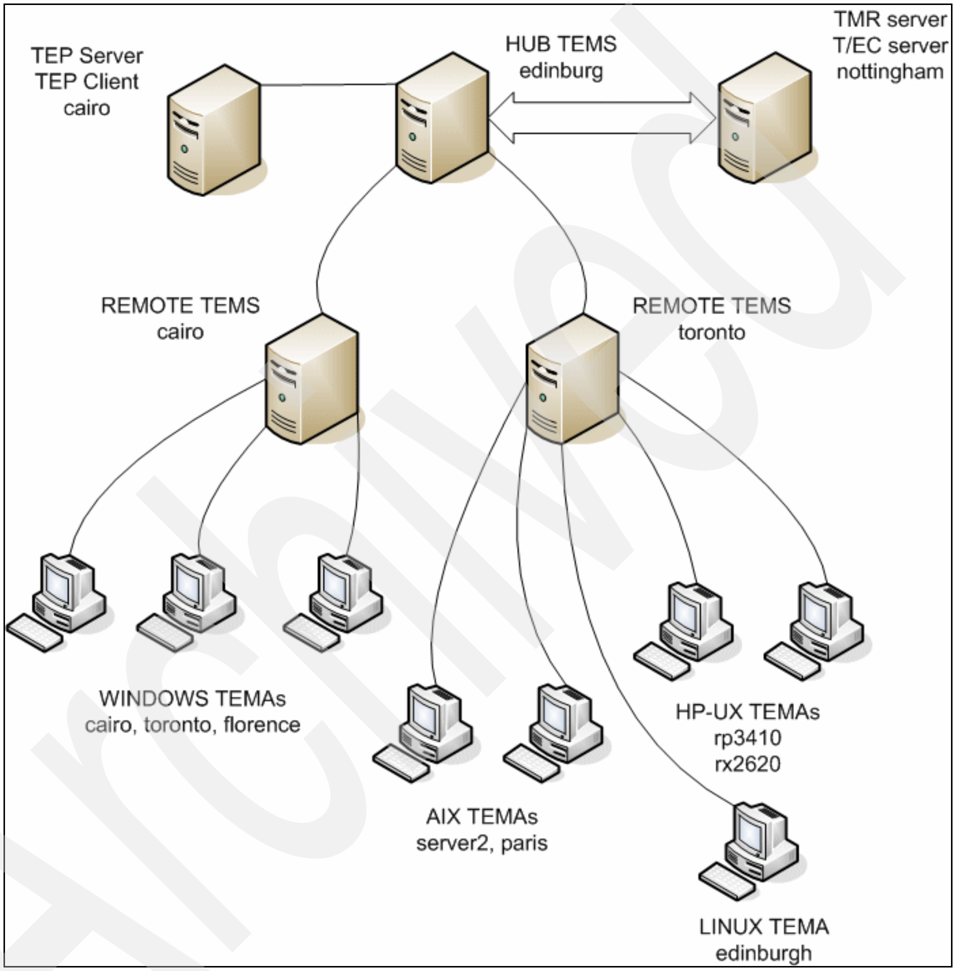


Figure 4-2 IBM Tivoli Monitoring V6.2 environment

4.3 Upgrading your IBM Tivoli Monitoring V5.1.2 environment

In this section, we describe the sequence of steps required to perform the upgrade from IBM Tivoli Monitoring V5.1.2 (also referred to as V5) to IBM Tivoli Monitoring V6.2 (also referred to as V6), which consists of migrating the V5 resources to V6 resources.

This is accomplished using a migration toolkit that is detailed in 4.4, “IBM Tivoli Monitoring Migration Toolkit” on page 191.

We also provide an overview of the two monitoring infrastructures, comparing them from the architectural and operational point of view.

4.3.1 Comparing the infrastructures from an architectural point of view

Let us start our discussion by comparing the IBM Tivoli Monitoring V5.1.2 architecture with IBM Tivoli Monitoring V6.2.

- Tivoli Management Framework

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

- Tivoli Monitoring Services

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

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

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

- Security
- Data transfer and storage
- Mechanisms for notification
- Installer
- User interface presentation

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

Figure 4-3 shows a comparison of the infrastructural elements of the two architectures.

On the left hand side, you see an IBM Tivoli Monitoring V5.1.2 environment based on the Tivoli Management Framework architecture; on the right hand side, you see the IBM Tivoli Monitoring V6.2 environment that uses the so called Tivoli Monitoring Services architecture.

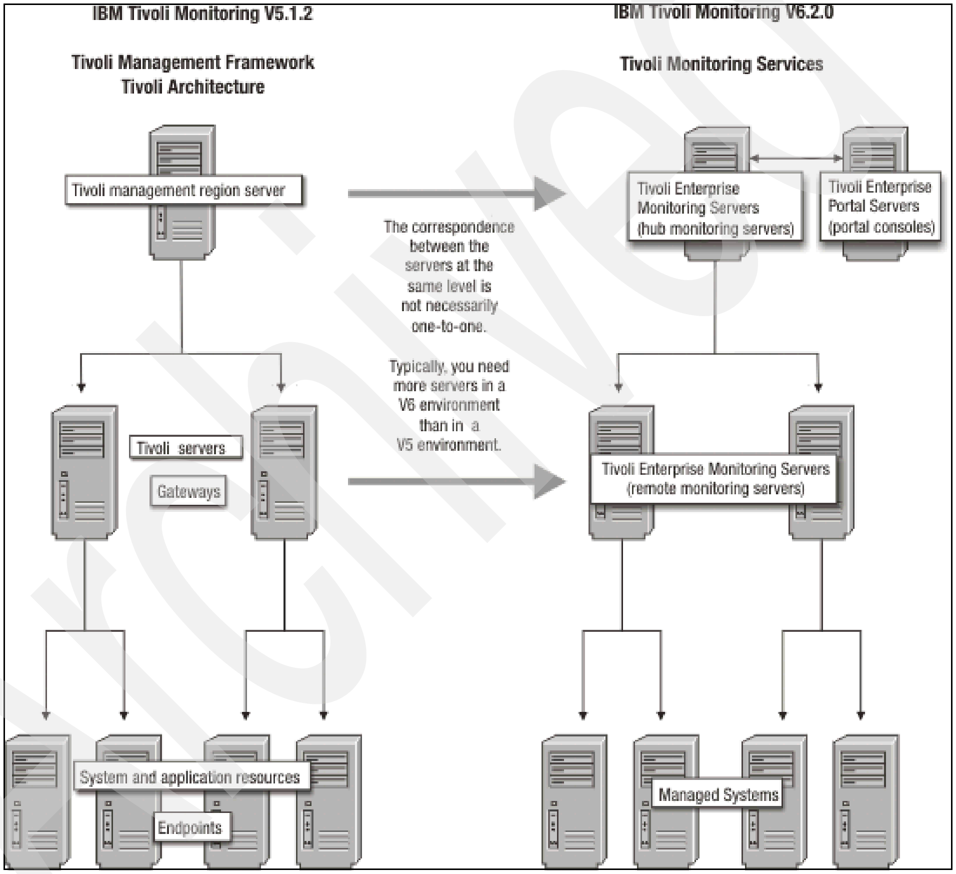

IBM Tivoli Monitoring V5.1.2
Tivoli Management Framework
Tivoli Architecture
IBM Tivoli Monitoring V6.2.0
Tivoli Monitoring Services
Tivoli management region server
Tivoli Enterprise Monitoring Servers (hub monitoring servers)
Tivoli Enterprise Portal Servers (portal consoles)
The correspondence between the servers at the same level is not necessarily one-to-one.
Typically, you need more servers in a V6 environment than in a V5 environment.
Tivoli servers
Gateways
Tivoli Enterprise Monitoring Servers (remote monitoring servers)
System and application resources
Endpoints
Managed Systems

Figure 4-3 Comparison of a Version 5.1.2 and Version 6.2.0 architecture

- Top layer

  Table 4-1 shows a comparison of the top layer components.

Table 4-1 Top layer components comparison

Tivoli Management Region (TMR) server and other Tivoli servers	**Hub Tivoli Enterprise Monitoring Server (hub monitoring server) and Tivoli Enterprise Portal Server**
In the Tivoli architecture, the Tivoli Management Region server is the central point of control.	In V6, the hub Tivoli Enterprise Monitoring Server and the Tivoli Enterprise Portal Server share this role. The monitoring server provides for security and authentication, message and event notification, the installer, and central storage of data that is collected from monitored systems. The portal server is responsible mainly for user interface presentation. You can connect more than one portal server to a hub monitoring server, but V6 communications can only use one of them. The monitoring server are capable of offering all or most of the same infrastructure services as those provided by the Tivoli Management Region server, but not necessarily in the corresponding level. For example, from the Tivoli Management Region server, an administrator can authorize other Tivoli servers to install the Tivoli desktop or to install Tivoli Management Framework products. In the V6 architecture, middle-level monitoring servers (called remote monitoring server) do not have this broad capability. Infrastructure services are centered mostly in the hub monitoring server and portal server at the top of the hierarchy.

- Middle layer

  Table 4-2 shows the comparison of the middle layer components.

Table 4-2 Middle layer components comparison

Tivoli gateways	**Remote Tivoli Enterprise Monitoring Servers (remote monitoring servers)**
In the Tivoli architecture, Tivoli gateways provide distributed control and infrastructure services.	A hub monitoring server is connected to one or more remote monitoring servers. The remote monitoring server performs a function similar to that of a Tivoli gateway: by serving a limited number of monitored systems, it reduces the data processing load of the hub monitoring server. However, a remote monitoring server performs more processing functions than a gateway, and so cannot support the same number of endpoints. When your infrastructure is being assessed, a scaling algorithm determines how many remote monitoring servers are required, and which endpoints will be served by them.

Note: These servers are normally installed remotely from the hub monitoring server, on a separate physical computer, and are normally called remote monitoring servers. However, if you have a small enough environment where the hub monitoring server can service all of the endpoints without needing a remote monitoring server, you do not need to install a remote server, but your baseline file must contain the definition for both the HubServer and the Server that, in this case, will point to the same physical system. Refer to “Viewing and editing the baseline file” on page 201 for more details.

- Bottom layer

Table 4-3 on page 167 shows the bottom layer components comparison.

Table 4-3 Bottom layer components comparison

System and application resources on endpoints	Managed systems
In V5, the targets of the monitoring software are referred to as system and application resources. Monitored system and application resources reside mainly on endpoints. They can also reside on Tivoli servers.	In V6, the targets of the monitoring software are referred to as managed systems. A managed system is a system, subsystem, application, or other entity that the product is monitoring and managing, not just a physical endpoint. IBM Tivoli Monitoring product components, such as the hub and remote monitoring server, can also be managed systems.

Monitoring agents and managed systems

In V6, Tivoli Enterprise Monitoring Agents (or monitoring agents) collect information from managed systems. A managed system is an operating system, application, or other entity that the product is monitoring and managing. The information that a monitoring agent collects is data that is useful in measuring the performance and availability of the managed system.

Monitoring agents are of two types:

- OS monitoring agents

  Monitoring agents that monitor operating systems, called OS monitoring agents, are a special category of monitoring agents. An OS monitoring agent monitors the operating system attributes, such as available disk space, the amount of memory usage, or process and processor information.

- Application monitoring agents

  Application agents monitor entities other than operating systems. Application monitoring agents are included with the products that run on the V6 base. For example, the IBM Tivoli Monitoring V6 for Databases product includes a DB2 monitoring agent.

Each agent is capable on its own of performing the data collection activity and communicating the result to its monitoring server. However, when more than one agent is installed on a physical computer, the architecture ensures that there is no redundancy. For example, in Figure 4-4, an OS agent and three application agents have been installed on a physical computer. When the first agent was installed, the communications infrastructure module, known as Tivoli Enterprise Monitoring Agent Framework, was also installed.

When subsequent agents were installed, the installation detected that the infrastructure module was already present and did not install it again.

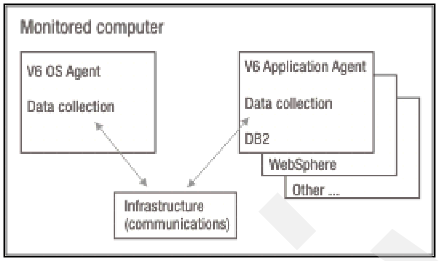


Figure 4-4 Monitoring agents and managed systems

In the above example, each monitoring agent collects data from one managed system and is installed on the same computer. However, some agents (for example, SAP R/3® agents) can monitor multiple systems remotely from a different computer.

Each monitored computer often contains several monitoring agents. The monitoring agents send their collected data to be displayed in table and chart views in the Tivoli Enterprise Portal (the user interface).

In a large enterprise, a remote monitoring server distributes the network load resulting from the communications of multiple monitoring agents on many systems.

4.3.2 Comparing the infrastructures from an operational point of view

In this section, we first compare the monitoring logic in V5 and V6, and then we compare some of the common operations.

Monitoring software has the following fundamental goals:

1. Collect data from monitored resources.
2. Determine if there is a problem.

3. Provide features that help an administrator respond to and resolve the problem.

Figure 4-5 compares the components used to achieve the first two goals in V5 and in V6.

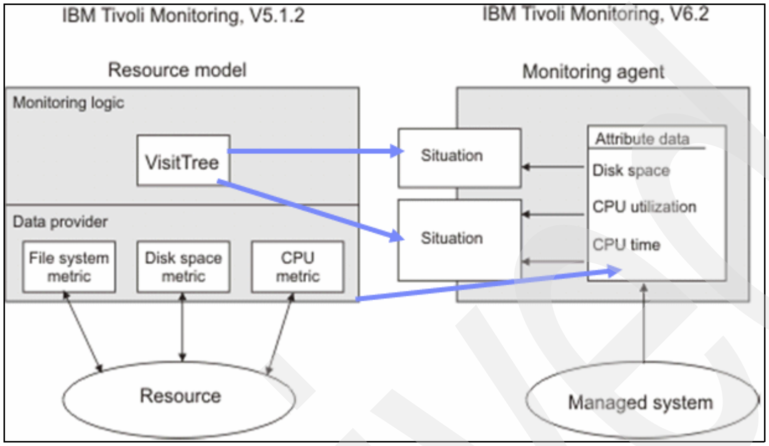


Figure 4-5 Logic comparison between V5 and V6

Table 4-4 introduces a high level comparison between the concept of a resource model for IBM Tivoli Monitoring V5.1.2 and the corresponding concept of a monitoring agent and situation for IBM Tivoli Monitoring V6.2.

Table 4-4 Resource model versus monitoring agents and situations

Resource model	**Monitoring agent and situations**
In V5, multiple resource models perform the job of both data collection and problem determination. Each resource model is defined for a single resource. It is divided into two parts: the monitoring logic and the data provider, the latter containing the metric information needed to determine what data needs to be collected. The resource model processes this data in the VisitTree to determine if an action needs to be taken (such as run a script or send an event).	In V6, the job of data collection and problem determination is divided between two entities: ► A monitoring agent collects information about the attributes of a particular managed system. ► Multiple situations hosted by the agent use the collected attribute data to determine if there are problems.

Discovering and responding to problems

A main goal of systems monitoring software is to assist the administrator in discovering and responding to problems. To accomplish this goal, both V5 and V6 provide:

- Means of notification, such as e-mail and Tivoli Enterprise Console events.
- A way of classifying problems so the user can separate critical problems from less severe problems.
- Automated responses to fix a problem, for example, running a program when a threshold is reached.

The sections that follow compare how these features are implemented in V5 and in V6.

Low disk space scenario

Imagine that you are a system administrator responsible for making sure that all Windows systems within your domain are running smoothly. One of the resources that you track is the free disk space. You want to know when the following system conditions occur:

- Disk space falls between 5% and 10% on any system. You want the monitoring software to respond to this serious, but not critical, condition by sending an alert event and by automatically running Script A. Script A empties the recycle bin and temporary directories.
- Disk space falls below 5% on any system. You want the monitoring software to respond to this critical condition by sending an alert event and by automatically running Script B. Script B empties the recycle bin, temporary directories, and other non-essential directories.

Responding to low disk space in V5 (Figure 4-6 on page 171) shows how you can achieve the results you want for the disk space scenario with a single resource model in V5.

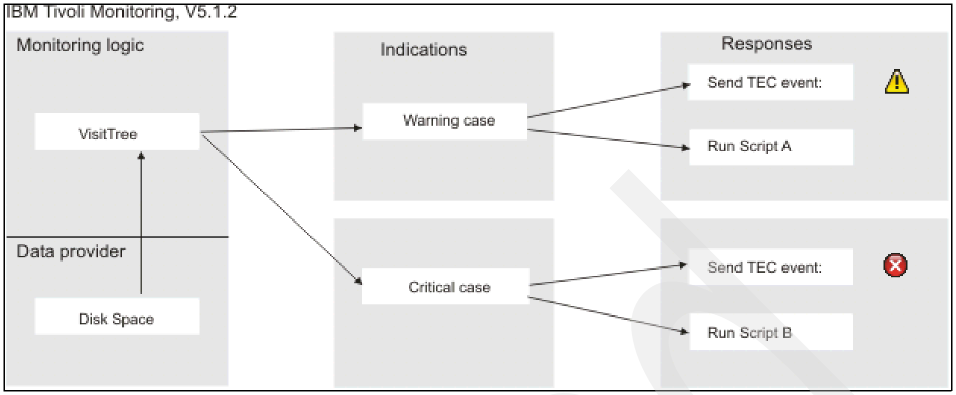


Figure 4-6 Disk space scenario in IBM Tivoli Monitoring V5.1.2

In V5, a resource model has a set of indications, each one of which responds to a specific condition with a specific set of responses. A variety of notifications can be sent, and scripts can be run. To handle the disk space scenario, you can create a single resource model with two different indications:

1. Select the warning indication and specify less than 10 percent free disk space as the threshold. Then specify the responses for this indication: A "warning" alert event (yellow triangle with the exclamation mark) is sent to the Tivoli Enterprise Console and Script A is run.
2. Select the critical indication and specify less than 5 percent disk space as the threshold. Then specify the responses for this indication: A "critical" alert event (red circle with the x) is sent to the Tivoli Enterprise Console server, and Script B is run.

Responding to low disk space in V6

Figure 4-7 shows how you can achieve the results you want for the disk space scenario with two situations in V6.

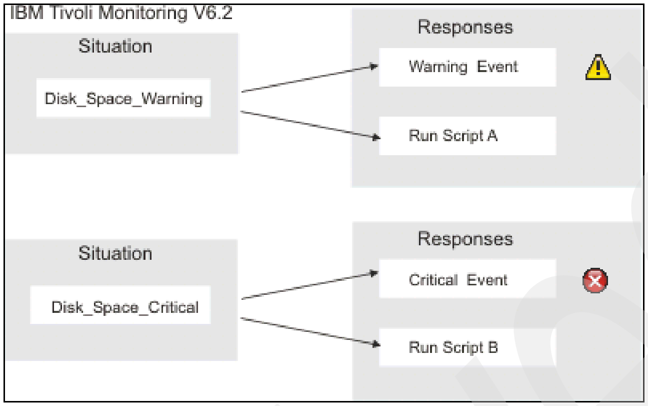


Figure 4-7 Disk space scenario IBM Tivoli Monitoring V6.2

In V5, a single resource model can have multiple thresholds and indications, with a different set of responses for each indication. V6 situations, on the other hand, do not have indications. A situation is a formula that evaluates to true or false. When you create a situation, you can specify a set of responses to take place when the situation becomes true.

To handle the disk space scenario, you can create different situations, each with its own set of responses:

1. The following situation, named DiskSpace_Warning, becomes true when disk space is between 5% and 10% on any managed system to which the situation is distributed:

   ```
   (VALUE (% Free) >= 5) AND (VALUE (% Free) <= 10)
   ```

   You can specify that when this situation becomes true, the following responses take place:

   – A warning event is sent to the Tivoli Enterprise Portal, which displays a warning alert indicator in the Navigator. The Navigator is the navigation tree that you see in the left pane of the Tivoli Enterprise Portal.

   > **Note:** To display alert indicators in the Navigator, you must associate the situation with Navigator items

   The Warning indicators are displayed over icons that represent managed systems where disk space has fallen between 5% and 10%.

   - Script A runs on these managed systems.

2. The following situation, named DiskSpace_Critical, becomes true when disk space falls below 5% on any managed system to which the situation is distributed:

   ```
   VALUE (% Free) < 5
   ```

   You can specify that when this situation becomes true, the following responses take place:

   - A critical event is sent to the Tivoli Enterprise Portal, which displays a Critical alert indicator in the Navigator. The Critical indicators are displayed over icons that represent Windows managed systems where disk space has fallen below 5%.
   - Script B runs on these managed systems.

Comparing the responses

We can compare the responses, as shown in Table 4-5.

A resource model in IBM Tivoli Monitoring V5.1.2 has various indications, each of which has a set of responses. The response is triggered by the indication logic. Responses in IBM Tivoli Monitoring V6.2 take place when a situation becomes true.

Table 4-5 Response comparison in V5 and V6

IBM Tivoli Monitoring V5.1.2	IBM Tivoli Monitoring V6.2
Send an event to an IBM Tivoli Enterprise Console server. You can specify the severity of the event and to which server to send the event.	Send an event to an IBM Tivoli Enterprise Console server. You can specify the severity of the event and to which server to send the event.

IBM Tivoli Monitoring V5.1.2	IBM Tivoli Monitoring V6.2
Send an e-mail to one or more recipients.	Do either of the following (but not both): ► Send a message to the Universal Message Console. The Universal Message Console is a view that you add to the Tivoli Enterprise Portal workspace. It displays messages generated by situation and policy activities. In addition to the message text, you can specify an event severity and include attribute values in the message ► Run a system command (called a Take Action command) on the managed system. The command can be a single action or a script containing several commands. You can specify any command that helps to resolve the problem, such as logging information or stopping a job that is overusing resources
Post a message to a Tivoli notice group.	
Run a local or remote program, such as a C program or shell script.	
Run a specified task from a Tivoli task library.	
Log a message to a local or remote file.	
N/A.	Display a situation event indicator icon when a situation becomes true. The available event indicator icons reflect the severity of the situation event
N/A.	Play a sound when the event indicator icon is displayed

Comparing situation events and Tivoli Enterprise Console events

This section discusses situation events and Tivoli Enterprise Console events.

Situation events

The Tivoli Enterprise Portal events discussed in the previous section are also called situation events. A situation event is an internal event record that Tivoli Enterprise Portal always opens when a situation becomes true. If associated with a Navigator item, a situation event can have a severity or state of:

- Fatal
- Critical
- Minor
- Warning
- Informational

- Unknown

Event indicators overlay items (nodes) in the Navigator. The Navigator (or Navigator view) is an expandable navigation tree in the left pane of the Tivoli Enterprise Portal window like the one shown in Figure 4-8.

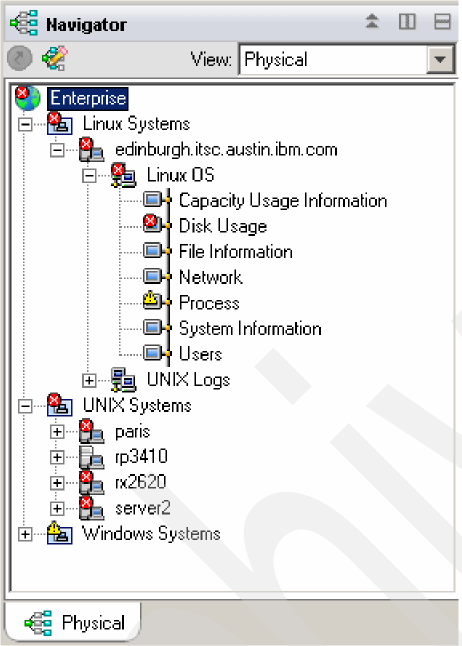


Figure 4-8 Navigator view showing a true situation

The above example shows a Linux computer named edinburgh.itsc.ausin.ibm.com that has a Linux OS agent that monitors various attributes of the system.

In the above example, there are events with two level of severity: Warning and Critical. However, as you move up the Navigator hierarchy, the events are consolidated to show only the indicator of the highest severity.

You can move your mouse pointer over any event indicator to open a fly-over window that lists all the situations that caused the events at that level of the Navigator and below. The fly-over window also shows the managed systems where the events occurred, the date and time of events, and other information.

Events also have a status, which indicates what user intervention has taken place, if any, toward resolving the problem. Details of situation events, such as event severity and status, the name of the situation that triggered the event, and the name of the system where the situation is running, are listed in Situation Event Console views.

Tivoli Enterprise Console events

Another response you can enable for a situation is to send a Tivoli Enterprise Console event to a Tivoli Enterprise Console server. Unlike situation events, which are always opened when a situation becomes true, the sending of Tivoli Enterprise Console events is optional. You can specify any of the Tivoli Enterprise Console severities for the event. Tivoli Enterprise Console events are almost identical in number and meaning to Situation events. The default mapping of these events to the Tivoli Enterprise Portal events is described in Table 4-6.

Table 4-6 Mapping of events

Tivoli Enterprise Portal (situation) events	Tivoli Enterprise Console events
Minor	MINOR
Warning	WARNING
N/A	HARMLESS
Informational	INFORMATIONAL
Unknown	UNKNOWN

This is the default mapping. But you can reconfigure this based on your needs.

Comparing the monitoring schedules

In IBM Tivoli Monitoring V5.1.2, the monitoring schedule controls when and how often a resource model performs the monitoring of a system or application resource. You set schedules for individual resource models. When you set a schedule, you can specify:

- A start date and time and stop date and time for the schedule.
- The monitoring frequency. The monitoring frequency specifies how often the resource model collects data and compares it to a threshold. The default monitoring frequency is hourly. The maximum is once per minute.
- A set of rules that define restrictions, preventing the monitoring from being performed when they are in force.

When you create a situation in IBM Tivoli Monitoring V6.2, you specify a sampling interval, similar to the monitoring frequency in IBM Tivoli Monitoring

V5.1.2. The sampling interval specifies how often the monitoring server requests data from the monitoring agent and compares the returned values against the situation. The default sampling interval is 15 minutes. The maximum is once every 30 seconds. A sampling interval can also be expressed in days, for example, once every 7 days. You can specify a sampling interval for individual situations only.

There are two ways that you can implement a date and time schedule for situations in IBM Tivoli Monitoring V6.2:

- You can set up a policy workflow in which situations that are true only on specified days and times are used to start or stop situations that monitor system conditions.
- You can embed situations that evaluate to true on specified days and times. You can create new situations or you can use predefined situations that V6 provides to set day and time constraints.

  For example, the following situation can be embedded in any situation that you do not want to run on Sundays when the computer is being serviced:

  ```
  (Day Of Week! = ’Sunday’)
  ```

  The Not_Sunday situation is embedded in the Windows_Services_Start situation, which uses the attributes Start Type and Current State:

  ```
  ( Start Type == ’Automatic’ AND Current State == ’Stopped’ AND
  SIT(Not_Sunday) == True )
  ```

4.3.3 Comparing the infrastructures from a distribution point of view

In this section, we compare the distribution mechanism between IBM Tivoli Monitoring V5.1.2 and IBM Tivoli Monitoring V6.2.

Distribution in IBM Tivoli Monitoring V5.1.2

In IBM Tivoli Monitoring V5.1.2, multiple resource models are contained in profiles. Profiles are owned by profile managers. You distribute resource models within a profile by distributing the profile to the subscribers of the profile manager that owns the profile. Subscribers to a profile manager can include application objects, endpoints, or other profile managers.

Figure 4-9 shows an example of how subscribers can be organized in a multi-level distribution hierarchy that enables different administrative teams to target specific types of system and application resources within the enterprise. A team that monitors operating systems can distribute OS resource models, which belong to the OS profile manager at the top of the hierarchy, to all systems in the enterprise. Another team monitors only Enterprise Resource Monitoring (ERP) applications. A third team is responsible only for databases. Because you can restrict which team has access to each profile manager, each team can operate independently of the others. The position of a profile manager in the hierarchy does not determine access. It only determines how resource models are distributed.

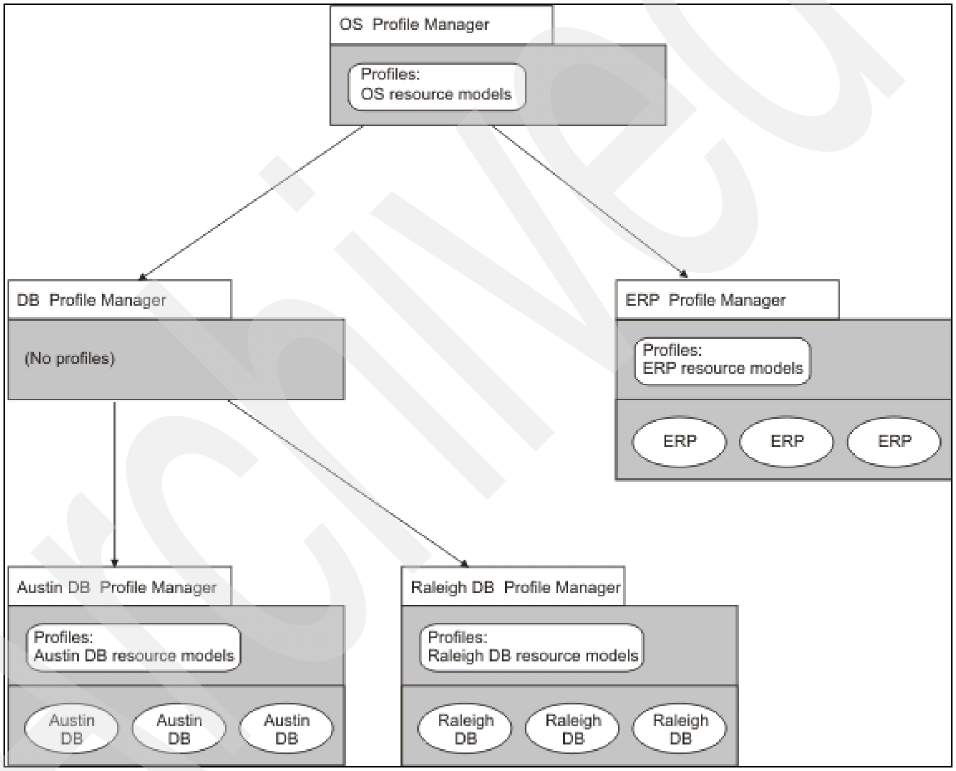


Figure 4-9 Distribution flow in IBM Tivoli Monitoring V5.1.2

The Austin DB profile manager and the Raleigh DB profile manager subscribe to the DB profile manager rather than directly to the OS profile manager. The intervening DB profile manager makes it possible for the database team to organize and manage the profile managers at the bottom of the hierarchy without needing access to the OS profile manager. For example, they can add a Los

Angeles DB profile manager. The database team can also add profiles to the DB profile manager to be distributed to all of the subscribing profile managers.

Distribution in IBM Tivoli Monitoring V6.2

In IBM Tivoli Monitoring V6.2, you can distribute a situation to one or more managed systems or managed system lists, as shown in Figure 4-10. A managed system list contains one or more managed systems that are monitored by the same type of monitoring agent. (For example, a managed system list can include Windows systems but not both Windows and UNIX systems.) The managed system list is a grouping mechanism that enables an administrator to distribute a situation to many managed systems quickly. Unlike IBM Tivoli Monitoring V5.1.2 resource models, which must be redistributed every time the resource models are updated, changes to a situation take effect automatically on the managed systems to which it has already been distributed. You can use managed system lists to emulate a single level of nesting of IBM Tivoli Monitoring V5.1.2 profile managers.

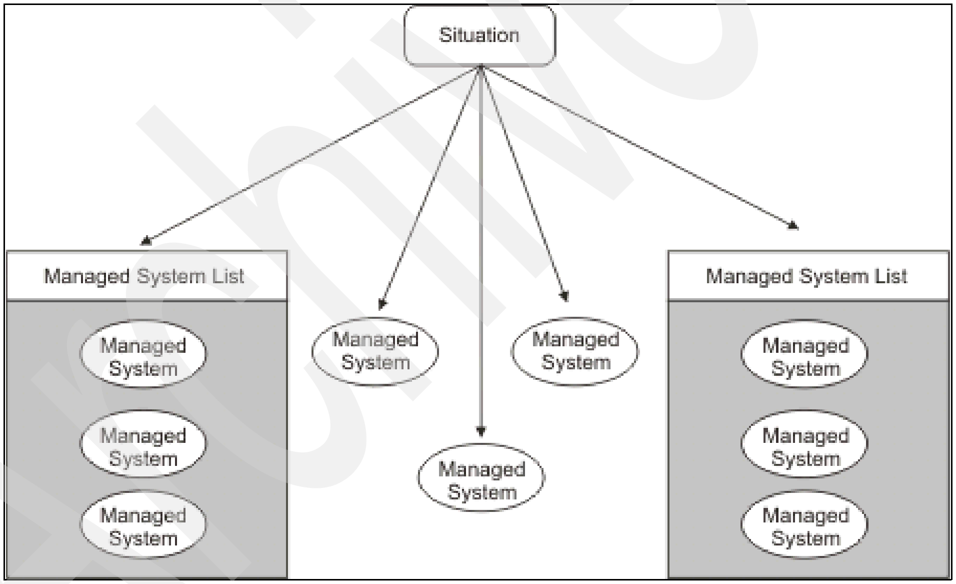


Figure 4-10 Distribution flow in IBM Tivoli Monitoring V6.2

4.3.4 Installing the migration toolkit

The migration toolkit is packaged like any other Tivoli product, so its installation is pretty straightforward.

Example 4-1 shows a sample installation directory outlook.

Example 4-1 Migration toolkit installation directory

```
After unpacked the installation file you will have a directory
structure similar to the following:

C:\Documents and Settings\salustri\Desktop\MTK>dir
 Volume in drive C has no label.
 Volume Serial Number is 046B-C174

 Directory of C:\Documents and Settings\salustri\Desktop\MTK

10/05/2007  01:31 PM    <DIR>          .
10/05/2007  01:31 PM    <DIR>          ..
10/05/2007  01:25 PM    <DIR>          CFG
08/08/2007  10:01 AM                61 CONTENTS.LST
08/08/2007  10:01 AM         8,920,131 FILE1.PKT
08/08/2007  10:01 AM            36,105 FILE10.PKT
08/08/2007  10:01 AM            36,093 FILE11.PKT
08/08/2007  10:01 AM            36,031 FILE12.PKT
08/08/2007  10:01 AM            36,065 FILE13.PKT
08/08/2007  10:01 AM            36,008 FILE14.PKT
08/08/2007  10:01 AM            94,855 FILE15.PKT
08/08/2007  10:01 AM           948,853 FILE2.PKT
08/08/2007  10:01 AM           573,017 FILE3.PKT
08/08/2007  10:01 AM           938,911 FILE4.PKT
08/08/2007  10:01 AM           949,552 FILE5.PKT
08/08/2007  10:01 AM           854,895 FILE6.PKT
08/08/2007  10:01 AM           871,809 FILE7.PKT
08/08/2007  10:01 AM            16,754 FILE8.PKT
08/08/2007  10:01 AM            36,005 FILE9.PKT
08/08/2007  10:01 AM             1,470 MTK.IND
10/05/2007  01:24 PM    <DIR>          samples
10/05/2007  01:24 PM    <DIR>          schema
```

Prerequisites

Before installing the migration toolkit on you system, you should make sure that some prerequisites are met.

As indicated in the MTK.IND file, the migration toolkit depends on these products:

- mtk:depends:TMF_3.7.1
- mtk:depends:5.1.2-ITM-FP10

This means that you should have at least Tivoli Management Framework 3.7.1 or above and IBM Tivoli Monitoring 5.1.2 Fix Pack 10 or above.

For details regarding the operating systems that support the toolkit installation, refers to "Software and hardware requirements" in *Upgrading from IBM Tivoli Monitoring V5.1.2*, GC32-1976

Example 4-2 shows some commands used to check for the installation prerequisites in our environment.

Example 4-2 Prerequisites check

```
Framework version 3.7 or higher:

C:\>wlsinst -p |grep Framework
Tivoli Management Framework 4.1.1
Tivoli Java Client Framework 4.1.1

IBM JRE 1.4.2 or 1.5.0 provided with ITM 6.2:

C:\WINDOWS>java -fullversion
java full version "J2RE 1.5.0 IBM Windows 32 build pwi32devifx-20070706
(SR5 + IZ00983)"

ITM 5.1.2 fix pack 10 or higher:

C:\WINDOWS>wlsinst -ah|grep Monitoring
IBM Tivoli Monitoring - Gathering Historical Data Component, Version
5.1.2
IBM Tivoli Monitoring - Tivoli Enterprise Data Warehouse Support,
Version 5.1.2
IBM Tivoli Monitoring, Version 5.1.2
IBM Tivoli Monitoring Migration Toolkit - V5.1.2 to V6.2
IBM Tivoli Monitoring, Version 5.1.2 - fix pack 13
IBM Tivoli Monitoring Gathering Historical Data Component, Version
5.1.2 - fix pack 13
IBM Tivoli Monitoring Tivoli Enterprise Data Warehouse Support, Version
5.1.2 - fix pack 13

Tivoli Administrator roles requirements (super, senior, admin, user):

C:\WINDOWS>wgetadmin
Administrator:  Root_cairo-region
logins: CAIRO\Administrator@cairo.itsc.austin.ibm.com
roles:  global  backup, restore, Query_view, Query_execute, Query_edit,
RIM_view, RIM_update, HTTP_Control, Dist_control, Inventory_
```

```
view, Inventory_scan, Inventory_edit, Inventory_end_user, APM_Manage,
APM_Edit, APM_Admin, APM_View, policy, install_product, instal
l_client, user, admin, senior, super
        security_group_any_admin        user
        Root_cairo-region       admin, user, rconnect
notice groups:  TME Administration, TME Authorization, TME Diagnostics,
TME Scheduler, Inventory
```

Where to install the migration toolkit

The migration toolkit must be installed on every Tivoli Management Region server and gateway to be migrated, or those that are in the Tivoli Management Framework structure of endpoints to be migrated.

Note: The migration toolkit commands are only run from the Tivoli Management Region server, but the migration toolkit must be present on all of the gateways involved in the migration.

Installing the migration toolkit

As with any other Tivoli product, there are several ways to install it:

- Using IBM Tivoli Configuration Manager
- Using Tivoli Desktop
- Using Tivoli CLI

The method described for this book is the CLI one.

Example 4-3 shows the sequence of commands used to perform the installation in our test environment.

Example 4-3 Installing the migration toolkit

```
Before start the installation is suggested to run a backup of your
environment.

With a simple Tivoli backup, you can restore, in case of failures, a
previous Tivoli Management Framework database not containing the
migration toolkit product registration.
A Tivoli backup only is not enough to restore the binaries situation in
case of failure, so it’s your choise to either make a Tivoli backup
only or both Tivoli and installation directories backups.

Backup the Tivoli Management Framework database.
```

```
First make sure that the Tivoli environment is set by running the
setup_env.cmd script:

C:\WINDOWS\system32\drivers\etc\Tivoli>setup_env.cmd
C:\WINDOWS\SYSTEM32\DRIVERS\ETC\Tivoli\tmrset.txt
C:\Tivoli\db\cairo.db\region.out
        1 file(s) copied.
Tivoli environment variables configured.

C:\>wbkupdb

Starting the snapshot of the database files for cairo...
............................................................
............................................................
................
Starting the snapshot of the database files for toronto...
.............

Backup Complete.

Installation sintax using CLI:

First untar the installation image, once done, you can use the winstall
cli with the parameters indicated in the below example.
Note: Make sure to use the tar command provided with the Tivoli
Management Region server to untar the image and avoid the installation
image corruption that can occur while using other tools like WinZip.

C:\MTK>winstall -c "c:\MTK" -i MTK -y cairo toronto
MtkJavaDir="C:\Program Files\IBM\Java50\jre\bin"
Checking product dependencies...
 Patch 5.1.2-ITM-FP10 is already installed as needed.
  Product TMF_3.7.1 is already installed as needed.
 Dependency check completed.
Inspecting node cairo...
Inspecting node toronto...
Installing Product: IBM Tivoli Monitoring Migration Toolkit - V5.1.2 to
V6.2

Unless you cancel, the following operations will be executed:
  For the machines in the independent class:
    hosts: cairo, toronto
   need to copy the GBIN (generic) to:
         C:/Tivoli/bin/generic_unix
   need to copy the CAT (generic) to:
         C:/Tivoli/msg_cat
   need to copy the LCFNEW (generic) to:
         C:/Tivoli/bin/lcf_bundle.40
   need to copy the GBIN (generic) to:
         c:/Tivoli/bin/generic_unix
   need to copy the CAT (generic) to:
         c:/Tivoli/msg_cat
   need to copy the LCFNEW (generic) to:
         c:/Tivoli/bin/lcf_bundle.40

  For the machines in the w32-ix86 class:
    hosts: cairo, toronto
   need to copy the BIN (w32-ix86) to:
         C:/Tivoli/bin/w32-ix86
   need to copy the ALIDB (w32-ix86) to:
         C:/Tivoli/db/cairo.db
   need to copy the BIN (w32-ix86) to:
         c:/Tivoli/bin/w32-ix86

Creating product installation description object...Created.
Executing queued operation(s)
Distributing machine independent Generic Binaries --> cairo
 Product install completed successfully.
 Completed.

Distributing architecture specific Binaries --> cairo
 . Completed.

Distributing machine independent Message Catalogs --> cairo
  Completed.

Distributing architecture specific Server Database --> cairo
 .......Product install completed successfully.
AMKUT0052I The Java path was verified and stored.
 Completed.

Distributing machine independent LCF Images (new version) --> cairo
 . Completed.

Distributing machine independent Generic Binaries --> toronto
 .Product install completed successfully.
 Completed.

Distributing architecture specific Binaries --> toronto
 . Completed.
```

```
Distributing machine independent Message Catalogs --> toronto
  Completed.

Distributing machine independent LCF Images (new version) --> toronto
 . Completed.

Registering product installation attributes...Registered.

Finished product installation.

We selected cairo and toronto managed nodes cause they are both
gateways hosting Tivoli Management Agents with running IBM Tivoli
Monitoring 5.1.2 resource models that we want to migrate with the
migration toolkit.

Once the installation is complete, you can check its succesfull
registration by running this command:

C:\WINDOWS>wlsinst -p|grep -i toolkit
IBM Tivoli Monitoring Migration Toolkit - V5.1.2 to V6.2
```

Components added by the installation

The migration toolkit installation creates some new resources in your Tivoli Management Framework database:

- New classes

  A new distinguished resource is created:

  ```
  C:\>wlookup -a |grep MTK
  ```

  ```
  ITMMTKUpgradeITMManager
  1713357986.1.1110#TMF_SysAdmin::InstanceManager#
  ```

  This is the class responsible for managing the upgrade of the endpoints.

  ```
  C:\>wlookup -ar Classes |grep -i mtk
  ```

  ```
  ITMMTKUpgradeITMManagerEPA
  1713357986.1.1111#TMF_SysAdmin::InstanceManager#
  ```

  This is the class responsible for the downcall handler related to the OS Agent upgrades.

- New methods and attributes

  The above object add some methods and attributes that you can view with the following command:

  ```
  C:\>objcall 1713357986.1.1110#TMF_SysAdmin::InstanceManager#
  contents
  ```

  Example 4-4 lists the attributes and methods belonging to the ITMMTKUpgradeITMManager object.

Example 4-4 Attributes and methods added by ITMMTKUpgradeITMManager

```
C:\>wlookup ITMMTKUpgradeITMManager
1713357986.1.1110#TMF_SysAdmin::InstanceManager#

C:\>objcall 1713357986.1.1110#TMF_SysAdmin::InstanceManager# contents
ATTRIBUTE:_BOA_id
ATTRIBUTE:actions
ATTRIBUTE:behavior
ATTRIBUTE:class_objid
ATTRIBUTE:class_type
ATTRIBUTE:collections
ATTRIBUTE:debug
ATTRIBUTE:def_policies
ATTRIBUTE:dialog
ATTRIBUTE:extension
ATTRIBUTE:filters
ATTRIBUTE:impl_name
ATTRIBUTE:impl_type
ATTRIBUTE:indirect
ATTRIBUTE:initialized
ATTRIBUTE:interfaces
ATTRIBUTE:jdir
ATTRIBUTE:label
ATTRIBUTE:members
ATTRIBUTE:pres_object
ATTRIBUTE:pro
ATTRIBUTE:pro_name
ATTRIBUTE:prototypes
ATTRIBUTE:resource_host
ATTRIBUTE:skeleton
ATTRIBUTE:sort_name
ATTRIBUTE:state
ATTRIBUTE:val_policies
ATTRIBUTE:version
METHOD:_get_debug
```

```
METHOD:_get_jdir
METHOD:_set_debug
METHOD:_set_jdir
METHOD:assess
METHOD:scanTMR
```

- New Dependency Sets

  New dependencies are added to the DependencyMgr class, as shown in Example 4-5.

Example 4-5 Migration toolkit dependencies added to the DependencyMgr

```
To list the name of the dependencies you can run the following command:

C:\>wlookup -ar DependencyMgr|grep -i mtk
ITMMTKGetDataStore      1713357986.1.1115#Depends::Mgr#
ITMMTKInstallOSAgent    1713357986.1.1116#Depends::Mgr#

With these commands you can list the files associated to each
dependency that are sent to the endpoints when some methods are
invoked:

C:\>wdepset -v 1713357986.1.1115#Depends::Mgr#
aix4-r1:
bin/generic_unix/TME/ITMMTKUpgrade/ITMMTKUpgradeITMManager/java/data/getprofile
InfoMTK.sh,LCFNEW/AMK/bi

solaris2:
bin/generic_unix/TME/ITMMTKUpgrade/ITMMTKUpgradeITMManager/java/data/getprofile
InfoMTK.sh,LCFNEW/AMK/bi

hpux10:
bin/generic_unix/TME/ITMMTKUpgrade/ITMMTKUpgradeITMManager/java/data/getprofile
InfoMTK.sh,LCFNEW/AMK/bi

linux-ix86:
bin/generic_unix/TME/ITMMTKUpgrade/ITMMTKUpgradeITMManager/java/data/getprofile
InfoMTK.sh,LCFNEW/AMK/bi

linux-s390:
bin/generic_unix/TME/ITMMTKUpgrade/ITMMTKUpgradeITMManager/java/data/getprofile
InfoMTK.sh,LCFNEW/AMK/bi

linux-ppc:
bin/generic_unix/TME/ITMMTKUpgrade/ITMMTKUpgradeITMManager/java/data/getprofile
InfoMTK.sh,LCFNEW/AMK/bi
```

```
C:\>wdepset -v 1713357986.1.1116#Depends::Mgr#
aix4-r1:
bin/generic_unix/TME/ITMMTKUpgrade/ITMMTKUpgradeITMManager/java/data/createNode
.sh,LCFNEW/AMK/bin,8

solaris2:
bin/generic_unix/TME/ITMMTKUpgrade/ITMMTKUpgradeITMManager/java/data/createNode
.sh,LCFNEW/AMK/bin,8

hpux10:
bin/generic_unix/TME/ITMMTKUpgrade/ITMMTKUpgradeITMManager/java/data/createNode
.sh,LCFNEW/AMK/bin,8

linux-ix86:
bin/generic_unix/TME/ITMMTKUpgrade/ITMMTKUpgradeITMManager/java/data/createNode
.sh,LCFNEW/AMK/bin,8

linux-s390:
bin/generic_unix/TME/ITMMTKUpgrade/ITMMTKUpgradeITMManager/java/data/createNode
.sh,LCFNEW/AMK/bin,8

w32-ix86:
bin/generic_unix/TME/ITMMTKUpgrade/ITMMTKUpgradeITMManager/java/data/createNode
.sh,LCFNEW/AMK/bin,8
        bin/w32-ix86/tools/awk.exe,../../bin/w32-ix86/tools,8
        bin/w32-ix86/tools/bash.exe,../../bin/w32-ix86/tools,8
        bin/w32-ix86/tools/basename.exe,../../bin/w32-ix86/tools,8
        bin/w32-ix86/tools/cat.exe,../../bin/w32-ix86/tools,8
        bin/w32-ix86/tools/cmp.exe,../../bin/w32-ix86/tools,8
        bin/w32-ix86/tools/cp.exe,../../bin/w32-ix86/tools,8
        bin/w32-ix86/tools/cpp.exe,../../bin/w32-ix86/tools,8
        bin/w32-ix86/tools/cut.exe,../../bin/w32-ix86/tools,8

../lcf_bundle/bin/w32-ix86/tools/cygwinb19.dll,../../bin/w32-ix86/tools,8
        bin/w32-ix86/tools/cygwin1.dll,../../bin/w32-ix86/tools,8
        bin/w32-ix86/tools/date.exe,../../bin/w32-ix86/tools,8
        bin/w32-ix86/tools/dd.exe,../../bin/w32-ix86/tools,8
        bin/w32-ix86/tools/dirname.exe,../../bin/w32-ix86/tools,8
        bin/w32-ix86/tools/echo.exe,../../bin/w32-ix86/tools,8
        bin/w32-ix86/tools/egrep.exe,../../bin/w32-ix86/tools,8
        bin/w32-ix86/tools/env.exe,../../bin/w32-ix86/tools,8
        bin/w32-ix86/tools/expr.exe,../../bin/w32-ix86/tools,8
        bin/w32-ix86/tools/find.exe,../../bin/w32-ix86/tools,8
        bin/w32-ix86/tools/fgrep.exe,../../bin/w32-ix86/tools,8
        bin/w32-ix86/tools/getopt.exe,../../bin/w32-ix86/tools,8
        bin/w32-ix86/tools/grep.exe,../../bin/w32-ix86/tools,8
        bin/w32-ix86/tools/ls.exe,../../bin/w32-ix86/tools,8
        bin/w32-ix86/tools/mkdir.exe,../../bin/w32-ix86/tools,8
        bin/w32-ix86/tools/mv.exe,../../bin/w32-ix86/tools,8
        bin/w32-ix86/tools/ntprocinfo.exe,../../bin/w32-ix86/tools,8
        bin/w32-ix86/tools/ntfsinfo.exe,../../bin/w32-ix86/tools,8
        bin/w32-ix86/tools/perl.exe,../../bin/w32-ix86/tools,8
        bin/w32-ix86/tools/printenv.exe,../../bin/w32-ix86/tools,8
        bin/w32-ix86/tools/PSAPI.DLL,../../bin/w32-ix86/tools,8
        bin/w32-ix86/tools/pwd.exe,../../bin/w32-ix86/tools,8
        bin/w32-ix86/tools/rm.exe,../../bin/w32-ix86/tools,8
        bin/w32-ix86/tools/rmdir.exe,../../bin/w32-ix86/tools,8
        bin/w32-ix86/tools/sed.exe,../../bin/w32-ix86/tools,8
        bin/w32-ix86/tools/sh.exe,../../bin/w32-ix86/tools,8
        bin/w32-ix86/tools/slash.exe,../../bin/w32-ix86/tools,8
        bin/w32-ix86/tools/slashes.exe,../../bin/w32-ix86/tools,8
        bin/w32-ix86/tools/sleep.exe,../../bin/w32-ix86/tools,8
        bin/w32-ix86/tools/tail.exe,../../bin/w32-ix86/tools,8
        bin/w32-ix86/tools/tee.exe,../../bin/w32-ix86/tools,8
        bin/w32-ix86/tools/touch.exe,../../bin/w32-ix86/tools,8
        bin/w32-ix86/tools/tr.exe,../../bin/w32-ix86/tools,8
        bin/w32-ix86/tools/uname.exe,../../bin/w32-ix86/tools,8
        bin/w32-ix86/tools/tar.exe,../../bin/w32-ix86/tools,8
        bin/w32-ix86/tools/win32gnu.dll,../../bin/w32-ix86/tools,8
        bin/w32-ix86/tools/wc.exe,../../bin/w32-ix86/tools,8
        bin/w32-ix86/tools/xargs.exe,../../bin/w32-ix86/tools,8

linux-ppc:
bin/generic_unix/TME/ITMMTKUpgrade/ITMMTKUpgradeITMManager/java/data/createNode
.sh,LCFNEW/AMK/bin,8
```

- Uninstall object

  A new uninstall object named mtk is registered. It references an uninstall script at this location:

  `%BINDIR%\TME\ITMMTKUpgrade\ITMMTKUpgradeITMManager\rmmtk.sh`

  for Windows, or for UNIX based operating systems:

  `$BINDIR/TME/ITMMTKUpgrade/ITMMTKUpgradeITMManager/rmmtk.sh`

  This script is invoked when you run the **wuninst mtk** command to uninstall the migration toolkit.

- Directories used for the upgrade process

  As shown in Example 4-6, some directories are created and used later during the upgrade process.

Example 4-6 Directories created and used during the upgrade process

```
%DBDIR%\AMK
%DBDIR%\AMK\analyze
%DBDIR%\AMK\analyze\endpoints
%DBDIR%\AMK\analyze\profilemanagers
%DBDIR%\AMK\analyze\profiles
%DBDIR%\AMK\analyze\scans
%DBDIR%\AMK\analyze\scans\server
%DBDIR%\AMK\data
%DBDIR%\AMK\data\config
%DBDIR%\AMK\data\context
%DBDIR%\AMK\data\dictionaries
%DBDIR%\AMK\data\dictionaries\C
%DBDIR%\AMK\data\environments
%DBDIR%\AMK\data\gui
%DBDIR%\AMK\data\help
%DBDIR%\AMK\data\help\C
%DBDIR%\AMK\data\images
%DBDIR%\AMK\data\images\backup
%DBDIR%\AMK\data\mapping
%DBDIR%\AMK\data\scripts
%DBDIR%\AMK\data\styles
%DBDIR%\AMK\data\stylesheet
%DBDIR%\AMK\logs
%DBDIR%\AMK\temp
%DBDIR%\AMK\trace
```

- Mapping files

  Mapping files are used to map IBM Tivoli Monitoring V5.1.2 resource models to corresponding situations in IBM Tivoli Monitoring V6.2.

  They are located in this path for Windows:

  `%BINDIR%\..\generic_unix\TME\ITMMTKUpgrade\mapping`

  or in this path for UNIX based operating systems:

  `$BINDIR/../generic_unix/TME/ITMMTKUpgrade/mapping`

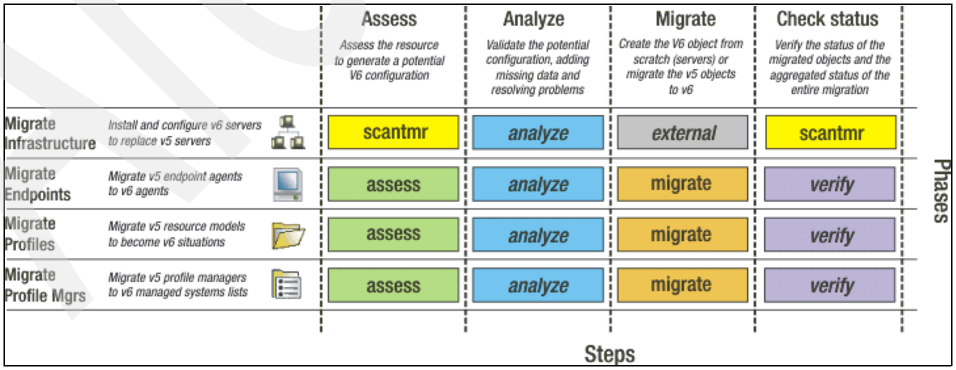
4.4 IBM Tivoli Monitoring Migration Toolkit

The upgrade tools and procedures are designed to transfer control to the new IBM Tivoli Monitoring V6.2 infrastructure while preserving the monitoring activity and monitored resources that are already in place; this way, there will not be a service disruption.

Let us briefly describe the main phases of the migration toolkit that will be then explained in the sections that follow:

- To enable IBM Tivoli Monitoring V6.2 to take over from IBM Tivoli Monitoring V5.1.2, the first requirement is to install a sufficient number of IBM Tivoli Monitoring V6.2 servers (hub and remote Tivoli Enterprise Monitoring Servers and Tivoli Enterprise Portal Servers) to handle the current monitoring requirements.
- The existing Tivoli endpoint systems, which host the monitored resources, can then be connected to the Tivoli Enterprise Monitoring Servers. Endpoints are connected to monitoring servers by deploying OS monitoring agents to the endpoints. The final result is that the endpoints become part of the IBM Tivoli Monitoring V6.2 environment. At the same time, however, they remain connected to the IBM Tivoli Monitoring V5.1.2 environment so that monitoring can continue until the old resource models are no longer needed.
- The next step is to replace the resource models in IBM Tivoli Monitoring V5.1.2 profiles with IBM Tivoli Monitoring V6.2 situations. Situations are associated with the appropriate monitoring agents and with lists of managed systems to be monitored. The managed system lists are created from the subscriber lists of profile managers.

Figure 4-11 shows the diagram of the phases and steps for the migration.



		Assess Assess the resource to generate a potential V6 configuration	Analyze Validate the potential configuration, adding missing data and resolving problems	Migrate Create the V6 object from scratch (servers) or migrate the v5 objects to v6	Check status Verify the status of the migrated objects and the aggregated status of the entire migration
Migrate Infrastructure	Install and configure v6 servers to replace v5 servers	scantmr	analyze	external	scantmr
Migrate Endpoints	Migrate v5 endpoint agents to v6 agents	assess	analyze	migrate	verify
Migrate Profiles	Migrate v5 resource models to become v6 situations	assess	analyze	migrate	verify
Migrate Profile Mgrs	Migrate v5 profile managers to v6 managed systems lists	assess	analyze	migrate	verify

Figure 4-11 Grid showing the migration phases and steps

The phases

We can summarize the phases described in Figure 4-11 on page 191 as follows:

1. Phase A: Migrate the infrastructure.
2. Phase B: Migrate endpoints.
3. Phase C: Migrate profiles.
4. Phase D: Migrate profile managers.

The steps

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

1. Assess: This step consists of an assessment of the IBM Tivoli Monitoring V5.1.2 resource and a mapping to the corresponding IBM Tivoli Monitoring V6.2 resource together with the upgrade status and migration settings.
2. Analyze: During this step, you analyze the IBM Tivoli Monitoring V5.1.2 resources that have not yet been migrated, inspect the proposed migration settings, and provide information when needed in the generated XML files.
3. Migrate: This steps represents the actual migration of a set of non-migrated IBM Tivoli Monitoring V5.1.2 resources to IBM Tivoli Monitoring V6.2.
4. Review results and check status: This is the last step to review the outcome of the object migration and monitor the overall status of the upgrade.

4.4.1 Phase A: Migrate from IBM Tivoli Monitoring V5.1.2 to IBM Tivoli Monitoring V6.2 infrastructure

This phase is the first in the order to migrate the infrastructure. It is composed of four steps that we will discuss in this section.

During this phase, the IBM Tivoli Monitoring V5.1.2 infrastructure is assessed and a corresponding IBM Tivoli Monitoring V6.2 infrastructure is proposed for review before its deployment.

Note: The Tivoli Management Region server is queried, looking for gateways and endpoints based on the IBM Tivoli Monitoring V5.1.2 boot methods.

Some internal calls are executed to query the endpoint manager to look at the endpoints' boot methods, therefore only endpoints that do have a boot method called DMAE_boot_engine are added to the baseline file for the infrastructure and mapped to OS agents. For the gateways, the location attribute of the IBM Tivoli Monitoring V5.1.2 installation object is queried to establish if it is installed on the gateway: only those gateways are added into the baseline file and mapped to a remote monitoring server.

The infrastructure migration for the entire Tivoli Management Framework region must complete before starting the migration of endpoints, profiles, and profile managers.

The same apply in the case of multiple-region architecture, so called HUB and SPOKE: in this case, you must complete the entire infrastructure migration for all regions before migrating any endpoints, profiles, and profile managers.

The tool can be accessed both by the command line using the **`witmmtk`** command and GUI. For the objective of this book, we will describe the command line options and we will present some screen captures with the migration status.

Step 1: Migrate servers – assess

This step consist of the execution of the **`witmmtk`** tool with the scantmr parameter.

You can either use the GUI or CLI to perform this operation, and there is no advantage in using one or the other method, as the GUI simply offers a user-friendly interface for entering the command parameters and then runs the command.

To use the command line, follow these steps:

1. Log on to the Tivoli server and source the Tivoli environment.
2. Enter the following command from any directory: **`witmmtk scantmr`** or **`witmmtk scan`**.

The resulting baseline file is named <tmroid>.xml, where tmroid is the OID (object ID) number that uniquely identifies the Tivoli Management Region.

Example 4-7 shows the output of the above command execution in our environment.

Example 4-7 witmmtk scan command execution

```
The Framework environment we used was made of two gateways and eight
endpoints as shown in the below “wep ls” output:

C:\Tivoli\db\cairo.db\AMK\analyze\profilemanagers>wep ls
G     1713357986.1.590  cairo-gw
1713357986.14.522+#TMF_endpoint::endpoint# florence-ep
1713357986.4.522+#TMF_endpoint::endpoint# cairo-ep
1713357986.8.522+#TMF_endpoint::endpoint# rp3410-ep
G      1713357986.6.66  toronto-gw
1713357986.11.522+#TMF_endpoint::endpoint# paris-ep
1713357986.15.522+#TMF_endpoint::endpoint# rx2620-ep
1713357986.16.522+#TMF_endpoint::endpoint# server2-ep
1713357986.17.522+#TMF_endpoint::endpoint# edinburgh-ep
1713357986.7.522+#TMF_endpoint::endpoint# toronto-ep

Run the following command with any other parameter but “scan”.

C:\Tivoli\db\cairo.db\AMK\analyze\scans>witmmtk scan

AMKUT0016I Processing the request.
.
AMKUT2504I Creating a new infrastructure baseline file
"C:\Tivoli\db\cairo.db\AMK\analyze\scans\1713357986.xml".
AMKUT2515I IBM Tivoli Monitoring is installed on gateway "cairo-gw".
AMKUT2515I IBM Tivoli Monitoring is installed on gateway "toronto-gw".
AMKUT2512I IBM Tivoli Monitoring is present on the endpoint
"server2-ep".
AMKUT2512I IBM Tivoli Monitoring is present on the endpoint "cairo-ep".
AMKUT2512I IBM Tivoli Monitoring is present on the endpoint
"toronto-ep".
AMKUT2512I IBM Tivoli Monitoring is present on the endpoint "paris-ep".
AMKUT2512I IBM Tivoli Monitoring is present on the endpoint
"florence-ep".
AMKUT2512I IBM Tivoli Monitoring is present on the endpoint
"rx2620-ep".
AMKUT2512I IBM Tivoli Monitoring is present on the endpoint
"edinburgh-ep".
AMKUT2512I IBM Tivoli Monitoring is present on the endpoint
"rp3410-ep".
```

```
AMKUT2520I Converting the Tivoli Management Region data into a new
infrastructure deployment model.
AMKUT2529I Converting the data from Tivoli Management Region "CAIRO"
into the baseline for the Tivoli Monitoring Services infrastruc
ture in IBM Tivoli Monitoring, version 6.2.
AMKUT2523I Defining a new hub monitoring server in the infrastructure
baseline.
AMKUT2538I The number of gateways used by IBM Tivoli Monitoring is 2.
AMKUT2539I The gateway "toronto-gw" contains 5 endpoints used with IBM
Tivoli Monitoring.
AMKUT2521I The scale factor for the calculated number of remote servers
for the gateway "toronto-gw" is 1. The scale factor for the
calculated number of endpoints for each remote server is 5.
AMKUT2525I Defining a new remote server element in the infrastructure
baseline for the gateway "toronto-gw".
AMKUT2527I Adding an OS monitoring agent element to the infrastructure
baseline for the endpoint "edinburgh-ep".
AMKUT2527I Adding an OS monitoring agent element to the infrastructure
baseline for the endpoint "florence-ep".
AMKUT2527I Adding an OS monitoring agent element to the infrastructure
baseline for the endpoint "paris-ep".
AMKUT2527I Adding an OS monitoring agent element to the infrastructure
baseline for the endpoint "rp3410-ep".
AMKUT2527I Adding an OS monitoring agent element to the infrastructure
baseline for the endpoint "rx2620-ep".
AMKUT2539I The gateway "cairo-gw" contains 3 endpoints used with IBM
Tivoli Monitoring.
AMKUT2521I The scale factor for the calculated number of remote servers
for the gateway "cairo-gw" is 1. The scale factor for the ca
lculated number of endpoints for each remote server is 3.
AMKUT2525I Defining a new remote server element in the infrastructure
baseline for the gateway "cairo-gw".
AMKUT2527I Adding an OS monitoring agent element to the infrastructure
baseline for the endpoint "cairo-ep".
AMKUT2527I Adding an OS monitoring agent element to the infrastructure
baseline for the endpoint "server2-ep".
AMKUT2527I Adding an OS monitoring agent element to the infrastructure
baseline for the endpoint "toronto-ep".
AMKUT2528I Writing the new deployment infrastructure to the
infrastructure baseline
"C:\Tivoli\db\cairo.db\AMK\analyze\scans\1713357
986.xml".
```

```
AMKUT0008I The command completed successfully. See log
"C:\Tivoli\db\cairo.db\AMK\logs\log_wmtkscantmr_20070921_16_01_58.log"f
or mor
e information.
```

The baseline file is placed in the following directory:

- $DBDIR/AMK/analyze/scans for UNIX or Windows using the bash shell
- %DBDIR%\AMK\analyze\scans for Windows

  where $DBDIR or %DBDIR% is the Tivoli environment variable used to reference the Tivoli object database directory.

As you can deduce by reading the output in Example 4-7 on page 194, these are the actions performed during the scan phase:

- Check that the IBM Tivoli Monitoring V5.1.2 is installed on the endpoints.
- Convert the Tivoli Management Region server into an hub Tivoli Enterprise Monitoring Server.
- Convert the Tivoli Management Region gateways into remote Tivoli Enterprise Monitoring Server.
- Convert each Tivoli Management Region endpoint into an IBM Tivoli Monitoring V6.2 OS agent.

In the following section, we provide some details about the resource mappings and the scaling factor used by the migration toolkit.

Mapping V5.1.2 infrastructure to V6.x

The **scantmr** tool surveys a Tivoli Management Region and produces an XML output file that maps Tivoli infrastructure components to a proposed V6.x infrastructure. Table 4-7 on page 197 shows the mapping between the IBM Tivoli Monitoring V5.1.2 and IBM Tivoli Monitoring V6.2 infrastructure components.

Table 4-7 Mapping between 5.1.2 and 6.x infrastructure components

V5.1.2 infrastructure component	Mapped V6.x infrastructure component
Tivoli Management Region server	One or more hub monitoring servers.
Tivoli gateway	One or more remote monitoring servers. If the infrastructure requires more that 15 remote monitoring servers to be attached to a hub monitoring server, an entry for a second hub monitoring server is created in the baseline file, and an extra remote monitoring server is allocated to the second hub monitoring server.
endpoints	Mapped to OS agents and assigned to each remote monitoring server. If the infrastructure requires that more than 500 endpoints need to be attached to a remote monitoring server, an entry for a second remote monitoring server is created and the endpoints distributed between them.

By architecture, each hub monitoring server is connected to at least one Tivoli Enterprise Portal Server.

> **Note:** The output file from the scan does not include the portal clients but only a stanza, referenced as PortalConsole in the baseline file, used internally to access the Tivoli Enterprise Portal Server.

The ratios of hub Tivoli Enterprise Monitoring Serverm to remote Tivoli Enterprise Monitoring Server and remote Tivoli Enterprise Monitoring Server to endpoints are called the scalability factors. The **scantmr** tool specifies a proposed assignment of endpoints to a remote Tivoli Enterprise Monitoring Server.

The **scantmr** tool, depending on scalability factors, might divide the endpoints on a Tivoli gateway between more than one remote Tivoli Enterprise Monitoring Server. At this point, the endpoints are not communicating with the Tivoli Enterprise Monitoring Server. You only connect endpoints to a Tivoli Enterprise Monitoring Server by deploying OS monitoring agents to the endpoints.

You deploy agents in the second step of the migration procedure when you start migrating endpoints. The endpoints remain connected to Tivoli gateways both before and after the migration.

Example 4-8 shows the baseline file results of the **scantmr** tool run in our environment.

Example 4-8 Sample baseline file from a real environment

```
<?xml version="1.0" encoding="UTF-8"?>
<!--Copyright IBM Corporation 2006-->
<?xml-stylesheet type="text/xsl"
href="../../data/stylesheet/Infrastructure.xsl"?>
<ITM6.2Infrastructure aggregateStatus="0"
xmlns="http://www.ibm.com/tivoli/itm/assess/infrastructure"
xmlns:itmst="http://www.ibm.com/Tivoli/ITM/MigrateStatus"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="http://www.ibm.com/tivoli/itm/assess/infrastructure
Infrastructure.xsd">
  <EventServer comment="" eventServerLabel="EventServer#cairo-region"
eventServerPort="AMK-REQUIRED-AMK:0"
eventServerTarget="AMK-REQUIRED-AMK:9.3.5.205" status="NOT_CONFIGURED"/>
  <HubServer aggregateStatus="0" hub_installDir="AMK-REQUIRED-AMK"
remote_control_endpoint="AMK-REQUIRED-AMK" sourceClass="ServerManagedNode"
sourceLabel="CAIRO" status="NOT_CONFIGURED" target="AMK-REQUIRED-AMK"
unix_OSAgent_installDir="/opt/IBM/ITM" windows_OSAgent_installDir="C:/IBM/ITM">
    <SOAPConsole hostname="AMK-REQUIRED-AMK" password="AMK-REQUIRED-AMK"
port="AMK-REQUIRED-AMK:1920" ssl="false" status="NOT_CONFIGURED"
user="AMK-REQUIRED-AMK:sysadmin"/>
    <PortalConsole hostname="AMK-REQUIRED-AMK" password="AMK-REQUIRED-AMK"
port="AMK-REQUIRED-AMK:1920" status="NOT_CONFIGURED" target="PORTAL1"
user="AMK-REQUIRED-AMK:sysadmin"/>
    <Server aggregateStatus="0" hostname="AMK-REQUIRED-AMK"
port="AMK-REQUIRED-AMK:1918" protocol="IP.PIPE" sourceClass="gateway"
sourceLabel="toronto-gw" status="NOT_CONFIGURED" target="AMK-REQUIRED-AMK"
unix_OSAgent_installDir="" windows_OSAgent_installDir="">
      <OSAgent hostname="edinburgh.itsc.austin.ibm.com" interp="linux-ix86"
osAgent_installDir="" password="AMK-REQUIRED-AMK" sourceClass="endpoint"
sourceLabel="edinburgh-ep" status="NOT_CONFIGURED" target="edinburgh:LZ"
user="AMK-REQUIRED-AMK"/>
      <OSAgent hostname="florence.itsc.austin.ibm.com" interp="w32-ix86"
osAgent_installDir="" password="AMK-REQUIRED-AMK" sourceClass="endpoint"
sourceLabel="florence-ep" status="NOT_CONFIGURED" target="Primary:FLORENCE:NT"
user="AMK-REQUIRED-AMK"/>
      <OSAgent hostname="paris.itsc.austin.ibm.com" interp="aix4-r1"
osAgent_installDir="" password="AMK-REQUIRED-AMK" sourceClass="endpoint"
sourceLabel="paris-ep" status="NOT_CONFIGURED" target="paris:KUX"
user="AMK-REQUIRED-AMK"/>
      <OSAgent hostname="rp3410.itsc.austin.ibm.com" interp="hpux10"
osAgent_installDir="" password="AMK-REQUIRED-AMK" sourceClass="endpoint"
sourceLabel="rp3410-ep" status="NOT_CONFIGURED" target="rp3410:KUX"
user="AMK-REQUIRED-AMK"/>
```

```
      <OSAgent hostname="rx2620.itsc.austin.ibm.com" interp="hpux10"
osAgent_installDir="" password="AMK-REQUIRED-AMK" sourceClass="endpoint"
sourceLabel="rx2620-ep" status="NOT_CONFIGURED" target="rx2620:KUX"
user="AMK-REQUIRED-AMK"/>
    </Server>
    <Server aggregateStatus="0" hostname="AMK-REQUIRED-AMK"
port="AMK-REQUIRED-AMK:1918" protocol="IP.PIPE" sourceClass="gateway"
sourceLabel="cairo-gw" status="NOT_CONFIGURED" target="AMK-REQUIRED-AMK"
unix_OSAgent_installDir="" windows_OSAgent_installDir="">
      <OSAgent hostname="cairo.itsc.austin.ibm.com" interp="w32-ix86"
osAgent_installDir="" password="AMK-REQUIRED-AMK" sourceClass="endpoint"
sourceLabel="cairo-ep" status="NOT_CONFIGURED" target="Primary:CAIRO:NT"
user="AMK-REQUIRED-AMK"/>
      <OSAgent hostname="server2.itsc.austin.ibm.com" interp="aix4-r1"
osAgent_installDir="" password="AMK-REQUIRED-AMK" sourceClass="endpoint"
sourceLabel="server2-ep" status="NOT_CONFIGURED" target="server2:KUX"
user="AMK-REQUIRED-AMK"/>
      <OSAgent hostname="9.3.4.200" interp="w32-ix86" osAgent_installDir=""
password="AMK-REQUIRED-AMK" sourceClass="endpoint" sourceLabel="toronto-ep"
status="NOT_CONFIGURED" target="AMK-Unknown" user="AMK-REQUIRED-AMK"/>
    </Server>
  </HubServer>
</ITM6.2Infrastructure>
```

So the XML representation of the infrastructure components can be summarized as follows:

```
<ITM6.2Infrastructure>
   <EventServer/>
   <HubServer>
      <SOAPConsole/>
      <PortalConsole/>
      <Server>
         <OSAgent/>
         <OSAgent/>
         <OSAgent/>
      </Server>
      <Server>
         <OSAgent/>
         <OSAgent/>
         <OSAgent/>
         </Server>
      </HubServer>
</ITM6.2Infrastructure>
```

Inter-connected Tivoli Management Regions

In environments where you have more than one Tivoli Management Region server interconnected, you must migrate the regions separately, giving them a separate baseline infrastructure.

If your interconnected Tivoli Management Region environment was of the hub-spoke variety, and you want to recreate a single structure under one hub Tivoli Enterprise Monitoring Server, you would need to migrate one region, and then, using the facilities of V6.x, add the endpoints from the other regions as managed systems.

However, in doing so, you must respect the scalability factors reported in the previous section, or risk unbalancing the loading of your monitoring system.

> **Attention:** It is technically possible to use the migration toolkit to migrate two separate regions: in this case, both are assigned to the same hub monitoring server. This practice is not recommended, because it takes no account of the scalability factors, and may result in object definitions from one of the regions overwriting the definitions of the other, with results that cannot be predicted.
>
> Similarly, do not assign endpoints from two different regions to the same remote server, for the same reasons.

Step 2: Migrate servers – analyze

This is a fundamental step that requires you to do the following with manual intervention:

- Examine the results of the assessment.
- Determine if you agree with the choices made by the migration toolkit.

  You can change the proposed V6.x topology shown in the baseline file by adding, moving, or deleting elements.

  For example, if you know that a particular zone of your network has communication problems, you may decide that 500 endpoints (heartbeats) for a particular Tivoli Enterprise Monitoring Server is too much. In this case, you would create an additional Tivoli Enterprise Monitoring Server entry and split the endpoints between them.

  While the **`scantmr`** tool proposes an infrastructure based on the available data, you are the final judge of what is needed for your monitoring environment. You might also want to delete from the baseline file OSAgent elements that represent mission-critical endpoints that you do not expect to migrate in the near future. This action prevents later commands from attempting to deploy agents or migrate resource models on these endpoints even if you inadvertently specify the endpoints as input.

- Check that the data copied from the V5.1.2 environment and the other generated default values (such as port numbers) are valid.
- Where you can, add the missing information to the various entries (in the GUI, wherever you see a field with an asterisk before it, when editing the file manually, or wherever you see the "AMK–REQUIRED–AMK" string). Much of this information may have to wait until you have completed the next step in the procedure.

The structure of the XML file is that each element of the infrastructure is an XML statement, each of which contains attributes that describe the element:

- Some of the attributes contain values you must edit.
- Some contain values you must not edit (such as the ID of the Tivoli Management Region server).
- Some contain default values that you can choose to edit (such as the port for secure communications).
- Some are not present in the file because they are optional, and you can choose to add them.

Viewing and editing the baseline file

To view and edit the baseline file, you can use either one of these methods:

- View the file with an Internet browser.
- View and edit the file with the GUI.
- View and edit the file with an XML editor.
- View and edit the file with a text editor.

For detailed information regarding the baseline file, refer to “Understanding the baseline file” in *Upgrading from IBM Tivoli Monitoring V5.1.2*, GC32-1976.

Note: While editing the baseline file, keep in mind that all the fields where you are expected to supply data are marked with an asterisk in the GUI. If you are editing manually, you will see the "AMK–REQUIRED–AMK" string.

The baseline file is fully described in Chapter 17, “Baseline infrastructure data file XML reference” in *Upgrading from IBM Tivoli Monitoring V5.1.2*, GC32-1976. The chapter explains the use of every element and full details of all the attributes.

If editing, you will see entries like:

```
AMK-REQUIRED-AMK
AMK-REQUIRED-AMK:1918
```

The second syntax indicates a default value that you can accept or modify.

Simply insert the appropriate value for AMK-REQUIRED-AMK, and remove the AMK-REQUIRED-AMK: entry after you change or confirm the proposed default value. The final result for the above example will, respectively, look like the following:

```
value
1918
```

A description of the various stanzas of the baseline file follows. We start from the file generated in the assess step to describe the content and the information you have to provide for each stanza.

- Event Server:

  ```
  <EventServer comment="" eventServerLabel="EventServer#cairo-region"
  eventServerPort="AMK-REQUIRED-AMK:0"
  eventServerTarget="AMK-REQUIRED-AMK:9.3.5.205"
  status="NOT_CONFIGURED"/>
  ```

  This stanza refers to the Tivoli Enterprise Console Event server and its port.

  Only secure Event Servers are listed in the baseline file. They are discovered with an internal call equivalent to a Name Registry lookup of the EventServer resource.

  The Event Server described in the eventServerLabel is therefore mapped to a CORBA name.

  During the migration phase for the profiles, a secure event server naming convention does not have any meaning because IBM Tivoli Monitoring V6.2 does not use the Tivoli Management Framework at all, so the event server is converted in a non-secure event server. The broadcast or failover techniques defined in the Tmw2kProfiles are maintained, but the secure event server that is in the baseline file is converted in the non-secure format of host name+port.

- HubServer:

  ```
  <HubServer aggregateStatus="0" hub_installDir="AMK-REQUIRED-AMK"
  remote_control_endpoint="AMK-REQUIRED-AMK"
  sourceClass="ServerManagedNode" sourceLabel="CAIRO"
  status="NOT_CONFIGURED" target="AMK-REQUIRED-AMK"
  unix_OSAgent_installDir="/opt/IBM/ITM"
  windows_OSAgent_installDir="C:/IBM/ITM">
  ```

  This is the stanza corresponding to the hub Tivoli Enterprise Monitoring Server where:

  – hub_installDir represents the hub Tivoli Enterprise Monitoring Server installation directory.

  – remote_control_endpoint represents the label of the endpoint located on the hub Tivoli Enterprise Monitoring Server that is used for the remote deployment of the agents using the migration toolkit. If you do not plan to use the migration toolkit to perform a remote deployment, simply leave it blank.

  – target represents the label of the hub Tivoli Enterprise Monitoring Server, which is the same label that was specified at installation time. If you are not sure about the exact name, run the **tacmd listsystems** command from your hub Tivoli Enterprise Monitoring Server.

  By default, the tool maps the Tivoli Management Region (TMR) server to the hub Tivoli Enterprise Monitoring Server in the IBM Tivoli Monitoring V6.2 infrastructure.

  You can change the above fields to point to the hub Tivoli Enterprise Monitoring Server you prefer. In our example, the TMR server name is cairo, but we used a hub Tivoli Enterprise Monitoring Server called edinburgh for the IBM Tivoli Monitoring V6.2 infrastructure.

  You should not care about the Framework classes you see inside the file. They are only for internal use.

  Regarding the status, you should not change the value. In the next phases, when the mapped resource is discovered as installed and the information specified in the baseline file is verified, the status will be automatically changed to DEPLOYED.

- SOAPConsole:

  ```
  <SOAPConsole hostname="AMK-REQUIRED-AMK" password="AMK-REQUIRED-AMK"
  port="AMK-REQUIRED-AMK:1920" ssl="false" status="NOT_CONFIGURED"
  user="AMK-REQUIRED-AMK:sysadmin"/>
  ```

This stanza is related to the SOAPConsole, used to connect to the hub Tivoli Enterprise Monitoring Server for the SOAP commands execution.

- PortalConsole:

```
<PortalConsole hostname="AMK-REQUIRED-AMK"
password="AMK-REQUIRED-AMK" port="AMK-REQUIRED-AMK:1920"
status="NOT_CONFIGURED" target="PORTAL1"
user="AMK-REQUIRED-AMK:sysadmin"/>
```

This stanza represents an internal Tivoli Enterprise Portal used to access the Tivoli Enterprise Portal Server.

- Server:

```
<Server aggregateStatus="0" hostname="AMK-REQUIRED-AMK"
port="AMK-REQUIRED-AMK:1918" protocol="IP.PIPE"
sourceClass="gateway" sourceLabel="toronto-gw"
status="NOT_CONFIGURED" target="AMK-REQUIRED-AMK"
unix_OSAgent_installDir="" windows_OSAgent_installDir="">
```

This stanza refers to the Tivoli Enterprise Monitoring Server. In this case, you have to specify only the host name of the computer hosting the remote Tivoli Enterprise Monitoring Server, its port, and its label.

> **Note:** If you have a small enough environment where the hub monitoring server can service all of the endpoints without needing a remote monitoring server, you do not need to install a remote server, but your baseline file must contain the definition for both the HubServer and the Server that in this case will point to the same physical system.
>
> The Server entry is a logic representation of a system that will handle OS agents, so it can be either a hub or remote server; it does not refer to the physical system.

By default, the tool maps each Tivoli gateways to a remote Tivoli Enterprise Monitoring Server in the IBM Tivoli Monitoring V6.2 infrastructure.

> **Note:** Only one protocol is supported by the migration toolkit; you cannot specify more than one in this phase. If needed, you have to manually reconfigure the component.

- OSAgent:

```
<OSAgent hostname="edinburgh.itsc.austin.ibm.com"
interp="linux-ix86" osAgent_installDir=""
password="AMK-REQUIRED-AMK" sourceClass="endpoint"
sourceLabel="edinburgh-ep" status="NOT_CONFIGURED"
target="edinburgh:LZ" user="AMK-REQUIRED-AMK"/>
```

This is the last stanza of the file that contains the mapping information of the endpoint to OSAgents.

The assumption that is made by the tool is that you want to deploy OS Agents on all the endpoints of your Tivoli Management Framework environment so that you can monitor resources on those computers.

The **scantmr** tool automatically adds the endpoint host names, such as other information. The only values you must provide at this stage are the user and password to access the OS (they are used for the remote deployment in case you deploy the agents through the migration toolkit).

Note: By default, the baseline file contains a target name for the OS Agent with the format:

```
shortname:<pc>
```

where pc is the product code; in the above example, it would be “edinburgh:LZ”.

During the migration, some checks are made on the name resolution to determine the final name of the OS Agent in the IBM Tivoli Monitoring V6.2 infrastructure:

1. Check per IP address
2. Check per affinity (internal code used to identify the agent type)
3. Check per name

Suppose that 1 and 2 are consistent and for point 3 you have only the fully qualified domain name (FQDN); the tool is sure that this is the right agent, so in the baseline file, the target element is updated to match the FQDN.

In case you have PAC agents, they are not discovered in this phase; this phase is only used to map the endpoint to an OS Agent. For the PAC mappings, refer to 4.4.3, “Phase B: Migrating the endpoints” on page 220.

Password management

There are special arrangements for adding passwords that minimize any security exposure created by leaving passwords in the "clear" in the baseline file.

The methods differ according to the editing method you are using:

- Editing the file with the GUI

  If you enter a password in the GUI, it is automatically replaced with asterisks as you type it, and is stored in encrypted form in the baseline file.

- Using the **setpwd** command

  Use the **setpwd** command to enter the password. If you run the command without supplying the password, it will prompt you for it. As you enter the password, the characters are not echoed on the screen, and the password is stored in encrypted form in the baseline file. Alternatively, you can supply the user ID and password as parameters to the command, limiting your potential security exposure to the elapsed time between typing the password in the command string and when you close the command window after the command has completed. There will also be a potential security exposure in the log file.

- Editing the file with an XML editor or a text editor

  If you type a password into the file when using an XML editor or text editor, the command is stored in the baseline file in "clear". You then run the **encpwd** command, which encrypts any unencrypted passwords it finds in the baseline file. Your security exposure is limited to the elapsed time between saving the baseline file with the editor and running the tool.

In our test, we run the **encpwd** command, as shown in Example 4-9.

Example 4-9   encpwd command output

```
C:\Tivoli\db\cairo.db\AMK\analyze\scans>witmmtk encpwd -f
1713357986.xml

AMKUT0016I Processing the request.
AMKUT0057I Loading the infrastructure baseline file:
"C:\Tivoli\db\cairo.db\AMK\analyze\scans\1713357986.xml".
AMKUT3003I Encoding passwords.

AMKUT0000I The command has completed.
```

Sample XML file that results from the analyze step

Once you have completed the analyze step, substituted all of the AMK-REQUIRED-AMK values with the right values, and encrypted the password, the resulting XML file will look like Example 4-10.

Example 4-10 Analyze step output XML file

```
<?xml version="1.0" encoding="UTF-8"?>
<!--Copyright IBM Corporation 2006-->
<?xml-stylesheet type="text/xsl"
href="../../data/stylesheet/Infrastructure.xsl"?>
<ITM6.2Infrastructure aggregateStatus="0"
xmlns="http://www.ibm.com/tivoli/itm/assess/infrastructure"
xmlns:itmst="http://www.ibm.com/Tivoli/ITM/MigrateStatus"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="http://www.ibm.com/tivoli/itm/assess/infrastructure
Infrastructure.xsd">
  <EventServer comment="" eventServerLabel="EventServer#cairo-region"
eventServerPort="0" eventServerTarget="9.3.5.205" status="CONFIGURED"/>
  <HubServer aggregateStatus="0" hub_installDir="/opt/IBM/ITM"
remote_control_endpoint="edinburgh-ep" sourceClass="ServerManagedNode"
sourceLabel="CAIRO" status="NOT_AVAILABLE" target="HUB_TEMS"
unix_OSAgent_installDir="/opt/IBM/ITM" windows_OSAgent_installDir="C:/IBM/ITM">
    <SOAPConsole hostname="edinburgh.itsc.austin.ibm.com"
password="AMKEnc:VVIslgoEiCQ=" port="1920" ssl="false" status="NOT_AVAILABLE"
user="sysadmin"/>
    <PortalConsole hostname="edinburgh.itsc.austin.ibm.com"
password="AMKEnc:VVIslgoEiCQ=" port="1920" status="NOT_AVAILABLE"
target="PORTAL1" user="sysadmin"/>
    <Server aggregateStatus="0" hostname="toronto.itsc.austin.ibm.com"
port="1918" protocol="IP.PIPE" sourceClass="gateway" sourceLabel="toronto-gw"
status="NOT_AVAILABLE" target="REMOTE_TORONTO" unix_OSAgent_installDir=""
windows_OSAgent_installDir="">
      <OSAgent hostname="edinburgh.itsc.austin.ibm.com" interp="linux-ix86"
osAgent_installDir="" password="AMKEnc:bkmBWvJXTlI=" sourceClass="endpoint"
sourceLabel="edinburgh-ep" status="NOT_AVAILABLE" target="edinburgh:LZ"
user="root"/>
    </Server>
    <Server aggregateStatus="0" hostname="cairo.itsc.austin.ibm.com"
port="1918" protocol="IP.PIPE" sourceClass="gateway" sourceLabel="cairo-gw"
status="NOT_AVAILABLE" target="REMOTE_CAIRO" unix_OSAgent_installDir=""
windows_OSAgent_installDir="">
      <OSAgent hostname="cairo.itsc.austin.ibm.com" interp="w32-ix86"
osAgent_installDir="" password="AMKEnc:91PFBMjUr8Y=" sourceClass="endpoint"
sourceLabel="cairo-ep" status="NOT_AVAILABLE" target="Primary:CAIRO:NT"
user="Administrator"/>
      <OSAgent hostname="florence.itsc.austin.ibm.com" interp="w32-ix86"
osAgent_installDir="" password="AMKEnc:91PFBMjUr8Y=" sourceClass="endpoint"
```

```
sourceLabel="florence-ep" status="NOT_AVAILABLE" target="Primary:FLORENCE:NT"
user="Administrator"/>
      <OSAgent hostname="paris.itsc.austin.ibm.com" interp="aix4-r1"
osAgent_installDir="" password="AMKEnc:bkmBWvJXTlI=" sourceClass="endpoint"
sourceLabel="paris-ep" status="NOT_AVAILABLE" target="paris:KUX" user="root"/>
      <OSAgent hostname="rp3410.itsc.austin.ibm.com" interp="hpux10"
osAgent_installDir="" password="AMKEnc:bkmBWvJXTlI=" sourceClass="endpoint"
sourceLabel="rp3410-ep" status="NOT_AVAILABLE" target="rp3410:KUX"
user="root"/>
      <OSAgent hostname="rx2620.itsc.austin.ibm.com" interp="hpux10"
osAgent_installDir="" password="AMKEnc:bkmBWvJXTlI=" sourceClass="endpoint"
sourceLabel="rx2620-ep" status="NOT_AVAILABLE" target="rx2620:KUX"
user="root"/>
      <OSAgent hostname="server2.itsc.austin.ibm.com" interp="aix4-r1"
osAgent_installDir="" password="AMKEnc:bkmBWvJXTlI=" sourceClass="endpoint"
sourceLabel="server2-ep" status="NOT_AVAILABLE" target="server2:KUX"
user="root"/>
      <OSAgent hostname="toronto.itsc.austin.ibm.com" interp="w32-ix86"
osAgent_installDir="" password="AMKEnc:91PFBMjUr8Y=" sourceClass="endpoint"
sourceLabel="toronto-ep" status="NOT_AVAILABLE" target="Primary:TORONTO:NT"
user="Administrator"/>
    </Server>
  </HubServer>
</ITM6.2Infrastructure>
```

Step 3: Migrate servers – migrate

When you have determined that the structure proposed by the **scantmr** tool is correct, or you have modified it to your satisfaction, you can use it as a roadmap to manually install the following V6.x server infrastructure:

- Hub monitoring server

  Represented by the HubServer elements in the baseline file.

- Portal server

  One portal server for every hub server. Represented by the PortalConsole elements in the baseline file. If you have a Tivoli Enterprise Portal Server already available, you do not need to install a new one.

- SOAP Service

  The IBM Tivoli Monitoring Web Services (the SOAP service) on every hub server. Represented by the SOAPConsole elements in the baseline file. If the computer where you will install the hub monitoring server already has the SOAP service installed, you do not need to install a new one.

- Remote monitoring server

  The remote Tivoli Enterprise Monitoring Server will replace the Tivoli gateways. Represented by the Server elements in the baseline file.

- Event Server

  IBM Tivoli Enterprise Console event servers (optional). Represented by the EventServer elements in the baseline file. These are automatically mapped if they exist as Tivoli Management Framework objects. They are used for non-secure event mapping while migrating the Tmw2kProfiles.

  All the information you need to install these servers and services are described in the *IBM Tivoli Monitoring: Installation and Setup Guide*, GC32-9407.

- Endpoint lcfd on hub monitoring server

  Each hub Tivoli Enterprise Monitoring Server must have a Tivoli Management Framework endpoint lcfd installed on it to enable OS Agents deployment by the migrate tool. If you intend to deploy all V6.x agents to endpoints without using the migration toolkit, this is not needed.

Installing Tivoli Management Framework endpoint on hub Tivoli Enterprise Monitoring Server to enable migration toolkit OS Agent deployment

One of the most time-consuming parts of the migration is the deployment of the OSAgents on the V5.1.2 endpoints, transforming them into V6.x managed systems. You can do this in one of the following ways:

- Manually install the OSAgent on an endpoint.
- Use distribution software to install the OSAgent remotely.
- Let the migration toolkit deploy the OSAgent for you.

If you want to let the migration toolkit deploy the OSAgent for you, you must first install an endpoint lcfd on the appropriate hub Tivoli Enterprise Monitoring Server in your configuration.

If you are re-using an existing hub Tivoli Enterprise Monitoring Server, you may already have an endpoint installed. If not, you must install it. The endpoint lcfd is required so that the migration toolkit can launch Tivoli Management Framework tasks on the hub Tivoli Enterprise Monitoring Server. An example of this task is the execution of a script called creteNode.sh that is sent to the Tivoli Enterprise Monitoring Server endpoint as a dependency of the migration toolkit; it is used to remote deploy the OS agents.

The instructions for installing the endpoint lcfd are given in your Tivoli Management Framework documentation. The name (label) of the installed endpoint must be added to the infrastructure baseline in the remote_control_endpoint field of the HubServer element.

If you do not intend to deploy OSAgents using the migration toolkit, you can omit this step.

Preparing agent images for deployment

To deploy OS agents on the endpoints in your network, the migration toolkit leverages the Remote Deployment function of V6.x, which requires the preparation of the agent images. When the monitoring servers have been installed, ensure you have followed all the steps to enable Remote Deployment, as described in the V6.x documentation.

The preparation consist of these steps:

1. Install the application support for the specific agent on the infrastructure components, hub Tivoli Enterprise Monitoring Server, Tivoli Enterprise Portal Server, and Tivoli Enterprise Portal client.
2. Seed the infrastructure components with the support installed.
3. Load the images of the agent to be deployed in the hub Tivoli Enterprise Monitoring Server depot.

> **Note:** The remote deployment using the migration toolkit uses the hub Tivoli Enterprise Monitoring Server depot for the OS Agent installation, regardless of the remote monitoring server the agent is connected to.
>
> When deploying application agents using the migration toolkit, the process uses the depot of the remote Tivoli Enterprise Monitoring Server to which the application agent will be connected. You still need to add the application support for that agent and seed it for the hub Tivoli Enterprise Monitoring Server, remote Tivoli Enterprise Monitoring Server, Tivoli Enterprise Portal Server, and Tivoli Enterprise Console client to correctly manage the agents in your environment.

Once the migration has been completed, so that all the IBM Tivoli Monitoring V6.2 resources have been deployed, you can update the status of the baseline file.

Step 4: Updating the baseline file and the deployment status

This step requires you to update the baseline file with the information about the servers you have installed. It is essential to the migration that all the V6.x servers and services are installed and the communication with them configured in the baseline file before you start to migrate the endpoints.

In a migration that involves several hub or remote Tivoli Enterprise Monitoring Servers, it is a good practice to run the **scantmr** tool and check the status after each server is installed.

Running the tool also checks the connectivity with the new servers and services, as the tool uses the address and user credential information to check the connection with the servers and services, and will not give the DEPLOYED status for an item until a connection has been successfully established.

Updating the baseline file

The methods available to you to edit the baseline file are those described in "Viewing and editing the baseline file" on page 201.

In particular, note the information about entering passwords. Add to the baseline file all the information arising from the installation of the servers.

Running the scantmr tool to validate the updated file

You must now rerun the **scantmr** tool to validate the data added to the file and update the deployment status.

Use exactly the same command as when you first ran the **scantmr** tool.

> **Note:** If you have moved or renamed the baseline file from its default name or location, remember that if you do not specify the –f <filename> option to identify the moved or renamed file, **scantmr** assumes that there is no input file and creates one from scratch, just as in step 2. On the other hand, if you already have a file with the default name in the default location, you can overwrite it to create a file from scratch using the –o force option.

The command does the following:

1. It opens the baseline file as input.
2. It validates the data in the file and makes any necessary changes.
3. For each server or service, it attempts to make the defined connection. If it is successful, it changes the status of the element to "DEPLOYED".

4. It calculates the deployment percentage (aggregate status), both for each Server element, and the HubServer element or elements. In order to proceed to the next step, all servers and services (not the OSAgents) must be in the "DEPLOYED" status.

Example 4-11 shows the output of the validation command in our environment.

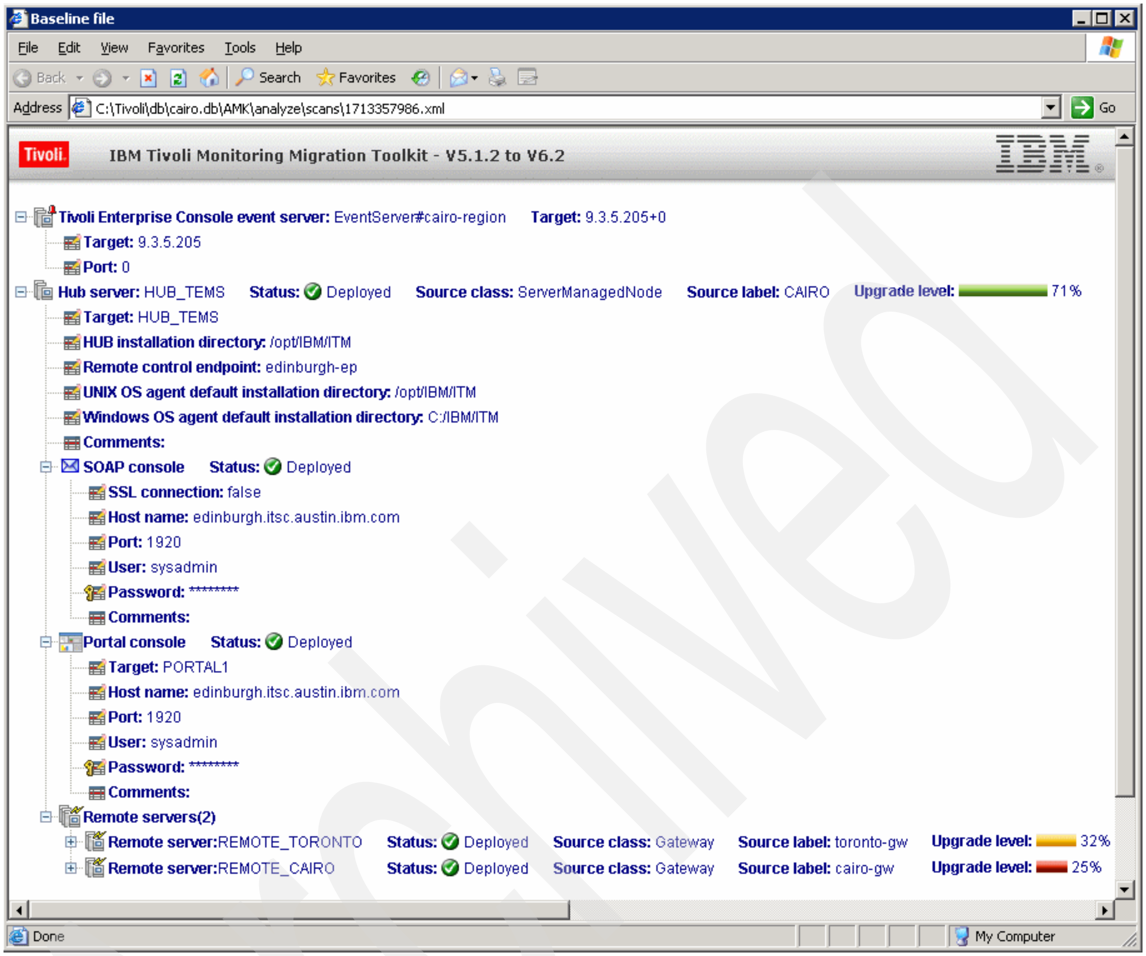
Example 4-11 Baseline file validation after updates

```
C:\Tivoli\db\cairo.db\AMK\analyze\scans>witmmtk scan

AMKUT0016I Processing the request.
AMKUT0057I Loading the infrastructure baseline file:
"C:\Tivoli\db\cairo.db\AMK\analyze\scans\1713357986.xml".
AMKUT2535W OS monitoring agent "cairo.itsc.austin.ibm.com" was not
found.
AMKUT2535W OS monitoring agent "florence.itsc.austin.ibm.com" was not
found.
AMKUT2535W OS monitoring agent "paris.itsc.austin.ibm.com" was not
found.
AMKUT2535W OS monitoring agent "rp3410.itsc.austin.ibm.com" was not
found.
AMKUT2535W OS monitoring agent "rx2620.itsc.austin.ibm.com" was not
found.
AMKUT2535W OS monitoring agent "server2.itsc.austin.ibm.com" was not
found.
AMKUT2535W OS monitoring agent "toronto.itsc.austin.ibm.com" was not
found.

AMKUT0010W The command completed with warnings. See log
"C:\Tivoli\db\cairo.db\AMK\logs\log_wmtkscantmr_20070924_15_59_26.log"
for m
ore information.

The new XML file will now looks like the following:

<?xml version="1.0" encoding="UTF-8"?>
<!--Copyright IBM Corporation 2006-->
<?xml-stylesheet type="text/xsl"
href="../../data/stylesheet/Infrastructure.xsl"?>
<ITM6.2Infrastructure aggregateStatus="71"
xmlns="http://www.ibm.com/tivoli/itm/assess/infrastructure"
xmlns:itmst="http://www.ibm.com/Tivoli/ITM/MigrateStatus"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="http://www.ibm.com/tivoli/itm/assess/infrastructure
Infrastructure.xsd">
```

```
  <EventServer comment="" eventServerLabel="EventServer#cairo-region"
eventServerPort="0" eventServerTarget="9.3.5.205" status="CONFIGURED"/>
  <HubServer aggregateStatus="71" hub_installDir="/opt/IBM/ITM"
remote_control_endpoint="edinburgh-ep" sourceClass="ServerManagedNode"
sourceLabel="CAIRO" status="DEPLOYED" target="HUB_TEMS"
unix_OSAgent_installDir="/opt/IBM/ITM"
windows_OSAgent_installDir="C:/IBM/ITM">
    <SOAPConsole hostname="edinburgh.itsc.austin.ibm.com"
password="AMKEnc:VVIslgoEiCQ=" port="1920" ssl="false"
status="DEPLOYED" user="sysadmin"/>
    <PortalConsole hostname="edinburgh.itsc.austin.ibm.com"
password="AMKEnc:VVIslgoEiCQ=" port="1920" status="DEPLOYED"
target="PORTAL1" user="sysadmin"/>
    <Server aggregateStatus="32" hostname="toronto.itsc.austin.ibm.com"
port="1918" protocol="IP.PIPE" sourceClass="gateway"
sourceLabel="toronto-gw" status="DEPLOYED" target="REMOTE_TORONTO"
unix_OSAgent_installDir="" windows_OSAgent_installDir="">
      <OSAgent hostname="edinburgh.itsc.austin.ibm.com"
interp="linux-ix86" osAgent_installDir=""
password="AMKEnc:bkmBWvJXTlI=" sourceClass="endpoint"
sourceLabel="edinburgh-ep" status="DEPLOYED"
target="edinburgh.itsc.austin.ibm.com:LZ" user="root"/>
      <OSAgent hostname="paris.itsc.austin.ibm.com" interp="aix4-r1"
osAgent_installDir="" password="AMKEnc:bkmBWvJXTlI="
sourceClass="endpoint" sourceLabel="paris-ep" status="NOT_DEPLOYED"
target="paris:KUX" user="root"/>
      <OSAgent hostname="rp3410.itsc.austin.ibm.com" interp="hpux10"
osAgent_installDir="" password="AMKEnc:bkmBWvJXTlI="
sourceClass="endpoint" sourceLabel="rp3410-ep" status="NOT_DEPLOYED"
target="rp3410:KUX" user="root"/>
      <OSAgent hostname="rx2620.itsc.austin.ibm.com" interp="hpux10"
osAgent_installDir="" password="AMKEnc:bkmBWvJXTlI="
sourceClass="endpoint" sourceLabel="rx2620-ep" status="NOT_DEPLOYED"
target="rx2620:KUX" user="root"/>
      <OSAgent hostname="server2.itsc.austin.ibm.com" interp="aix4-r1"
osAgent_installDir="" password="AMKEnc:bkmBWvJXTlI="
sourceClass="endpoint" sourceLabel="server2-ep" status="NOT_DEPLOYED"
target="server2:KUX" user="root"/>
    </Server>
    <Server aggregateStatus="25" hostname="cairo.itsc.austin.ibm.com"
port="1918" protocol="IP.PIPE" sourceClass="gateway"
sourceLabel="cairo-gw" status="DEPLOYED" target="REMOTE_CAIRO"
unix_OSAgent_installDir="" windows_OSAgent_installDir="">
      <OSAgent hostname="cairo.itsc.austin.ibm.com" interp="w32-ix86"
osAgent_installDir="" password="AMKEnc:91PFBMjUr8Y="
```

```
sourceClass="endpoint" sourceLabel="cairo-ep" status="NOT_DEPLOYED" 
target="Primary:CAIRO:NT" user="Administrator"/>
      <OSAgent hostname="florence.itsc.austin.ibm.com" 
interp="w32-ix86" osAgent_installDir="" password="AMKEnc:91PFBMjUr8Y=" 
sourceClass="endpoint" sourceLabel="florence-ep" status="NOT_DEPLOYED" 
target="Primary:FLORENCE:NT" user="Administrator"/>
     <OSAgent hostname="toronto.itsc.austin.ibm.com" interp="w32-ix86" 
osAgent_installDir="" password="AMKEnc:91PFBMjUr8Y=" 
sourceClass="endpoint" sourceLabel="toronto-ep" status="NOT_DEPLOYED" 
target="Primary:TORONTO:NT" user="Administrator"/>
    </Server>
  </HubServer>
</ITM6.2Infrastructure>
```

If you access the GUI, it is possible to view a graphic version of the deployment status, as shown in Figure 4-12 on page 215 and Figure 4-13 on page 216.


Baseline file
File Edit View Favorites Tools Help
Back Search Favorites
Address C:\Tivoli\db\cairo.db\AMK\analyze\scans\1713357986.xml
Go
Tivoli
IBM Tivoli Monitoring Migration Toolkit - V5.1.2 to V6.2
IBM
Done
My Computer

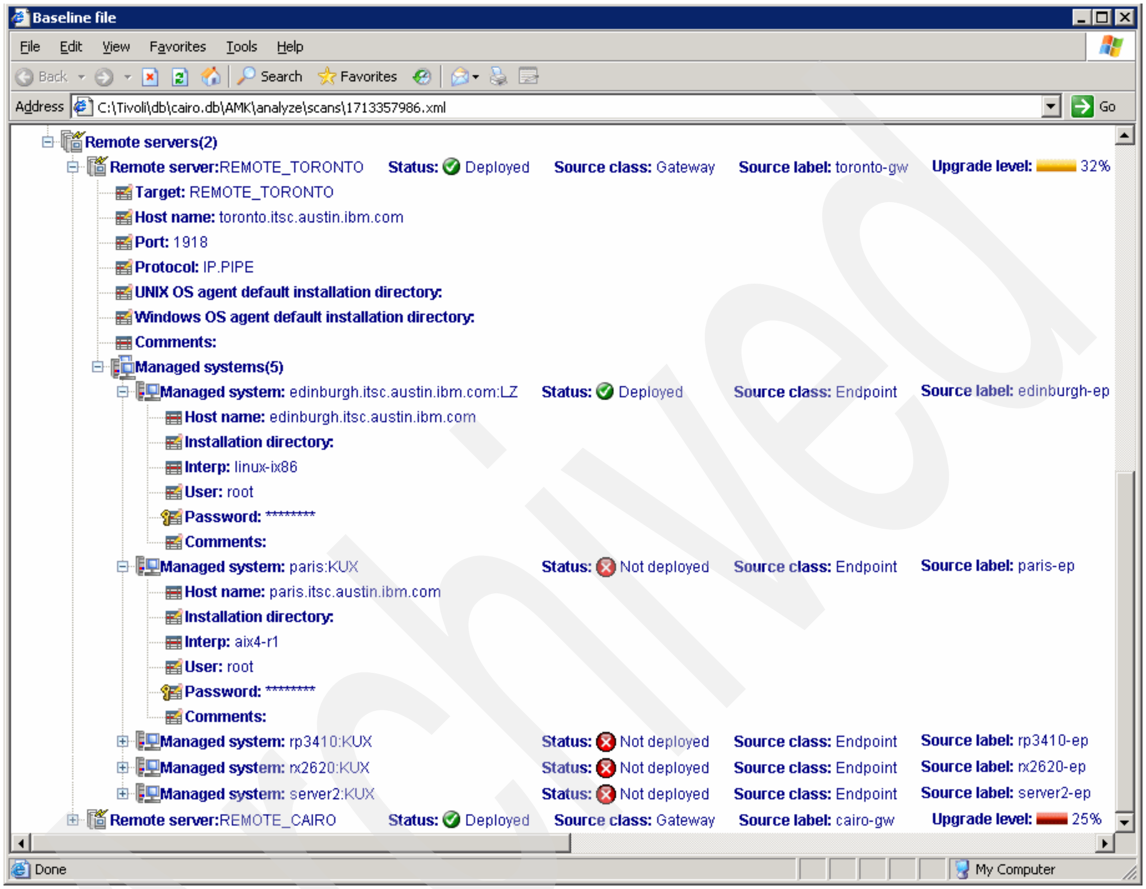
Tivoli Enterprise Console event server: EventServer#cairo-region **Target:** 9.3.5.205+0
- **Target:** 9.3.5.205
- **Port:** 0

Hub server: HUB_TEMS **Status:** ✓ Deployed **Source class:** ServerManagedNode **Source label:** CAIRO **Upgrade level:** 🟩 71%
- **Target:** HUB_TEMS
- **HUB installation directory:** /opt/IBM/ITM
- **Remote control endpoint:** edinburgh-ep
- **UNIX OS agent default installation directory:** /opt/IBM/ITM
- **Windows OS agent default installation directory:** C:/IBM/ITM
- **Comments:**
- **SOAP console** **Status:** ✓ Deployed
  - **SSL connection:** false
  - **Host name:** edinburgh.itsc.austin.ibm.com
  - **Port:** 1920
  - **User:** sysadmin
  - **Password:** ********
  - **Comments:**
- **Portal console** **Status:** ✓ Deployed
  - **Target:** PORTAL1
  - **Host name:** edinburgh.itsc.austin.ibm.com
  - **Port:** 1920
  - **User:** sysadmin
  - **Password:** ********
  - **Comments:**
- **Remote servers(2)**
  - **Remote server:**REMOTE_TORONTO **Status:** ✓ Deployed **Source class:** Gateway **Source label:** toronto-gw **Upgrade level:** 🟨 32%
  - **Remote server:**REMOTE_CAIRO **Status:** ✓ Deployed **Source class:** Gateway **Source label:** cairo-gw **Upgrade level:** 🟥 25%

Figure 4-12 Infrastructure component deployment status

In Figure 4-12, you can see that the main infrastructure components, hub Tivoli Enterprise Monitoring Server, Tivoli Enterprise Portal Server, and remote Tivoli Enterprise Monitoring Server, have been deployed successfully.

The upper right corner shows the overall Upgrade level (in this case, 71%). Scrolling down the page and expanding the Remote server entries, you can see the OS Agents deployment status, as shown in Figure 4-13.


Baseline file
File Edit View Favorites Tools Help
Back Search Favorites
Address C:\Tivoli\db\cairo.db\AMK\analyze\scans\1713357986.xml
Go
Done
My Computer

Remote servers(2)
Remote server:REMOTE_TORONTO Status: Deployed Source class: Gateway Source label: toronto-gw Upgrade level: 32%
Target: REMOTE_TORONTO
Host name: toronto.itsc.austin.ibm.com
Port: 1918
Protocol: IP.PIPE
UNIX OS agent default installation directory:
Windows OS agent default installation directory:
Comments:
Managed systems(5)
Managed system: edinburgh.itsc.austin.ibm.com:LZ Status: Deployed Source class: Endpoint Source label: edinburgh-ep
Host name: edinburgh.itsc.austin.ibm.com
Installation directory:
Interp: linux-ix86
User: root
Password: ********
Comments:
Managed system: paris:KUX Status: Not deployed Source class: Endpoint Source label: paris-ep
Host name: paris.itsc.austin.ibm.com
Installation directory:
Interp: aix4-r1
User: root
Password: ********
Comments:
Managed system: rp3410:KUX Status: Not deployed Source class: Endpoint Source label: rp3410-ep
Managed system: rx2620:KUX Status: Not deployed Source class: Endpoint Source label: rx2620-ep
Managed system: server2:KUX Status: Not deployed Source class: Endpoint Source label: server2-ep
Remote server:REMOTE_CAIRO Status: Deployed Source class: Gateway Source label: cairo-gw Upgrade level: 25%

Figure 4-13 OS Agent deployment status

4.4.2 Determining a migration strategy for endpoints, profiles, and profile managers

To migrate the endpoints, profiles, and profile managers in a Tivoli Management Region, it is best to divide the work into manageable stages.

Migrate a portion of the Tivoli Management Region at a time: a set of endpoints, the profiles distributed to those endpoints, and the profile managers that contain the profiles. By migrating a Tivoli Management Region in increments of reasonable size, you shorten the time it takes to reach the point where you can view and test monitoring data in the new environment.

The migration workflow

Each of the phases in the migration of the endpoints, profiles, and profile managers is an iterative process that follows this workflow:

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

Figure 4-14 shows the iterative nature of the process.

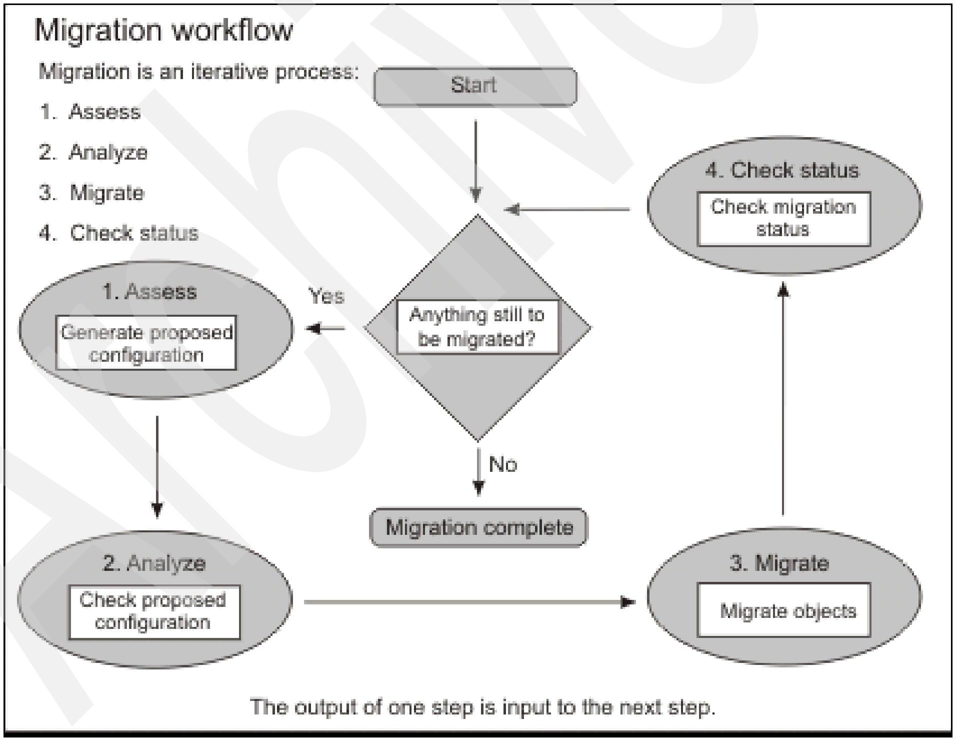

Migration workflow
Migration is an iterative process:
1. Assess
2. Analyze
3. Migrate
4. Check status
Start
4. Check status
Check migration status
1. Assess
Generate proposed configuration
Yes
Anything still to be migrated?
No
Migration complete
2. Analyze
Check proposed configuration
3. Migrate
Migrate objects
The output of one step is input to the next step.

Figure 4-14 The migration workflow

The following sections describe the upgrade workflow in more detail.

Assess

The Assess tool assesses endpoints, profiles, and profile managers. The assessment tools gather data about V5.1.2 resources and produce XML assess files that contain the following information:

- A mapping of V5.1.2 resources to proposed equivalent V6.x resources. For example, in an assessment of profiles, the output file maps each resource model (the source) to proposed equivalent situations (the target).

  > **Note:** The assessment is made of the resource models on the server, not those actually in use on the endpoint.

- The upgrade status of the V5.1.2 resources that were included in the assessment, indicating which resources have been upgraded and which have not.

Analyze

In this step, you analyze the output data, and check that it provides the result you want. The corresponding step for the infrastructure allowed you to reshape the infrastructure from the proposed version. In this case, however, we do not recommend modifying the results of the assessment, unless you are forced to because the tool found a problem. If you want your monitoring results to be the same in V6.x as in V5.1.2, you must leave the results as they are.

The migration toolkit provides various methods of viewing the XML files.

Migrate

The migration step implements the specifications from the assessment. The tool deploys V6.x resources based on the specifications in the output file from the Assess tool.

Check status

When the migration is complete, check the logs for errors and also, in the case of endpoint migration, recalculate the infrastructure completion percentage.

Migration modes

The migration toolkit gives you three possible way of migrating endpoints, profiles, and profile managers:

1. Migrating by phase

   This is an horizontal migration approach; once you have completed the infrastructure migration and chosen a first set of endpoints to migrate, perform every step of each phase as follows:

   – Assess, analyze, and migrate the endpoints in the first set.

   – Assess, analyze, and migrate the profiles on the endpoints in the first set.

   – Assess, analyze, and migrate the profile managers that contain the profiles for the first set.

   After you complete a migration for one set of endpoints and their associated profiles and profile managers, repeat the procedure for another subdivision, and so on, until the whole environment is migrated.

2. Migrating by step

   This is a vertical migration approach; once you have completed the infrastructure migration and chosen a first set of endpoints to migrate, perform every step of each phase as follows:

   – Assess the endpoints.

   – Assess the profiles.

   – Assess the profile managers.

   – Analyze the assessment.

   – Migrate the endpoint.

   – Migrate the profiles.

   – Migrate the profile managers.

3. Migrating by assessing a profile manager first

   This is a mixed migration approach; once you have completed the infrastructure migration and chosen a profile manager to migrate, you must follow this migration sequence:

   – Assess the profile manager that automatically assesses its profiles and endpoints and any other nested profile manager with their respective resources.

   – Analyze the assessment.

   – Migrate the endpoints.

   – Migrate the profiles.

- Migrate the profile managers.

  After you complete a migration for one profile manager, repeat the procedure for another profile manager, and so on, until the whole environment is migrated.

  The advantage of this scenario is that your migration unit corresponds to a V5.1.2 entity: a profile manager, which you may prefer as a unit for verification purposes.

For the scope of this book, we used the migration by phase procedure to migrate our resources.

4.4.3 Phase B: Migrating the endpoints

Once you choose the migration strategy that best fits in your environment, you can start migrating the endpoints. As with any other phase in the migration, it is made of four steps: assess, analyze, migrate, and status check.

In our environment, we used the migration toolkit to deploy most of the OS agent and an application agent, IBM Tivoli Monitoring for Databases V6.2.

> **Important:** The migration toolkit is only capable of migrating V6.2 products, so IBM Tivoli Monitoring V6.2 OS agent is the one that is deployed. In case you have an old V5.1.x PAC or a V6.1 agent, the tool is not able to perform the migration. In that case, a manual migration to V6.2 is required.

Here we have a brief description of this phase's steps, with real output from our environment.

Step 5: Migrate endpoints – assess

This step results in the creation of an XML file for each endpoint that determines which OS monitoring agent and application monitoring agents will be deployed.

The full mapping logic is:

- The assessment is driven by the agent mapping files.
- Endpoints become OS agents.
- Application objects become application agents.

Example 4-12 on page 221 shows the execution of the step in our environment.

Example 4-12 Migrate endpoints - assess step

```
We started from the endpoints list in our environment:

C:\>wlookup -ar endpoint |grep 1713357986
cairo-ep        1713357986.4.522+#TMF_endpoint::endpoint#
edinburgh-ep    1713357986.17.522+#TMF_endpoint::endpoint#
florence-ep     1713357986.14.522+#TMF_endpoint::endpoint#
paris-ep        1713357986.11.522+#TMF_endpoint::endpoint#
rp3410-ep       1713357986.8.522+#TMF_endpoint::endpoint#
rx2620-ep       1713357986.15.522+#TMF_endpoint::endpoint#
server2-ep      1713357986.16.522+#TMF_endpoint::endpoint#
toronto-ep      1713357986.7.522+#TMF_endpoint::endpoint#

Given that list, we built a text files, one for Windows, one for UNIX
and Linux OS, with this content:

C:\Tivoli\db\cairo.db\AMK\analyze\endpoints>more windows_ep.txt
@Endpoint:florence-ep
@Endpoint:cairo-ep
@Endpoint:toronto-ep

C:\Tivoli\db\cairo.db\AMK\analyze\endpoints>more unix_linux_ep.txt
@Endpoint:paris-ep
@Endpoint:rx2620-ep
@Endpoint:server2-ep
@Endpoint:edinburgh-ep
@Endpoint:rp3410-ep

We then run these commands to create the XML files for each endpoint:

C:\Tivoli\db\cairo.db\AMK\analyze\endpoints>witmmtk assess -i
windows_ep.txt

AMKUT5053I The assess tool is checking each endpoint for
responsiveness. This might take a few minutes.

AMKUT0016I Processing the request.
.
AMKUT5003I Loading the resource snapshot for the assessment.
AMKUT0057I Loading the infrastructure baseline file:
"C:\Tivoli\db\cairo.db\AMK\analyze\scans\1713357986.xml".
AMKUT5006I Starting the resource assessment.
AMKUT5075I Converting endpoint "florence-ep".
AMKUT5073I Converting application object "florence-ep".
```

```
AMKUT5075I Converting endpoint "cairo-ep".
AMKUT5073I Converting application object "MDIST2@DB2@cairo-ep".
AMKUT5073I Converting application object "PLANNER@DB2@cairo-ep".
AMKUT5075I Converting endpoint "toronto-ep".
AMKUT5073I Converting application object "toronto-ep".
AMKUT5007I All resources are assessed. Processing is complete.
.

AMKUT0008I The command completed successfully. See log
"C:\Tivoli\db\cairo.db\AMK\logs\log_wmtkassess_20070926_16_23_41.log"fo
r more information.
```

As you can see in the above output, for cairo-ep endpoint, the assess step discovered a running IBM Tivoli Monitoring for Databases DB2 Component Software Tmw2kProfile distributed and running on the system.

Follow the command for UNIX and Linux endpoints:

```
C:\Tivoli\db\cairo.db\AMK\analyze\endpoints>witmmtk assess -i
unix_linux_ep.txt

AMKUT5053I The assess tool is checking each endpoint for
responsiveness. This might take a few minutes.

AMKUT0016I Processing the request.
.....
AMKUT5003I Loading the resource snapshot for the assessment.
AMKUT0057I Loading the infrastructure baseline file:
"C:\Tivoli\db\cairo.db\AMK\analyze\scans\1713357986.xml".
AMKUT5006I Starting the resource assessment.
AMKUT5075I Converting endpoint "paris-ep".
AMKUT5073I Converting application object "paris-ep".
AMKUT5075I Converting endpoint "rx2620-ep".
AMKUT5073I Converting application object "rx2620-ep".
AMKUT5075I Converting endpoint "server2-ep".
AMKUT5073I Converting application object "server2-ep".
AMKUT5075I Converting endpoint "edinburgh-ep".
AMKUT5073I Converting application object "edinburgh-ep".
AMKUT5075I Converting endpoint "rp3410-ep".
AMKUT5073I Converting application object "rp3410-ep".
AMKUT5007I All resources are assessed. Processing is complete.
.
```

```
AMKUT0008I The command completed successfully. See log
"C:\Tivoli\db\cairo.db\AMK\logs\log_wmtkassess_20070926_16_24_53.log"fo
r more information.
```

At this point all the XML files for the assessed endpoint have been generated. You generally do not need to modify anything in the XML file, unless you have some PACs installed that has been discovered by the assessment step.

Example 4-13 shows a sample XML file of an endpoint that has been assessed. This endpoint had only standard IBM Tivoli Monitoring V5.1.2 Tmw2kProfiles.

Example 4-13 Sample XML file of an assessed endpoint with only OS profiles

```
<?xml version="1.0" encoding="UTF-8"?>
<!--Copyright IBM Corporation 2006-->
<?xml-stylesheet type="text/xsl"
href="../../data/stylesheet/endpointAssess.xsl"?>
<endpointAssess aggregateStatus="0"
hostname="rp3410.itsc.austin.ibm.com" interp="hpux10" name="rp3410-ep"

xmlns="http://www.ibm.com/tivoli/itm/assess/endpoint"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"

xsi:schemaLocation="http://www.ibm.com/tivoli/itm/assess/endpoint
endpointAssess.xsd">
  <OSTargetAgent name="rp3410:KUX" product="KUX" status="NOT_DEPLOYED"
truncated="false">
    <SourceApplication sourceClass="endpoint" sourceObject="rp3410-ep">
      <Runningprofiles>
        <profile name="CUSTOM_PORT"/>
        <profile name="CUSTOM_PROCESS"/>
        <profile name="HPUX"/>
      </Runningprofiles>
    </SourceApplication>
  </OSTargetAgent>
</endpointAssess>

As you can see there are no values that must be edited
```

Example 4-14 shows a sample XML file of an endpoint that has been assessed. This endpoint had both standard IBM Tivoli Monitoring V5.1.2 Tmw2kProfiles and some coming from IBM Tivoli Monitoring for Databases - DB2 Component Software.

Example 4-14 Sample XML file of an assessed endpoint with OS and PACs profiles

```
<?xml version="1.0" encoding="UTF-8"?>
<!--Copyright IBM Corporation 2006-->
<?xml-stylesheet type="text/xsl"
href="../../data/stylesheet/endpointAssess.xsl"?>
<endpointAssess aggregateStatus="0"
hostname="cairo.itsc.austin.ibm.com" interp="w32-ix86" name="cairo-ep"
xmlns="http://www.ibm.com/tivoli/itm/assess/endpoint"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="http://www.ibm.com/tivoli/itm/assess/endpoint
endpointAssess.xsd">
  <OSTargetAgent name="Primary:CAIRO:NT" product="KNT"
status="NOT_DEPLOYED" truncated="false">
    <SourceApplication sourceClass="endpoint" sourceObject="cairo-ep">
      <Runningprofiles>
        <profile name="WINDOWS"/>
      </Runningprofiles>
    </SourceApplication>
  </OSTargetAgent>
  <TargetAgent deploy="true" name="DB2:CAIRO:UD" product="KUD"
status="NOT_DEPLOYED" truncated="false">
    <Context>
      <Variable name="ECDB2VERSION" value="8"/>
      <Variable name="@HOSTNAME" value="CAIRO"/>
      <Variable name="@INTERP" value="w32-ix86"/>
      <Variable name="ECDB2INSTANCE" value="DB2"/>
      <Variable name="ECDATABASE" value="MDIST2"/>
      <Variable name="ECNODENUM" value=""/>
    </Context>
    <Settings>
      <ParametricSetting name="INSTANCE"
sourceVariable="ECDB2INSTANCE"/>
      <UserSetting name="_WIN32_STARTUP_.Username"
value="AMK-REQUIRED-AMK"/>
      <UserSetting name="_WIN32_STARTUP_.Password" type="password"
value="AMK-REQUIRED-AMK"/>
    </Settings>
    <SourceApplication sourceClass="DB2DatabaseManager"
sourceObject="MDIST2@DB2@cairo-ep">
```

```
      <Runningprofiles>
        <profile name="DB2"/>
      </Runningprofiles>
    </SourceApplication>
    <SourceApplication sourceClass="DB2DatabaseManager"
sourceObject="PLANNER@DB2@cairo-ep">
      <Runningprofiles>
        <profile name="DB2"/>
      </Runningprofiles>
    </SourceApplication>
  </TargetAgent>
</endpointAssess>

In this case there are some elements with “AMK-REQUIRED-AMK” that must
be edited to match the PAC ResoueceModel configuration.
```

Step 6: Migrate endpoints – analyze

After creating the assess files, you should check that the number of files created corresponds with your expectations, given the input to the command.

Each endpoint assess file contains elements that describe the OS agent that will be deployed, and any application agent that is appropriate. You may decide you want to check this information.

Note: You only need to edit the endpoint assess file if an object, such as an application agent, requires a password, or some other user setting, as part of its configuration.

In these cases, the assess tool creates a UserSetting for the agent to contain the information. The UserSettings can be recognized because the field does not have a value (the text "AMK–REQUIRED–AMK" is displayed instead in the file, and an asterisk marks the field name in the GUI). Furthermore, if the field in question is a password, the type attribute of the UserSetting is set to a value of password, but this attribute is not displayed in the GUI, so use an editor to view the endpoint assess file, if you want to be sure that a UserSetting is classified as a password.

Step 7: Migrate endpoints – migrate

The migrate tool is used to:

- Deploy the OS monitoring agents to the endpoint
- Assign the endpoint to the target Tivoli Enterprise Monitoring Server identified in the baseline file

The endpoint now becomes a managed system that is part of the IBM Tivoli Monitoring V6.2 infrastructure. It also updates the endpoint assess file status.

If an agent is already on the endpoint as a result of being deployed it manually, or in a previous migration step, it is not deployed again.

Example 4-15 shows how to migrate one of the assessed endpoints.

Example 4-15 Endpoint migration

```
C:\Tivoli\db\cairo.db\AMK\analyze\endpoints>witmmtk migrate -x
rp3410-ep.xml -u
.
AMKUT0016I Processing the request.

AMKUT0057I Loading the infrastructure baseline file:
"C:\Tivoli\db\cairo.db\AMK\analyze\scans\1713357986.xml".
AMKUT7075I Processing endpoint: "rp3410-ep".
AMKUT7600I Processing the OS agent for endpoint "rp3410-ep". Note: this
operation might take up to 15 minutes to complete.
AMKUT7150I Processing endpoint "rp3410-ep": the agent "rp3410:KUX" was
deployed to the target endpoint.
AMKUT7010W The agent "rp3410:KUX" has already been deployed, but with a
different name "rp3410.itsc.austin.ibm.com:KUX" than that us
ed in the endpoint assess file. The assess file and infrastructure
baseline (if appropriate) have been updated with the new name.
.
AMKUT0010W The command completed with warnings. See log
"C:\Tivoli\db\cairo.db\AMK\logs\log_wmtkmigrate_20070927_13_20_41.log"
for more information.

The above warning message, simply means that the default managed system
name contained in the baseline file, rp3410:KUX has been converted into
the FQDN as result of the network resolution check during the
installation. The final managed system name is
rp3410.itsc.austin.ibm.com:KUX
```

After the migration, both the endpoint and the baseline XML files are updated with the deployment status.

Example 4-16 shows the final status of the XML file after the migration is complete.

Example 4-16 Updated XML file for the migrated endpoint

```
<?xml version="1.0" encoding="UTF-8"?>
<!--Copyright IBM Corporation 2006-->
<?xml-stylesheet type="text/xsl"
href="../../data/stylesheet/endpointAssess.xsl"?>
<endpointAssess aggregateStatus="100"
hostname="rp3410.itsc.austin.ibm.com" interp="hpux10" name="rp3410-ep"
xmlns="http://www.ibm.com/tivoli/itm/assess/endpoint"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="http://www.ibm.com/tivoli/itm/assess/endpoint
endpointAssess.xsd">
  <OSTargetAgent name="rp3410.itsc.austin.ibm.com:KUX" product="KUX"
status="DEPLOYED" truncated="false">
    <SourceApplication sourceClass="endpoint" sourceObject="rp3410-ep">
      <Runningprofiles>
        <profile name="CUSTOM_PORT"/>
        <profile name="CUSTOM_PROCESS"/>
        <profile name="HPUX"/>
      </Runningprofiles>
    </SourceApplication>
  </OSTargetAgent>
</endpointAssess>

As you can see, the status is now changed to “DEPLOYED”. It is
reflected into the baseline file and the migration process percentage
will be updated as well.
```

Agent deployment

The tool deploys agents to the endpoints, provided you have satisfied these prerequisites:

- Endpoint lcfd is installed on the hub monitoring server.

  You have installed the Tivoli Management Framework endpoint lcfd on the hub monitoring server.

- Agent images are prepared.

  The OS agent deployment uses the Remote Deployment function of V6.x, which requires the preparation of the agent images for deployment. Ensure you have followed all the steps to enable Remote Deployment, as described in the V6.x documentation.

Agent deployment elapsed times and timeout

When migrating endpoints, the tool has to physically deploy the code for the appropriate agents on the managed systems (endpoints) identified by the options. To maximize performance, the tool adopts a multi-threading approach, using 10 threads. It launches these threads for the first 10 endpoints to be migrated. As soon as a thread task completes, with the successful or unsuccessful deployment of the agents on the endpoint, it launches another migration using that thread. Endpoint migration can be a lengthy process, depending on how many and which agents are to be deployed, the network speed, and other factors. You should assume a minimum of one minute, but an endpoint with several application agents to deploy as well as the OS agent might take more than 20 minutes.

The **`migrate`** command employs a timeout for each agent deployment determined by the value of the MTK_TIMEOUT environment variable on the hub monitoring server, which has a default value of 10 minutes. This is deliberately set to twice the default timeout (300 seconds) used by the Remote Deployment function (for the **`tacmd createNode`** and **`tacmd addSystem`** commands). If you change this TIMEOUT value on the hub monitoring server, you should make a corresponding proportional change to the MTK_TIMEOUT environment variable.

Step 8: Migrate endpoints – status check

After the migration has completed, there are no obligatory tasks to be performed. However, you might want to verify the results of the migration for one or more endpoints, and you might want to monitor the progress of the entire migration.

1. If you want to verify the migration operation, open the output file from the **`witmmtk migrate`** command and verify that the OS agent was deployed to the endpoint. The aggregateStatus tag for the endpoint should specify "100" to indicate that the migration of the endpoint is 100% complete.
2. The status of the endpoint in the baseline infrastructure file should now be "DEPLOYED". You can view the baseline file to check this, and to check the overall infrastructure migration percentage.

Troubleshooting the remote deployment

The remote OS agent deployment with the migration toolkit leverages the Remote Deployment functionalities provided by IBM Tivoli Monitoring V6.2.

As stated in the previous sections, it uses the remote control endpoint installed on the hub Tivoli Enterprise Monitoring Server.

The log of the agent deployment is therefore found on the hub Tivoli Enterprise Monitoring Server, in the remote control endpoint installation file structure, identified by the LCF_DATDIR environment variable:

- `$LCF_DATDIR/LCFNEW/AMK/out_<hostname>_<timestamp>.log` for UNIX and Linux or
- `%LCF_DATDIR%\LCFNEW\AMK\out_<hostname>_<timestamp>.log` for Windows

Example 4-17 shows the output of an endpoint migration execution and the location of the agent deployment log file.

Example 4-17 Endpoint migration output and agent deployment log

```
MIGRATION COMMAND
The following command has been used to migrate the endpoint called
server2-ep to a UNIX OS agent using the migration toolkit:

C:\Tivoli\db\cairo.db\AMK\analyze\endpoints>witmmtk migrate -x
server2-ep.xml -u
.
AMKUT0016I Processing the request.

AMKUT0057I Loading the infrastructure baseline file:
"C:\Tivoli\db\cairo.db\AMK\analyze\scans\1713357986.xml".
AMKUT7075I Processing endpoint: "server2-ep".
AMKUT7600I Processing the OS agent for endpoint "server2-ep". Note:
this operation might take up to 15 minutes to complete.
AMKUT7150I Processing endpoint "server2-ep": the agent "server2:KUX"
was deployed to the target endpoint.
AMKUT7010W The agent "server2:KUX" has already been deployed, but with
a different name "server2.itsc.austin.ibm.com:KUX" than that
used in the endpoint assess file. The assess file and infrastructure
baseline (if appropriate) have been updated with the new name.
.
AMKUT0010W The command completed with warnings. See log
"C:\Tivoli\db\cairo.db\AMK\logs\log_wmtkmigrate_20070928_10_24_07.log"
for more information.

RESULTING XML FILE
The above warning regard the UNIX OS agent label that has been
converted using the FQDN format.
Once the endpoint has been migrated, the baseline file for the endpoint
is updated as well with the updated deployment status as shows in the
following XML file.

<?xml version="1.0" encoding="UTF-8"?>
```

```
<!--Copyright IBM Corporation 2006-->
<?xml-stylesheet type="text/xsl"
href="../../data/stylesheet/endpointAssess.xsl"?>
<endpointAssess aggregateStatus="100"
hostname="server2.itsc.austin.ibm.com" interp="aix4-r1"
name="server2-ep"

xmlns="http://www.ibm.com/tivoli/itm/assess/endpoint"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"

xsi:schemaLocation="http://www.ibm.com/tivoli/itm/assess/endpoint
endpointAssess.xsd">
  <OSTargetAgent name="server2.itsc.austin.ibm.com:KUX" product="KUX"
status="DEPLOYED" truncated="false">
    <SourceApplication sourceClass="endpoint"
sourceObject="server2-ep">
      <Runningprofiles>
        <profile name="AIX"/>
        <profile name="CUSTOM_PORT"/>
        <profile name="CUSTOM_PROCESS"/>
      </Runningprofiles>
    </SourceApplication>
  </OSTargetAgent>
</endpointAssess>

LOG FILE
On the hub Tivoli Enterprise Monitoring Server, edinburgh in this case,
there is a directory containing the log file for the remote agent
deployment operation. The path is /opt/Tivoli/lcf/dat/1/LCFNEW/AMK:

[root@edinburgh AMK]# tail -f
out_command_server2.itsc.austin.ibm.com_119099664
7.log
bin/tacmd login -s edinburgh.itsc.austin.ibm.com:1920 -u sysadmin -p
xxxxx

Validating user...

KUIC00007I: User sysadmin logged into server on
https://edinburgh.itsc.austin.ib
m.com:34562.
login status = 0
bin/tacmd createNode -h server2.itsc.austin.ibm.com -p PORT=1918
SERVER=toronto.
```

```
itsc.austin.ibm.com PROTOCOL=IP.PIPE -d /opt/IBM/ITM -u root -w xxxxx
-o TIMEOUT
=900
KUICCN001I Initializing required services...
KUICCN039I Attempting to connect to host server2.itsc.austin.ibm.com
...
KUICCN050I Distributing file 69 of 69 (156.9 MB / 157.1 MB)...
KUICCN002I Beginning the installation and configuration process...

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

As you can see in the above output, the command executed for the UNIX OS agent deployment is simply a **tacmd createNode** followed by parameters taken from the endpoint and infrastructure baseline XML files.
On the Tivoli Enterprise Monitoring Server endpoint, there is a script that is used to build the command that is then executed on the hub Tivoli Enterprise Monitoring Server itself.
The script, with its full path is called:

$LCF_DATDIR/LCFNEW/AMK/bin/createNode.sh
for UNIX and Linux or:
%LCF_DATDIR%\LCFNEW\AMK\bin\createNode.sh
for Windows.

4.4.4 Phase C: Migrating the profiles

As with the other phases in the migration process, this one is made of four steps: assess, analyze, migrate, and status check.

In this case, the resources to be migrated are profiles, and are called Tmw2kProfile for the Tivoli Management Framework; they represent the IBM Tivoli Monitoring V5.1.2 profile that contains the resource models.

After you perform these steps, the profiles will be migrated to situations.

Step 9: Migrate profiles – assess

The Assess tool is used, in this step, to prepare an XML file for each profile that creates, from the profile and the resource model mapping files, the situations that will later be deployed to the endpoints.

> **Attention:** You must not assess a profile until the endpoints to which it distributes have been migrated.

The full mapping logic is:

- The assessment is driven by the resource models defined on the server, therefore if a resource model has been updated on the server, but the updated version has not been deployed, it is the updated version that is assessed.
- The assessment uses the resource model mapping files supplied with the migration toolkit to map each V5 resource model indication to one or more V6 situations.
- Situations are created from the resource model logic and the resource model configuration (parameters, thresholds, and context variables).

Example 4-18 shows the execution of the step in our environment.

Example 4-18 MIgrate profiles - assess step

```
We started from the profiles list in our environment:

C:\>wlookup -ar Tmw2kProfile
AIX     1713357986.1.1367#TMW2K::All#
CUSTOM_PORT     1713357986.1.1378#TMW2K::All#
CUSTOM_PROCESS  1713357986.1.1376#TMW2K::All#
DB2     1713357986.1.1348#TMW2K::All#
HPUX    1713357986.1.1380#TMW2K::All#
LINUX   1713357986.1.1370#TMW2K::All#
SPR_NtProfile   1713357986.1.1063#TMW2K::All#
SPR_UNIXProfile 1713357986.1.1062#TMW2K::All#
WINDOWS 1713357986.1.1373#TMW2K::All#
tmw2kDefProfile 1713357986.1.1017#TMW2K::All#

From that list we selected the LINUX Tmw2kProfile to be assessed and we
created a file containing it:

C:\Tivoli\db\cairo.db\AMK\analyze\profiles>cat profiles.txt
@Tmw2kProfile:LINUX

We then run these commands to create the XML files for each profile:

C:\Tivoli\db\cairo.db\AMK\analyze\profiles>witmmtk assess -i
profiles.txt

AMKUT0016I Processing the request.
.
AMKUT5003I Loading the resource snapshot for the assessment.
```

```
AMKUT0057I Loading the infrastructure baseline file:
"C:\Tivoli\db\cairo.db\AMK\analyze\scans\1713357986.xml".
AMKUT5006I Starting the resource assessment.
AMKUT5074I Converting profile "LINUX".
AMKUT5078I Converting resource model "DMXCpu".
AMKUT5009I The number of "situations" created for resource model
"DMXCpu" is 6.
AMKUT5078I Converting resource model "DMXFileSystem".
AMKUT5009I The number of "situations" created for resource model
"DMXFileSystem" is 8.
AMKUT5078I Converting resource model "DMXMemory".
AMKUT5009I The number of "situations" created for resource model
"DMXMemory" is 6.
AMKUT5078I Converting resource model "DMXPhysicalDisk".
AMKUT5009I The number of "situations" created for resource model
"DMXPhysicalDisk" is 8.
AMKUT5007I All resources are assessed. Processing is complete.
.
AMKUT0008I The command completed successfully. See log
"C:\Tivoli\db\cairo.db\AMK\logs\log_wmtkassess_20071010_14_44_54.log"fo
r more information.
```

At this point, all the XML files for the assessed profiles have been generated.

You do not need to modify anything in these files that identify the situations that will be deployed. They are used as input to the migrate tool.

Example 4-19 shows a sample XML file of a profile that has been assessed.

Example 4-19 Sample XML file of an assessed profile

```
This XML file is the resutl of the assessment of the LINUX
Tmw2kProfile:

<?xml version="1.0" encoding="UTF-8"?>
<!--Copyright IBM Corporation 2006-->
<?xml-stylesheet type="text/xsl"
href="../../data/stylesheet/ProfileAssess.xsl"?>
<ProfileAssess aggregateStatus="0" comment="" name="LINUX"
xmlns="http://www.ibm.com/tivoli/itm/assess/profile"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="http://www.ibm.com/tivoli/itm/assess/profile
ProfileAssess.xsd">
  <ResourceModelAssess aggregateStatus="0" comment="" name="DMXCpu">
    <TargetSituation action="" advice=""
affinity="00f20000000000000000000000000000#m000000000" applicationID="KUX"
```

```
association="kux.01190_0_0:620" autoStart="true" description="High_WaitCPUUsage
LINUX ITM5 RM:DMXCpu" displayItem="" displaySeverity="Warning" distribution=""
eventSeverity="WARNING" multipleIntervals="NYN"
name="UX5_55a_HIGH_WAITCPUUSE_0" persistence="4" predicate="*IF ( *VALUE
System.Wait_I/O *GT 10 )" samplingIntervalDays="0" samplingIntervalTime="0:1:0"
status="NOT_DEPLOYED"/>
    <TargetSituation action="" advice=""
affinity="00f2000000000000000000000000000#m000000000" applicationID="KUX"
association="kux.01190_0_0:620" autoStart="true" description="Low_IdleCPUUsage
LINUX ITM5 RM:DMXCpu" displayItem="" displaySeverity="Warning" distribution=""
eventSeverity="WARNING" multipleIntervals="NYN" name="UX5_55a_LOW_IDLECPUUSE_0"
persistence="4" predicate="*IF ( *VALUE System.Idle_CPU *LT 10 )"
samplingIntervalDays="0" samplingIntervalTime="0:1:0" status="NOT_DEPLOYED"/>
    <TargetSituation action="" advice=""
affinity="00f2000000000000000000000000000#m000000000" applicationID="KUX"
association="kux.01190_0_0:620" autoStart="true" description="High_SysCPUUsage
LINUX ITM5 RM:DMXCpu" displayItem="" displaySeverity="Warning" distribution=""
eventSeverity="WARNING" multipleIntervals="NYN" name="UX5_55a_HIGH_SYSCPUUSE_0"
persistence="4" predicate="*IF ( *VALUE System.System_CPU *GT 80 )"
samplingIntervalDays="0" samplingIntervalTime="0:1:0" status="NOT_DEPLOYED"/>
    <TargetSituation action="" advice=""
affinity="000000000000000000000G000000000#m000000000" applicationID="KLZ"
association="klz.System_Information" autoStart="true"
description="High_WaitCPUUsage LINUX ITM5 RM:DMXCpu" displayItem=""
displaySeverity="Warning" distribution="" eventSeverity="WARNING"
multipleIntervals="NYN" name="LZ5_55a_HIGH_WAITCPUUSE_0" persistence="4"
predicate="*IF ( *VALUE Linux_CPU.Wait_IO_CPU *GT 10 )"
samplingIntervalDays="0" samplingIntervalTime="0:1:0" status="NOT_DEPLOYED"/>
    <TargetSituation action="" advice=""
affinity="000000000000000000000G000000000#m000000000" applicationID="KLZ"
association="klz.System_Information" autoStart="true"
description="Low_IdleCPUUsage LINUX ITM5 RM:DMXCpu" displayItem=""
displaySeverity="Warning" distribution="" eventSeverity="WARNING"
multipleIntervals="NYN" name="LZ5_55a_LOW_IDLECPUUSE_0" persistence="4"
predicate="*IF ( *VALUE Linux_CPU.Idle_CPU *LT 10 )" samplingIntervalDays="0"
samplingIntervalTime="0:1:0" status="NOT_DEPLOYED"/>
    <TargetSituation action="" advice=""
affinity="000000000000000000000G000000000#m000000000" applicationID="KLZ"
association="klz.System_Information" autoStart="true"
description="High_SysCPUUsage LINUX ITM5 RM:DMXCpu" displayItem=""
displaySeverity="Warning" distribution="" eventSeverity="WARNING"
multipleIntervals="NYN" name="LZ5_55a_HIGH_SYSCPUUSE_0" persistence="4"
predicate="*IF ( *VALUE Linux_CPU.System_CPU *GT 80 )" samplingIntervalDays="0"
samplingIntervalTime="0:1:0" status="NOT_DEPLOYED"/>
  </ResourceModelAssess>
  <ResourceModelAssess aggregateStatus="0" comment="" name="DMXFileSystem">
    <TargetSituation action="" advice=""
affinity="00f2000000000000000000000000000#m000000000" applicationID="KUX"
association="kux.00310_0_00" autoStart="true" description="LowPercSpcAvail
```

```
LINUX ITM5 RM:DMXFileSystem" displayItem="" displaySeverity="Critical"
distribution="" eventSeverity="CRITICAL" multipleIntervals="NYN"
name="UX5_55a_LowPercSpcAvail1_0" persistence="4" predicate="*IF ( *VALUE
Disk.Space_Available_Percent *LT 15 )" samplingIntervalDays="0"
samplingIntervalTime="0:2:0" status="NOT_DEPLOYED"/>
    <TargetSituation action="" advice=""
affinity="00f20000000000000000000000000000#m000000000" applicationID="KUX"
association="kux.00310_0_00" autoStart="true" description="LowKAvail LINUX ITM5
RM:DMXFileSystem" displayItem="" displaySeverity="Critical" distribution=""
eventSeverity="CRITICAL" multipleIntervals="NYN" name="UX5_55a_LowKAvail1_0"
persistence="4" predicate="*IF ( *VALUE Disk.Space_Available_MB *LT 7 )"
samplingIntervalDays="0" samplingIntervalTime="0:2:0" status="NOT_DEPLOYED"/>
    <TargetSituation action="" advice=""
affinity="00f20000000000000000000000000000#m000000000" applicationID="KUX"
association="kux.00310_0_00" autoStart="true" description="FragmentedFileSystem
LINUX ITM5 RM:DMXFileSystem" displayItem="" displaySeverity="Minor"
distribution="" eventSeverity="MINOR" multipleIntervals="NYN"
name="UX5_55a_FragFileSys1_0" persistence="4" predicate="*IF ( *VALUE
Disk.Space_Used_Percent *LT 85 *AND *VALUE Disk.Inodes_Used_Percent *GT 80 )"
samplingIntervalDays="0" samplingIntervalTime="0:2:0" status="NOT_DEPLOYED"/>
    <TargetSituation action="" advice=""
affinity="00f20000000000000000000000000000#m000000000" applicationID="KUX"
association="kux.00310_0_00" autoStart="true" description="LowPercInodesAvail
LINUX ITM5 RM:DMXFileSystem" displayItem="" displaySeverity="Warning"
distribution="" eventSeverity="WARNING" multipleIntervals="NYN"
name="UX5_55a_Low%InodesAvail1_0" persistence="4" predicate="*IF ( *VALUE
Disk.Inodes_Used_Percent *GE 80 )" samplingIntervalDays="0"
samplingIntervalTime="0:2:0" status="NOT_DEPLOYED"/>
    <TargetSituation action="" advice=""
affinity="0000000000000000000000G000000000#m000000000" applicationID="KLZ"
association="klz.Disk_Usage" autoStart="true" description="LowPercSpcAvail
LINUX ITM5 RM:DMXFileSystem" displayItem="" displaySeverity="Critical"
distribution="" eventSeverity="CRITICAL" multipleIntervals="NYN"
name="LZ5_55a_LowPercSpcAvail1_0" persistence="4" predicate="*IF ( *VALUE
Linux_Disk.Space_Available_Percent *LT 15 )" samplingIntervalDays="0"
samplingIntervalTime="0:2:0" status="NOT_DEPLOYED"/>
    <TargetSituation action="" advice=""
affinity="0000000000000000000000G000000000#m000000000" applicationID="KLZ"
association="klz.Disk_Usage" autoStart="true" description="LowKAvail LINUX ITM5
RM:DMXFileSystem" displayItem="" displaySeverity="Critical" distribution=""
eventSeverity="CRITICAL" multipleIntervals="NYN" name="LZ5_55a_LowKAvail1_0"
persistence="4" predicate="*IF ( *VALUE Linux_Disk.Space_Available *LT 7 )"
samplingIntervalDays="0" samplingIntervalTime="0:2:0" status="NOT_DEPLOYED"/>
    <TargetSituation action="" advice=""
affinity="0000000000000000000000G000000000#m000000000" applicationID="KLZ"
association="klz.Disk_Usage" autoStart="true" description="FragmentedFileSystem
LINUX ITM5 RM:DMXFileSystem" displayItem="" displaySeverity="Minor"
distribution="" eventSeverity="MINOR" multipleIntervals="NYN"
name="LZ5_55a_FragFileSys1_0" persistence="4" predicate="*IF ( *VALUE
Linux_Disk.Space_Used_Percent *LT 85 *AND *VALUE Linux_Disk.Inodes_Used_Percent
*GT 80 )" samplingIntervalDays="0" samplingIntervalTime="0:2:0"
status="NOT_DEPLOYED"/>
    <TargetSituation action="" advice=""
affinity="0000000000000000000000G000000000#m000000000" applicationID="KLZ"
association="klz.Disk_Usage" autoStart="true" description="LowPercInodesAvail
LINUX ITM5 RM:DMXFileSystem" displayItem="" displaySeverity="Warning"
distribution="" eventSeverity="WARNING" multipleIntervals="NYN"
name="LZ5_55a_Low%InodesAvail1_0" persistence="4" predicate="*IF ( *VALUE
Linux_Disk.Inodes_Available_Percent *LT 20 )" samplingIntervalDays="0"
samplingIntervalTime="0:2:0" status="NOT_DEPLOYED"/>
  </ResourceModelAssess>
  <ResourceModelAssess aggregateStatus="0" comment="" name="DMXMemory">
    <TargetSituation action="" advice=""
affinity="00f20000000000000000000000000000#m000000000" applicationID="KUX"
association="kux.01190_0_0:620" autoStart="true" description="LowStorage LINUX
ITM5 RM:DMXMemory" displayItem="" displaySeverity="Critical" distribution=""
eventSeverity="CRITICAL" multipleIntervals="NYN" name="UX5_55a_LOWSTORAGE_0"
persistence="20" predicate="*IF ( *VALUE UNIX_Memory.Virtual_Storage_Pct_Avail
*LT 40 )" samplingIntervalDays="0" samplingIntervalTime="0:1:0"
status="NOT_DEPLOYED"/>
    <TargetSituation action="" advice=""
affinity="00f20000000000000000000000000000#m000000000" applicationID="KUX"
association="kux.01190_0_0:620" autoStart="true" description="Thrashing LINUX
ITM5 RM:DMXMemory" displayItem="" displaySeverity="Critical" distribution=""
eventSeverity="CRITICAL" multipleIntervals="NYN" name="UX5_55a_THRASHING_0"
persistence="6" predicate="*IF ( *VALUE UNIX_Memory.Page_Ins *GT 400 *AND
*VALUE UNIX_Memory.Page_Outs *GT 400 )" samplingIntervalDays="0"
samplingIntervalTime="0:1:0" status="NOT_DEPLOYED"/>
    <TargetSituation action="" advice=""
affinity="00f20000000000000000000000000000#m000000000" applicationID="KUX"
association="kux.01190_0_0:620" autoStart="true" description="LowSwap LINUX
ITM5 RM:DMXMemory" displayItem="" displaySeverity="Critical" distribution=""
eventSeverity="CRITICAL" multipleIntervals="NYN" name="UX5_55a_LOWSWAP_0"
persistence="4" predicate="*IF ( *VALUE UNIX_Memory.Avail_Swap_Space_Pct *LT 30
)" samplingIntervalDays="0" samplingIntervalTime="0:1:0"
status="NOT_DEPLOYED"/>
    <TargetSituation action="" advice=""
affinity="0000000000000000000000G000000000#m000000000" applicationID="KLZ"
association="klz.System_Information" autoStart="true" description="LowStorage
LINUX ITM5 RM:DMXMemory" displayItem="" displaySeverity="Critical"
distribution="" eventSeverity="CRITICAL" multipleIntervals="NYN"
name="LZ5_55a_LOWSTORAGE_0" persistence="20" predicate="*IF ( *VALUE
Linux_VM_Stats.Virtual_Storage_Pct_Avail *LT 40 )" samplingIntervalDays="0"
samplingIntervalTime="0:1:0" status="NOT_DEPLOYED"/>
    <TargetSituation action="" advice=""
affinity="0000000000000000000000G000000000#m000000000" applicationID="KLZ"
association="klz.System_Information" autoStart="true" description="Thrashing
LINUX ITM5 RM:DMXMemory" displayItem="" displaySeverity="Critical"
```

```
distribution="" eventSeverity="CRITICAL" multipleIntervals="NYN"
name="LZ5_55a_THRASHING_0" persistence="6" predicate="*IF ( *VALUE
Linux_System_Statistics.Pages_paged_in_per_sec *GT 400 *AND *VALUE
Linux_System_Statistics.Pages_paged_out_per_sec *GT 400 )"
samplingIntervalDays="0" samplingIntervalTime="0:1:0" status="NOT_DEPLOYED"/>
    <TargetSituation action="" advice=""
affinity="0000000000000000000000G000000000#m000000000" applicationID="KLZ"
association="klz.System_Information" autoStart="true" description="LowSwap
LINUX ITM5 RM:DMXMemory" displayItem="" displaySeverity="Critical"
distribution="" eventSeverity="CRITICAL" multipleIntervals="NYN"
name="LZ5_55a_LOWSWAP_0" persistence="4" predicate="*IF ( *VALUE
Linux_VM_Stats.Swap_Pct_Avail *LT 30 )" samplingIntervalDays="0"
samplingIntervalTime="0:1:0" status="NOT_DEPLOYED"/>
  </ResourceModelAssess>
  <ResourceModelAssess aggregateStatus="0" comment="" name="DMXPhysicalDisk">
    <TargetSituation action="" advice=""
affinity="00f20000000000000000000000000000#m000000000" applicationID="KUX"
association="kux.00310_0_00" autoStart="true"
description="HighPhysicalDiskReadBytes LINUX ITM5 RM:DMXPhysicalDisk"
displayItem="Disk_Performance.Disk_Name_U" displaySeverity="Minor"
distribution="" multipleIntervals="NYN" name="UX5_55a_HIDISKREADBYTE_0"
persistence="10" predicate="*IF ( *VALUE Disk_Performance.Disk_Read_Bytes_Sec
*GT 1572864 *AND *VALUE Disk_Performance.Busy_Percent *GT 90 )"
samplingIntervalDays="0" samplingIntervalTime="0:2:0" status="NOT_DEPLOYED"/>
    <TargetSituation action="" advice=""
affinity="00f20000000000000000000000000000#m000000000" applicationID="KUX"
association="kux.00310_0_00" autoStart="true"
description="HighPhysicalDiskWriteBytes LINUX ITM5 RM:DMXPhysicalDisk"
displayItem="Disk_Performance.Disk_Name_U" displaySeverity="Minor"
distribution="" multipleIntervals="NYN" name="UX5_55a_HIDISKWRITBYTE_0"
persistence="10" predicate="*IF ( *VALUE Disk_Performance.Disk_Write_Bytes_Sec
*GT 1572864 *AND *VALUE Disk_Performance.Busy_Percent *GT 90 )"
samplingIntervalDays="0" samplingIntervalTime="0:2:0" status="NOT_DEPLOYED"/>
    <TargetSituation action="" advice=""
affinity="00f20000000000000000000000000000#m000000000" applicationID="KUX"
association="kux.00310_0_00" autoStart="true"
description="HighPhysicalPercentDiskTime LINUX ITM5 RM:DMXPhysicalDisk"
displayItem="Disk_Performance.Disk_Name_U" displaySeverity="Minor"
distribution="" eventSeverity="MINOR" multipleIntervals="NYN"
name="UX5_55a_HIPERCDISKTIME_0" persistence="10" predicate="*IF ( *VALUE
Disk_Performance.Busy_Percent *GT 90 )" samplingIntervalDays="0"
samplingIntervalTime="0:2:0" status="NOT_DEPLOYED"/>
    <TargetSituation action="" advice=""
affinity="00f20000000000000000000000000000#m000000000" applicationID="KUX"
association="kux.00310_0_00" autoStart="true"
description="HighPhysicalDiskXferRate LINUX ITM5 RM:DMXPhysicalDisk"
displayItem="Disk_Performance.Disk_Name_U" displaySeverity="Minor"
distribution="" multipleIntervals="NYN" name="UX5_55a_HIDISKXFERRATE_0"
persistence="10" predicate="*IF ( *VALUE Disk_Performance.Disk_Read_Bytes_Sec
*GT 1572864 *AND *VALUE Disk_Performance.Disk_Write_Bytes_Sec *GT 1572864 *AND
*VALUE Disk_Performance.Busy_Percent *GT 90 )" samplingIntervalDays="0"
samplingIntervalTime="0:2:0" status="NOT_DEPLOYED"/>
    <TargetSituation action="" advice=""
affinity="0000000000000000000000G000000000#m000000000" applicationID="KLZ"
association="klz.Disk_Usage" autoStart="true"
description="HighPhysicalDiskReadBytes LINUX ITM5 RM:DMXPhysicalDisk"
displayItem="Linux_IO_Ext.Device_Name" displaySeverity="Minor" distribution=""
multipleIntervals="NYN" name="LZ5_55a_HIDISKREADBYTE_0" persistence="10"
predicate="*IF ( *VALUE Linux_IO_Ext.Read_bytes_per_sec *GT 1572864 *AND *VALUE
Linux_IO_Ext.Cpu_Util *GT 90 )" samplingIntervalDays="0"
samplingIntervalTime="0:2:0" status="NOT_DEPLOYED"/>
    <TargetSituation action="" advice=""
affinity="0000000000000000000000G000000000#m000000000" applicationID="KLZ"
association="klz.Disk_Usage" autoStart="true"
description="HighPhysicalDiskWriteBytes LINUX ITM5 RM:DMXPhysicalDisk"
displayItem="Linux_IO_Ext.Device_Name" displaySeverity="Minor" distribution=""
multipleIntervals="NYN" name="LZ5_55a_HIDISKWRITBYTE_0" persistence="10"
predicate="*IF ( *VALUE Linux_IO_Ext.Write_bytes_per_sec *GT 1572864 *AND
*VALUE Linux_IO_Ext.Cpu_Util *GT 90 )" samplingIntervalDays="0"
samplingIntervalTime="0:2:0" status="NOT_DEPLOYED"/>
    <TargetSituation action="" advice=""
affinity="0000000000000000000000G000000000#m000000000" applicationID="KLZ"
association="klz.Disk_Usage" autoStart="true"
description="HighPhysicalPercentDiskTime LINUX ITM5 RM:DMXPhysicalDisk"
displayItem="Linux_IO_Ext.Device_Name" displaySeverity="Minor" distribution=""
eventSeverity="MINOR" multipleIntervals="NYN" name="LZ5_55a_HIPERCDISKTIME_0"
persistence="10" predicate="*IF ( *VALUE Linux_IO_Ext.Cpu_Util *GT 90 )"
samplingIntervalDays="0" samplingIntervalTime="0:2:0" status="NOT_DEPLOYED"/>
    <TargetSituation action="" advice=""
affinity="0000000000000000000000G000000000#m000000000" applicationID="KLZ"
association="klz.Disk_Usage" autoStart="true"
description="HighPhysicalDiskXferRate LINUX ITM5 RM:DMXPhysicalDisk"
displayItem="Linux_IO_Ext.Device_Name" displaySeverity="Minor" distribution=""
multipleIntervals="NYN" name="LZ5_55a_HIDISKXFERRATE_0" persistence="10"
predicate="*IF ( *VALUE Linux_IO_Ext.Read_bytes_per_sec *GT 1572864 *AND *VALUE
Linux_IO_Ext.Write_bytes_per_sec *GT 1572864 *AND *VALUE Linux_IO_Ext.Cpu_Util
*GT 90 )" samplingIntervalDays="0" samplingIntervalTime="0:2:0"
status="NOT_DEPLOYED"/>
  </ResourceModelAssess>
  <TECEventServers status="NOT_DEPLOYED">
    <TECEventServer name="9.3.5.205" port="0"/>
  </TECEventServers>
</ProfileAssess>
```

All the above situation will be created by the Migrate tool on the IBM Tivoli Monitoring V6.2 environment.

At the end of the file there is a stanza related to the TECEventServers similar to the following:

```
<TECEventServers status="NOT_DEPLOYED">
    <TECEventServer name="9.3.5.205" port="0"/>
</TECEventServers>
```

This stanza refers to the Tivoli Enterprise Console Event server the events will be sent to and its port.

Only secure Event Servers are listed in the baseline file. They are discovered with an internal call equivalent to a Name Registry lookup of the EventServer resource.

The Event Server described in the `eventServerLabel` is therefore mapped to a CORBA name.

During the assess phase for the profiles, a secure event server naming convention (CORBA name) does not have any meaning cause IBM Tivoli Monitoring V6.2 does not use the Tivoli Management Framework at all, so the event server is converted in a non-secure event server. The broadcast or failover techniques defined in the Tmw2kProfiles are maintained, but the secure event server that is in the baseline file is converted to the non-secure format: hostname+port.

Note: If you do not want to use a specific event server that is defined in the Tmw2kProfile, you can either remove the whole stanza (Event Server) from the infrastructure baseline file or leave the eventServerPort and eventServerTarget empty.

All the event servers in the Tmw2kProfile are resolved one by one by the assess tool: if a secure server (CORBA name definition) is defined, but no references in the infrastructure baseline file are found, it is skipped. If found, it is converted to the non-secure format of ip+port.

Step 10: Migrate profiles – analyze

After creating the assess files, you should check that the number of files created corresponds with your expectations, given the input to the command.

Each profile assess file contains elements that describe the situations that will be created. They also describe the monitoring schedule that will be applied when the object has been migrated.

You may decide you want to check this information. For further details, refer to:

- Chapter 18, “Assess data file XML reference”, in *Upgrading from IBM Tivoli Monitoring V5.1.2*, GC32-1976, which describes the assess file, and gives details on how you can view it. It also explains the naming convention for situations.
- “Profile and situation validation techniques” in *Upgrading from IBM Tivoli Monitoring V5.1.2*, GC32-1976, which describes methods you can use to predict and validate the mapping of V5 resource indications to V6 situations.

Step 11: Migrate profiles – migrate

The migrate tool is used to create the V6 situations and update the profile assess file status.

Example 4-20 shows the steps used in our environment to migrate the profiles

Example 4-20 Profiles migration

```
With the -d option the command creates the situation for all the
available profile assess files in the profiles directory.

C:\Tivoli\db\cairo.db\AMK\analyze\profiles>witmmtk migrate -d
"%DBDIR%\AMK\analyze\profiles" -u
.
AMKUT0016I Processing the request.

AMKUT0057I Loading the infrastructure baseline file:
"C:\Tivoli\db\cairo.db\AMK\analyze\scans\1713357986.xml".
AMKUT7002E The file
"C:\Tivoli\db\cairo.db\AMK\analyze\profiles\profiles.txt" is not a
valid file.
AMKUT7076I Processing profile: "AIX".
AMKUT7078I Migrating resource model "DMXCpu" for hub monitoring server
"HUB_TEMS".
AMKUT7100I The situation "UX5_557_HIGH_WAITCPUUSE_0" was added.
AMKUT7100I The situation "UX5_557_LOW_IDLECPUUSE_0" was added.
AMKUT7100I The situation "UX5_557_HIGH_SYSCPUUSE_0" was added.
AMKUT7100I The situation "LZ5_557_HIGH_WAITCPUUSE_0" was added.
AMKUT7100I The situation "LZ5_557_LOW_IDLECPUUSE_0" was added.
AMKUT7100I The situation "LZ5_557_HIGH_SYSCPUUSE_0" was added.
AMKUT7078I Migrating resource model "DMXFileSystem" for hub monitoring
server "HUB_TEMS".
AMKUT7100I The situation "UX5_557_LowPercSpcAvail1_0" was added.
AMKUT7100I The situation "UX5_557_LowKAvail1_0" was added.
AMKUT7100I The situation "UX5_557_FragFileSys1_0" was added.
```

```
AMKUT7100I The situation "UX5_557_Low%InodesAvail1_0" was added.
AMKUT7100I The situation "LZ5_557_LowPercSpcAvail1_0" was added.
AMKUT7100I The situation "LZ5_557_LowKAvail1_0" was added.
AMKUT7100I The situation "LZ5_557_FragFileSys1_0" was added.
AMKUT7100I The situation "LZ5_557_Low%InodesAvail1_0" was added.
AMKUT7078I Migrating resource model "DMXMemory" for hub monitoring
server "HUB_TEMS".
AMKUT7100I The situation "UX5_557_LOWSTORAGE_0" was added.
AMKUT7100I The situation "UX5_557_THRASHING_0" was added.
AMKUT7100I The situation "UX5_557_LOWSWAP_0" was added.
AMKUT7100I The situation "LZ5_557_LOWSTORAGE_0" was added.
AMKUT7100I The situation "LZ5_557_THRASHING_0" was added.
AMKUT7100I The situation "LZ5_557_LOWSWAP_0" was added.
AMKUT7078I Migrating resource model "DMXPhysicalDisk" for hub
monitoring server "HUB_TEMS".
AMKUT7100I The situation "UX5_557_HIDISKREADBYTE_0" was added.
AMKUT7100I The situation "UX5_557_HIDISKWRITBYTE_0" was added.
AMKUT7100I The situation "UX5_557_HIPERCDISKTIME_0" was added.
AMKUT7100I The situation "UX5_557_HIDISKXFERRATE_0" was added.
AMKUT7100I The situation "LZ5_557_HIDISKREADBYTE_0" was added.
AMKUT7100I The situation "LZ5_557_HIDISKWRITBYTE_0" was added.
AMKUT7100I The situation "LZ5_557_HIPERCDISKTIME_0" was added.
AMKUT7100I The situation "LZ5_557_HIDISKXFERRATE_0" was added.
AMKUT7076I Processing profile: "DB2".
AMKUT7078I Migrating resource model "DB2DatabaseStatus" for hub
monitoring server "HUB_TEMS".
AMKUT7100I The situation "UD5_544_HiCurrentConnAg_0" was added.
AMKUT7100I The situation "UD5_544_HiCurrentConnAg_1" was added.
AMKUT7100I The situation "UD5_544_HiSpaceUsedDmsAg_0" was added.
AMKUT7100I The situation "UD5_544_HiSpaceUsedDmsAg_1" was added.
AMKUT7100I The situation "UD5_544_HiSpaceUsedSmsAg_0" was added.
AMKUT7100I The situation "UD5_544_HiSpaceUsedSmsAg_1" was added.
AMKUT7100I The situation "UD5_544_RestorePendingAg_0" was added.
AMKUT7100I The situation "UD5_544_RestorePendingAg_1" was added.
AMKUT7100I The situation "UD5_544_HiConnWaitAtHostAg_0" was added.
AMKUT7100I The situation "UD5_544_HiConnWaitAtHostAg_1" was added.
AMKUT7100I The situation "UD5_544_HiRecentConnRespAg_0" was added.
AMKUT7100I The situation "UD5_544_HiRecentConnRespAg_1" was added.
AMKUT7100I The situation "UD5_544_HiConnErrorsAg_0" was added.
AMKUT7100I The situation "UD5_544_HiConnErrorsAg_1" was added.
AMKUT7100I The situation "UD5_544_LastBackupOldAg_0" was added.
AMKUT7100I The situation "UD5_544_LastBackupOldAg_1" was added.
AMKUT7100I The situation "UD5_544_HiPctConnUsedAg_0" was added.
AMKUT7100I The situation "UD5_544_HiPctConnUsedAg_1" was added.
AMKUT7100I The situation "UD5_544_TsStatNotNormalAg_0" was added.
```

```
AMKUT7100I The situation "UD5_544_TsStatNotNormalAg_1" was added.
AMKUT7076I Processing profile: "HPUX".
AMKUT7078I Migrating resource model "DMXCpu" for hub monitoring server
"HUB_TEMS".
AMKUT7100I The situation "UX5_564_HIGH_WAITCPUUSE_0" was added.
AMKUT7100I The situation "UX5_564_LOW_IDLECPUUSE_0" was added.
AMKUT7100I The situation "UX5_564_HIGH_SYSCPUUSE_0" was added.
AMKUT7100I The situation "LZ5_564_HIGH_WAITCPUUSE_0" was added.
AMKUT7100I The situation "LZ5_564_LOW_IDLECPUUSE_0" was added.
AMKUT7100I The situation "LZ5_564_HIGH_SYSCPUUSE_0" was added.
AMKUT7078I Migrating resource model "DMXFileSystem" for hub monitoring
server "HUB_TEMS".
AMKUT7100I The situation "UX5_564_LowPercSpcAvail1_0" was added.
AMKUT7100I The situation "UX5_564_LowKAvail1_0" was added.
AMKUT7100I The situation "UX5_564_FragFileSys1_0" was added.
AMKUT7100I The situation "UX5_564_Low%InodesAvail1_0" was added.
AMKUT7100I The situation "LZ5_564_LowPercSpcAvail1_0" was added.
AMKUT7100I The situation "LZ5_564_LowKAvail1_0" was added.
AMKUT7100I The situation "LZ5_564_FragFileSys1_0" was added.
AMKUT7100I The situation "LZ5_564_Low%InodesAvail1_0" was added.
AMKUT7078I Migrating resource model "DMXMemory" for hub monitoring
server "HUB_TEMS".
AMKUT7100I The situation "UX5_564_LOWSTORAGE_0" was added.
AMKUT7100I The situation "UX5_564_THRASHING_0" was added.
AMKUT7100I The situation "UX5_564_LOWSWAP_0" was added.
AMKUT7100I The situation "LZ5_564_LOWSTORAGE_0" was added.
AMKUT7100I The situation "LZ5_564_THRASHING_0" was added.
AMKUT7100I The situation "LZ5_564_LOWSWAP_0" was added.
AMKUT7078I Migrating resource model "DMXPhysicalDisk" for hub
monitoring server "HUB_TEMS".
AMKUT7100I The situation "UX5_564_HIDISKREADBYTE_0" was added.
AMKUT7100I The situation "UX5_564_HIDISKWRITBYTE_0" was added.
AMKUT7100I The situation "UX5_564_HIPERCDISKTIME_0" was added.
AMKUT7100I The situation "UX5_564_HIDISKXFERRATE_0" was added.
AMKUT7100I The situation "LZ5_564_HIDISKREADBYTE_0" was added.
AMKUT7100I The situation "LZ5_564_HIDISKWRITBYTE_0" was added.
AMKUT7100I The situation "LZ5_564_HIPERCDISKTIME_0" was added.
AMKUT7100I The situation "LZ5_564_HIDISKXFERRATE_0" was added.
AMKUT7076I Processing profile: "LINUX".
AMKUT7078I Migrating resource model "DMXCpu" for hub monitoring server
"HUB_TEMS".
AMKUT7100I The situation "UX5_55a_HIGH_WAITCPUUSE_0" was added.
AMKUT7100I The situation "UX5_55a_LOW_IDLECPUUSE_0" was added.
AMKUT7100I The situation "UX5_55a_HIGH_SYSCPUUSE_0" was added.
AMKUT7100I The situation "LZ5_55a_HIGH_WAITCPUUSE_0" was added.
```

```
AMKUT7100I The situation "LZ5_55a_LOW_IDLECPUUSE_0" was added.
AMKUT7100I The situation "LZ5_55a_HIGH_SYSCPUUSE_0" was added.
AMKUT7078I Migrating resource model "DMXFileSystem" for hub monitoring
server "HUB_TEMS".
AMKUT7100I The situation "UX5_55a_LowPercSpcAvail1_0" was added.
AMKUT7100I The situation "UX5_55a_LowKAvail1_0" was added.
AMKUT7100I The situation "UX5_55a_FragFileSys1_0" was added.
AMKUT7100I The situation "UX5_55a_Low%InodesAvail1_0" was added.
AMKUT7100I The situation "LZ5_55a_LowPercSpcAvail1_0" was added.
AMKUT7100I The situation "LZ5_55a_LowKAvail1_0" was added.
AMKUT7100I The situation "LZ5_55a_FragFileSys1_0" was added.
AMKUT7100I The situation "LZ5_55a_Low%InodesAvail1_0" was added.
AMKUT7078I Migrating resource model "DMXMemory" for hub monitoring
server "HUB_TEMS".
AMKUT7100I The situation "UX5_55a_LOWSTORAGE_0" was added.
AMKUT7100I The situation "UX5_55a_THRASHING_0" was added.
AMKUT7100I The situation "UX5_55a_LOWSWAP_0" was added.
AMKUT7100I The situation "LZ5_55a_LOWSTORAGE_0" was added.
AMKUT7100I The situation "LZ5_55a_THRASHING_0" was added.
AMKUT7100I The situation "LZ5_55a_LOWSWAP_0" was added.
AMKUT7078I Migrating resource model "DMXPhysicalDisk" for hub
monitoring server "HUB_TEMS".
AMKUT7100I The situation "UX5_55a_HIDISKREADBYTE_0" was added.
AMKUT7100I The situation "UX5_55a_HIDISKWRITBYTE_0" was added.
AMKUT7100I The situation "UX5_55a_HIPERCDISKTIME_0" was added.
AMKUT7100I The situation "UX5_55a_HIDISKXFERRATE_0" was added.
AMKUT7100I The situation "LZ5_55a_HIDISKREADBYTE_0" was added.
AMKUT7100I The situation "LZ5_55a_HIDISKWRITBYTE_0" was added.
AMKUT7100I The situation "LZ5_55a_HIPERCDISKTIME_0" was added.
AMKUT7100I The situation "LZ5_55a_HIDISKXFERRATE_0" was added.
AMKUT7076I Processing profile: "WINDOWS".
AMKUT7078I Migrating resource model "TMW_Processor" for hub monitoring
server "HUB_TEMS".
AMKUT7100I The situation "NT5_55d_BusyHardware_0" was added.
AMKUT7100I The situation "NT5_55d_CpuCantKeepUp_0" was added.
AMKUT7100I The situation "NT5_55d_HighPctUsageDelta_0" was added.
AMKUT7100I The situation "NT5_55d_HighProcesses_0" was added.
AMKUT7100I The situation "NT5_55d_HwKeepingCpuBusy_0" was added.
AMKUT7100I The situation "NT5_55d_ProcessorBusy_0" was added.
AMKUT7078I Migrating resource model "TMW_LogicalDisk" for hub
monitoring server "HUB_TEMS".
AMKUT7100I The situation "NT5_55d_HighLogDiskPctTime_0" was added.
AMKUT7100I The situation "NT5_55d_HighLogDiskXferRat_0" was added.
AMKUT7100I The situation "NT5_55d_HighLogDiskReadByt_0" was added.
AMKUT7100I The situation "NT5_55d_LowLogDiskSpace_0" was added.
```

```
AMKUT7100I The situation "NT5_55d_LogDiskPossFrag_0" was added.
AMKUT7100I The situation "NT5_55d_SlowLogDiskDrive_0" was added.
AMKUT7100I The situation "NT5_55d_HighLogDiskWritByt_0" was added.
AMKUT7078I Migrating resource model "TMW_MemoryModel" for hub
monitoring server "HUB_TEMS".
AMKUT7100I The situation "NT5_55d_HighPaging_0" was added.
AMKUT7100I The situation "NT5_55d_LowAvailMemory_0" was added.
AMKUT7100I The situation "NT5_55d_LowAvailHardPaging_0" was added.
AMKUT7100I The situation "NT5_55d_LowAvailManyProbs_0" was added.
AMKUT7100I The situation "NT5_55d_LowAvailPageResize_0" was added.
AMKUT7100I The situation "NT5_55d_LowAvailSoftPaging_0" was added.
AMKUT7100I The situation "NT5_55d_LowAvailHighCache_0" was added.
AMKUT7100I The situation "NT5_55d_LowAvailHighWrkSet_0" was added.
AMKUT7100I The situation "NT5_55d_LowAvailSmPageFile_0" was added.
AMKUT7100I The situation "NT5_55d_LowCopyReadHits_0" was added.
AMKUT7100I The situation "NT5_55d_LowDataMapHits_0" was added.
AMKUT7100I The situation "NT5_55d_LowMDLReadHits_0" was added.
AMKUT7100I The situation "NT5_55d_LowPinReadHits_0" was added.
AMKUT7100I The situation "NT5_55d_MemoryLeakPrivate_0" was added.
AMKUT7100I The situation "NT5_55d_MemoryLeakSysCode_0" was added.
AMKUT7100I The situation "NT5_55d_MemoryLeakSysDrive_0" was added.
AMKUT7100I The situation "NT5_55d_PageFileResizing_0" was added.
.
AMKUT0010W The command completed with warnings. See log
"C:\Tivoli\db\cairo.db\AMK\logs\log_wmtkmigrate_20071010_16_03_14.log"
for more information.

The warning message is simply caused by the presence of the
“C:\Tivoli\db\cairo.db\AMK\analyze\profiles\profiles.txt” file in the
profiles directory: this is not a valid XML file so tool identify it is
not valid.

The command migrated all these Tmw2kProfiles that have been previously
assessed:

AIX     1713357986.1.1367#TMW2K::All#
DB2     1713357986.1.1348#TMW2K::All#
HPUX    1713357986.1.1380#TMW2K::All#
LINUX   1713357986.1.1370#TMW2K::All#
WINDOWS 1713357986.1.1373#TMW2K::All#
```

After the migration, the assess file is updated to show the status of the migration, as shown in Example 4-21 on page 245.

Example 4-21 Updated XML file for the migrated profiles

```
This example shows an updated XML file for an IBM Tivoli Monitoring for
Databases - DB2 Component Software Tmw2kProfile called DB2:

<?xml version="1.0" encoding="UTF-8"?>
<!--Copyright IBM Corporation 2006-->
<?xml-stylesheet type="text/xsl"
href="../../data/stylesheet/ProfileAssess.xsl"?>
<ProfileAssess aggregateStatus="100" comment="" name="DB2"
xmlns="http://www.ibm.com/tivoli/itm/assess/profile"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="http://www.ibm.com/tivoli/itm/assess/profile
ProfileAssess.xsd">
  <ResourceModelAssess aggregateStatus="100" comment=""
name="DB2DatabaseStatus">
    <TargetSituation action="" advice=""
affinity="0000000000000000000W00000000000#u000000000" applicationID="KUD"
association="zkud.KUDDBASEGROUP00:620" autoStart="true"
description="DB2_High_CurrentConnections DB2 ITM5 RM:DB2DatabaseStatus"
displayItem="" displaySeverity="Warning" distribution=""
multipleIntervals="NYN" name="UD5_544_HiCurrentConnAg_0" persistence="3"
predicate="*IF ( *VALUE KUD_DB2_DCS_Database.db_name_U *EQ 'MDIST2' *AND *VALUE
KUD_DB2_DCS_Database.db_partition *EQ 'Aggregated' *AND *VALUE
KUD_DB2_DCS_Database.gw_cur_cons *GT 50 )" samplingIntervalDays="0"
samplingIntervalTime="0:10:0" status="DEPLOYED">
      <SourceApplication name="MDIST2@DB2@cairo-ep"/>
    </TargetSituation>
    <TargetSituation action="" advice=""
affinity="0000000000000000000W00000000000#u000000000" applicationID="KUD"
association="zkud.KUDDBASEGROUP00:620" autoStart="true"
description="DB2_High_CurrentConnections DB2 ITM5 RM:DB2DatabaseStatus"
displayItem="" displaySeverity="Warning" distribution=""
multipleIntervals="NYN" name="UD5_544_HiCurrentConnAg_1" persistence="3"
predicate="*IF ( *VALUE KUD_DB2_DCS_Database.db_name_U *EQ 'PLANNER' *AND
*VALUE KUD_DB2_DCS_Database.db_partition *EQ 'Aggregated' *AND *VALUE
KUD_DB2_DCS_Database.gw_cur_cons *GT 50 )" samplingIntervalDays="0"
samplingIntervalTime="0:10:0" status="DEPLOYED">
      <SourceApplication name="PLANNER@DB2@cairo-ep"/>
    </TargetSituation>
    <TargetSituation action="" advice=""
affinity="0000000000000000000W00000000000#u000000000" applicationID="KUD"
association="zkud.TableSpace:620" autoStart="true"
description="DB2_High_SpaceUsedDMSTablespace DB2 ITM5 RM:DB2DatabaseStatus"
displayItem="KUDTABSPACE.TABLESPACE_NAME_U" displaySeverity="Critical"
distribution="" multipleIntervals="NYN" name="UD5_544_HiSpaceUsedDmsAg_0"
persistence="1" predicate="*IF ( *VALUE KUDTABSPACE.DB_NAME_U *EQ 'MDIST2' *AND
*VALUE KUDTABSPACE.db_partition *EQ 'Aggregated' *AND *VALUE
KUDTABSPACE.TABLESPACE_NAME_U *IN ('*') *AND *VALUE
KUDTABSPACE.SPACE_USED_DMS_TABLE_PCT *GT 85 )" samplingIntervalDays="0"
samplingIntervalTime="0:10:0" status="DEPLOYED">
      <SourceApplication name="MDIST2@DB2@cairo-ep"/>
    </TargetSituation>
    <TargetSituation action="" advice=""
affinity="00000000000000000000W00000000000#u000000000" applicationID="KUD"
association="zkud.TableSpace:620" autoStart="true"
description="DB2_High_SpaceUsedDMSTablespace DB2 ITM5 RM:DB2DatabaseStatus"
displayItem="KUDTABSPACE.TABLESPACE_NAME_U" displaySeverity="Critical"
distribution="" multipleIntervals="NYN" name="UD5_544_HiSpaceUsedDmsAg_1"
persistence="1" predicate="*IF ( *VALUE KUDTABSPACE.DB_NAME_U *EQ 'PLANNER'
*AND *VALUE KUDTABSPACE.db_partition *EQ 'Aggregated' *AND *VALUE
KUDTABSPACE.TABLESPACE_NAME_U *IN ('*') *AND *VALUE
KUDTABSPACE.SPACE_USED_DMS_TABLE_PCT *GT 85 )" samplingIntervalDays="0"
samplingIntervalTime="0:10:0" status="DEPLOYED">
      <SourceApplication name="PLANNER@DB2@cairo-ep"/>
    </TargetSituation>
    <TargetSituation action="" advice=""
affinity="00000000000000000000W00000000000#u000000000" applicationID="KUD"
association="zkud.TableSpace:620" autoStart="true"
description="DB2_High_SpaceUsedSMSTablespace DB2 ITM5 RM:DB2DatabaseStatus"
displayItem="KUDTABSPACE.TABLESPACE_NAME_U" displaySeverity="Critical"
distribution="" multipleIntervals="NYN" name="UD5_544_HiSpaceUsedSmsAg_0"
persistence="1" predicate="*IF ( *VALUE KUDTABSPACE.DB_NAME_U *EQ 'MDIST2' *AND
*VALUE KUDTABSPACE.db_partition *EQ 'Aggregated' *AND *VALUE
KUDTABSPACE.TABLESPACE_NAME_U *IN ('*') *AND *VALUE
KUDTABSPACE.SPACE_USED_SMS_TABLE *GT 50000 )" samplingIntervalDays="0"
samplingIntervalTime="0:10:0" status="DEPLOYED">
      <SourceApplication name="MDIST2@DB2@cairo-ep"/>
    </TargetSituation>
    <TargetSituation action="" advice=""
affinity="00000000000000000000W00000000000#u000000000" applicationID="KUD"
association="zkud.TableSpace:620" autoStart="true"
description="DB2_High_SpaceUsedSMSTablespace DB2 ITM5 RM:DB2DatabaseStatus"
displayItem="KUDTABSPACE.TABLESPACE_NAME_U" displaySeverity="Critical"
distribution="" multipleIntervals="NYN" name="UD5_544_HiSpaceUsedSmsAg_1"
persistence="1" predicate="*IF ( *VALUE KUDTABSPACE.DB_NAME_U *EQ 'PLANNER'
*AND *VALUE KUDTABSPACE.db_partition *EQ 'Aggregated' *AND *VALUE
KUDTABSPACE.TABLESPACE_NAME_U *IN ('*') *AND *VALUE
KUDTABSPACE.SPACE_USED_SMS_TABLE *GT 50000 )" samplingIntervalDays="0"
samplingIntervalTime="0:10:0" status="DEPLOYED">
      <SourceApplication name="PLANNER@DB2@cairo-ep"/>
    </TargetSituation>
    <TargetSituation action="" advice=""
affinity="00000000000000000000W00000000000#u000000000" applicationID="KUD"
association="zkud.KUDDBASEGROUP00:620" autoStart="true"
description="DB2_True_RestorePending DB2 ITM5 RM:DB2DatabaseStatus"
displayItem="KUDDBASEGROUP01.db_name_U" displaySeverity="Critical"
distribution="" eventSeverity="CRITICAL" multipleIntervals="NYN"
```

```
name="UD5_544_RestorePendingAg_0" persistence="1" predicate="*IF ( *VALUE
KUDDBASEGROUP01.db_name_U *EQ 'MDIST2' *AND *VALUE KUDDBASEGROUP01.db_partition
*EQ 'Aggregated' *AND *VALUE KUDDBASEGROUP01.restore_pending *EQ 'TRUE' )"
samplingIntervalDays="0" samplingIntervalTime="0:10:0" status="DEPLOYED">
      <SourceApplication name="MDIST2@DB2@cairo-ep"/>
    </TargetSituation>
    <TargetSituation action="" advice=""
affinity="0000000000000000000W00000000000#u000000000" applicationID="KUD"
association="zkud.KUDDBASEGROUP00:620" autoStart="true"
description="DB2_True_RestorePending DB2 ITM5 RM:DB2DatabaseStatus"
displayItem="KUDDBASEGROUP01.db_name_U" displaySeverity="Critical"
distribution="" eventSeverity="CRITICAL" multipleIntervals="NYN"
name="UD5_544_RestorePendingAg_1" persistence="1" predicate="*IF ( *VALUE
KUDDBASEGROUP01.db_name_U *EQ 'PLANNER' *AND *VALUE
KUDDBASEGROUP01.db_partition *EQ 'Aggregated' *AND *VALUE
KUDDBASEGROUP01.restore_pending *EQ 'TRUE' )" samplingIntervalDays="0"
samplingIntervalTime="0:10:0" status="DEPLOYED">
      <SourceApplication name="PLANNER@DB2@cairo-ep"/>
    </TargetSituation>
    <TargetSituation action="" advice=""
affinity="0000000000000000000W00000000000#u000000000" applicationID="KUD"
association="zkud.KUDDBASEGROUP00:620" autoStart="true"
description="DB2_High_ConnWaitingForHost DB2 ITM5 RM:DB2DatabaseStatus"
displayItem="" displaySeverity="Warning" distribution=""
eventSeverity="WARNING" multipleIntervals="NYN"
name="UD5_544_HiConnWaitAtHostAg_0" persistence="3" predicate="*IF ( *VALUE
KUD_DB2_DCS_Database.db_name_U *EQ 'MDIST2' *AND *VALUE
KUD_DB2_DCS_Database.db_partition *EQ 'Aggregated' *AND *VALUE
KUD_DB2_DCS_Database.gw_cons_wait_host *GT 30 )" samplingIntervalDays="0"
samplingIntervalTime="0:10:0" status="DEPLOYED">
      <SourceApplication name="MDIST2@DB2@cairo-ep"/>
    </TargetSituation>
    <TargetSituation action="" advice=""
affinity="0000000000000000000W00000000000#u000000000" applicationID="KUD"
association="zkud.KUDDBASEGROUP00:620" autoStart="true"
description="DB2_High_ConnWaitingForHost DB2 ITM5 RM:DB2DatabaseStatus"
displayItem="" displaySeverity="Warning" distribution=""
eventSeverity="WARNING" multipleIntervals="NYN"
name="UD5_544_HiConnWaitAtHostAg_1" persistence="3" predicate="*IF ( *VALUE
KUD_DB2_DCS_Database.db_name_U *EQ 'PLANNER' *AND *VALUE
KUD_DB2_DCS_Database.db_partition *EQ 'Aggregated' *AND *VALUE
KUD_DB2_DCS_Database.gw_cons_wait_host *GT 30 )" samplingIntervalDays="0"
samplingIntervalTime="0:10:0" status="DEPLOYED">
      <SourceApplication name="PLANNER@DB2@cairo-ep"/>
    </TargetSituation>
    <TargetSituation action="" advice=""
affinity="0000000000000000000W00000000000#u000000000" applicationID="KUD"
association="zkud.KUDDBASEGROUP00:620" autoStart="true"
description="DB2_High_MostRecentConnectResponse DB2 ITM5 RM:DB2DatabaseStatus"
```

```
displayItem="" displaySeverity="Warning" distribution=""
eventSeverity="WARNING" multipleIntervals="NYN"
name="UD5_544_HiRecentConnRespAg_0" persistence="3" predicate="*IF ( *VALUE
KUD_DB2_DCS_Database.db_name_U *EQ 'MDIST2' *AND *VALUE
KUD_DB2_DCS_Database.db_partition *EQ 'Aggregated' *AND *VALUE
KUD_DB2_DCS_Database.recent_con_rsp_time *GT 5 )" samplingIntervalDays="0"
samplingIntervalTime="0:10:0" status="DEPLOYED">
      <SourceApplication name="MDIST2@DB2@cairo-ep"/>
    </TargetSituation>
    <TargetSituation action="" advice=""
affinity="00000000000000000000W00000000000#u000000000" applicationID="KUD"
association="zkud.KUDDBASEGROUP00:620" autoStart="true"
description="DB2_High_MostRecentConnectResponse DB2 ITM5 RM:DB2DatabaseStatus"
displayItem="" displaySeverity="Warning" distribution=""
eventSeverity="WARNING" multipleIntervals="NYN"
name="UD5_544_HiRecentConnRespAg_1" persistence="3" predicate="*IF ( *VALUE
KUD_DB2_DCS_Database.db_name_U *EQ 'PLANNER' *AND *VALUE
KUD_DB2_DCS_Database.db_partition *EQ 'Aggregated' *AND *VALUE
KUD_DB2_DCS_Database.recent_con_rsp_time *GT 5 )" samplingIntervalDays="0"
samplingIntervalTime="0:10:0" status="DEPLOYED">
      <SourceApplication name="PLANNER@DB2@cairo-ep"/>
    </TargetSituation>
    <TargetSituation action="" advice=""
affinity="00000000000000000000W00000000000#u000000000" applicationID="KUD"
association="zkud.KUDDBASEGROUP00:620" autoStart="true"
description="DB2_High_ConnectionErrors DB2 ITM5 RM:DB2DatabaseStatus"
displayItem="" displaySeverity="Warning" distribution=""
eventSeverity="WARNING" multipleIntervals="NYN" name="UD5_544_HiConnErrorsAg_0"
persistence="1" predicate="*IF ( *VALUE KUD_DB2_DCS_Database.db_name_U *EQ
'MDIST2' *AND *VALUE KUD_DB2_DCS_Database.db_partition *EQ 'Aggregated' *AND
*VALUE KUD_DB2_DCS_Database.gw_comm_errors_for_int *GT 100 )"
samplingIntervalDays="0" samplingIntervalTime="0:10:0" status="DEPLOYED">
      <SourceApplication name="MDIST2@DB2@cairo-ep"/>
    </TargetSituation>
    <TargetSituation action="" advice=""
affinity="00000000000000000000W00000000000#u000000000" applicationID="KUD"
association="zkud.KUDDBASEGROUP00:620" autoStart="true"
description="DB2_High_ConnectionErrors DB2 ITM5 RM:DB2DatabaseStatus"
displayItem="" displaySeverity="Warning" distribution=""
eventSeverity="WARNING" multipleIntervals="NYN" name="UD5_544_HiConnErrorsAg_1"
persistence="1" predicate="*IF ( *VALUE KUD_DB2_DCS_Database.db_name_U *EQ
'PLANNER' *AND *VALUE KUD_DB2_DCS_Database.db_partition *EQ 'Aggregated' *AND
*VALUE KUD_DB2_DCS_Database.gw_comm_errors_for_int *GT 100 )"
samplingIntervalDays="0" samplingIntervalTime="0:10:0" status="DEPLOYED">
      <SourceApplication name="PLANNER@DB2@cairo-ep"/>
    </TargetSituation>
    <TargetSituation action="" advice=""
affinity="00000000000000000000W00000000000#u000000000" applicationID="KUD"
association="zkud.KUDDBASEGROUP00:620" autoStart="true"
```

```
description="DB2_Old_LastBackupTimestamp DB2 ITM5 RM:DB2DatabaseStatus"
displayItem="KUDDBASEGROUP01.db_name_U" displaySeverity="Critical"
distribution="" multipleIntervals="NYN" name="UD5_544_LastBackupOldAg_0"
persistence="2" predicate="*IF ( *VALUE KUDDBASEGROUP01.db_name_U *EQ 'MDIST2'
*AND *VALUE KUDDBASEGROUP01.db_partition *EQ 'Aggregated' *AND *VALUE
KUDDBASEGROUP01.days_since_last_backup *GT 2 )" samplingIntervalDays="0"
samplingIntervalTime="0:10:0" status="DEPLOYED">
      <SourceApplication name="MDIST2@DB2@cairo-ep"/>
    </TargetSituation>
    <TargetSituation action="" advice=""
affinity="00000000000000000000W00000000000#u000000000" applicationID="KUD"
association="zkud.KUDDBASEGROUP00:620" autoStart="true"
description="DB2_Old_LastBackupTimestamp DB2 ITM5 RM:DB2DatabaseStatus"
displayItem="KUDDBASEGROUP01.db_name_U" displaySeverity="Critical"
distribution="" multipleIntervals="NYN" name="UD5_544_LastBackupOldAg_1"
persistence="2" predicate="*IF ( *VALUE KUDDBASEGROUP01.db_name_U *EQ 'PLANNER'
*AND *VALUE KUDDBASEGROUP01.db_partition *EQ 'Aggregated' *AND *VALUE
KUDDBASEGROUP01.days_since_last_backup *GT 2 )" samplingIntervalDays="0"
samplingIntervalTime="0:10:0" status="DEPLOYED">
      <SourceApplication name="PLANNER@DB2@cairo-ep"/>
    </TargetSituation>
    <TargetSituation action="" advice=""
affinity="00000000000000000000W00000000000#u000000000" applicationID="KUD"
association="zkud.KUDDBASEGROUP00:620" autoStart="true"
description="DB2_High_PctConnectionsUsed DB2 ITM5 RM:DB2DatabaseStatus"
displayItem="KUDDBASEGROUP01.db_name_U" displaySeverity="Warning"
distribution="" eventSeverity="WARNING" multipleIntervals="NYN"
name="UD5_544_HiPctConnUsedAg_0" persistence="3" predicate="*IF ( *VALUE
KUDDBASEGROUP01.db_name_U *EQ 'MDIST2' *AND *VALUE KUDDBASEGROUP01.db_partition
*EQ 'Aggregated' *AND *VALUE KUDDBASEGROUP01.cur_cons_pct *GT 80 )"
samplingIntervalDays="0" samplingIntervalTime="0:10:0" status="DEPLOYED">
      <SourceApplication name="MDIST2@DB2@cairo-ep"/>
    </TargetSituation>
    <TargetSituation action="" advice=""
affinity="00000000000000000000W00000000000#u000000000" applicationID="KUD"
association="zkud.KUDDBASEGROUP00:620" autoStart="true"
description="DB2_High_PctConnectionsUsed DB2 ITM5 RM:DB2DatabaseStatus"
displayItem="KUDDBASEGROUP01.db_name_U" displaySeverity="Warning"
distribution="" eventSeverity="WARNING" multipleIntervals="NYN"
name="UD5_544_HiPctConnUsedAg_1" persistence="3" predicate="*IF ( *VALUE
KUDDBASEGROUP01.db_name_U *EQ 'PLANNER' *AND *VALUE
KUDDBASEGROUP01.db_partition *EQ 'Aggregated' *AND *VALUE
KUDDBASEGROUP01.cur_cons_pct *GT 80 )" samplingIntervalDays="0"
samplingIntervalTime="0:10:0" status="DEPLOYED">
      <SourceApplication name="PLANNER@DB2@cairo-ep"/>
    </TargetSituation>
    <TargetSituation action="" advice=""
affinity="00000000000000000000W00000000000#u000000000" applicationID="KUD"
association="zkud.TableSpace:620" autoStart="true"
```

```
description="DB2_False_TablespaceNormalStatus DB2 ITM5 RM:DB2DatabaseStatus"
displayItem="KUDTABSPACE.TABLESPACE_NAME_U" displaySeverity="Warning"
distribution="" eventSeverity="WARNING" multipleIntervals="NYN"
name="UD5_544_TsStatNotNormalAg_0" persistence="2" predicate="*IF ( *VALUE
KUDTABSPACE.DB_NAME_U *EQ 'MDIST2' *AND *VALUE KUDTABSPACE.db_partition *EQ
'Aggregated' *AND *VALUE KUDTABSPACE.TABLESPACE_NAME_U *IN ('*') *AND *VALUE
KUDTABSPACE.TBSP_STATUS *NE '0' )" samplingIntervalDays="0"
samplingIntervalTime="0:10:0" status="DEPLOYED">
      <SourceApplication name="MDIST2@DB2@cairo-ep"/>
    </TargetSituation>
    <TargetSituation action="" advice=""
affinity="00000000000000000000W00000000000#u000000000" applicationID="KUD"
association="zkud.TableSpace:620" autoStart="true"
description="DB2_False_TablespaceNormalStatus DB2 ITM5 RM:DB2DatabaseStatus"
displayItem="KUDTABSPACE.TABLESPACE_NAME_U" displaySeverity="Warning"
distribution="" eventSeverity="WARNING" multipleIntervals="NYN"
name="UD5_544_TsStatNotNormalAg_1" persistence="2" predicate="*IF ( *VALUE
KUDTABSPACE.DB_NAME_U *EQ 'PLANNER' *AND *VALUE KUDTABSPACE.db_partition *EQ
'Aggregated' *AND *VALUE KUDTABSPACE.TABLESPACE_NAME_U *IN ('*') *AND *VALUE
KUDTABSPACE.TBSP_STATUS *NE '0' )" samplingIntervalDays="0"
samplingIntervalTime="0:10:0" status="DEPLOYED">
      <SourceApplication name="PLANNER@DB2@cairo-ep"/>
    </TargetSituation>
  </ResourceModelAssess>
  <TECEventServers status="DEPLOYED">
    <TECEventServer name="9.3.5.205" port="0"/>
  </TECEventServers>
</ProfileAssess>

The status of each situation is changed to “DEPLOYED”.
```

Step 12: Migrate profiles – status check

After the migration has completed, there are no obligatory tasks to be performed. However, you might want to verify the results of the migration for one or more profiles, or examine in detail one or more situations.

The situations are not indicated in the infrastructure file, so you will not need to recalculate the overall status. If you want to verify the migration operation, open the output file from the **witmmtk migrate** command and verify that the situation was created. The aggregateStatus tag for the profile should specify "100" to indicate that the migration of the profile is 100% complete.

You can also check on the hub Tivoli Enterprise Monitoring Server if the situations have been successfully created.

Example 4-22 on page 251 guides you on how to perform this check on the hub monitoring server.

Example 4-22 Checking situations on the hub Tivoli Enterprise Monitoring Server

```
You can either use the Tivoli Enterprise Portal to check the situations
in the Situation Editor, or the tacmd listSit CLI. Before using this
command you must login into the hub monitoring server using this
command:

[root@edinburgh /]# tacmd login -s localhost -u root -t 1440

 Password?
Validating user...

KUIC00007I: User root logged into server on https://localhost:41120.

Suppose that you want now to list all the mapped Windows OS situations
that has NT5 as prefix. You can get this list running the following
command:

[root@edinburgh 1]# tacmd listSit|grep NT5
NT5_55d_BusyHardware_0          Windows OS
NT5_55d_CpuCantKeepUp_0         Windows OS
NT5_55d_LowCopyReadHits_0       Windows OS
NT5_55d_LowAvailSmPageFile_0    Windows OS
NT5_55d_HighLogDiskWritByt_0    Windows OS
NT5_55d_HwKeepingCpuBusy_0      Windows OS
NT5_55d_LogDiskPossFrag_0       Windows OS
NT5_55d_LowAvailHardPaging_0    Windows OS
NT5_55d_LowAvailHighCache_0     Windows OS
NT5_55d_LowAvailHighWrkSet_0    Windows OS
NT5_55d_LowAvailManyProbs_0     Windows OS
NT5_55d_HighLogDiskPctTime_0    Windows OS
NT5_55d_HighLogDiskReadByt_0    Windows OS
NT5_55d_SlowLogDiskDrive_0      Windows OS
NT5_55d_LowAvailSoftPaging_0    Windows OS
NT5_55d_HighLogDiskXferRat_0    Windows OS
NT5_55d_LowDataMapHits_0        Windows OS
NT5_55d_LowLogDiskSpace_0       Windows OS
NT5_55d_LowMDLReadHits_0        Windows OS
NT5_55d_LowPinReadHits_0        Windows OS
NT5_55d_MemoryLeakPrivate_0     Windows OS
NT5_55d_MemoryLeakSysCode_0     Windows OS
NT5_55d_ProcessorBusy_0         Windows OS
NT5_55d_PageFileResizing_0      Windows OS
NT5_55d_LowAvailMemory_0        Windows OS
NT5_55d_LowAvailPageResize_0    Windows OS
```

```
NT5_55d_HighPctUsageDelta_0     Windows OS
NT5_55d_HighProcesses_0         Windows OS
NT5_55d_MemoryLeakSysDrive_0    Windows OS
NT5_55d_HighPaging_0            Windows OS

To view one of these situations, use the below command:

[root@edinburgh 1]# tacmd viewsit -s NT5_55d_HighLogDiskPctTime_0
Name                      : NT5_55d_HighLogDiskPctTime_0
Description               : TMW_HighLogicalPercentDiskTime WINDOWS ITM5
RM:TMW_L
ogicalDisk
Type                      : Windows OS
Formula                   : *IF ( *VALUE NT_Logical_Disk.Disk_Name *NE '_Total'
*AND *VALUE NT_Logical_Disk.Disk_Queue_Length *GT 3 *AND *VALUE
NT_Logical_Disk.
%_Disk_Time *GT 90 *AND *VALUE NT_Logical_Disk.Disk_Bytes/Sec *LE 1572864 )
Sampling Interval         : 0/0:2:0
Run At Start Up           : Yes
Distribution              :
Text                      :
Action Location           : Agent
Action Selection          :
Universal Message Category:
Universal Message Severity:
Universal Message         :
True For Multiple Items   : Action on First item only
TEC Severity              : Warning
TEC Forwarding            : Y
TEC Destination           : 1

If you are familiar with the situations, you will notice that the
Distribution is empty. This is because the profile managers are not yet
migrated to managed systems list.
With the next and last step the managed system lists will be created
and each situation updated with the corresponding Distribution list.
```

Mapping TEC server to Event Destinations

In this step, if the profile that you are migrating contains a TEC server, identified by a stanza similar to the following:

```
<TECEventServers status="DEPLOYED">
    <TECEventServer name="9.3.5.205" port="0"/>
</TECEventServers>
```

the IP address is mapped to an event destination for IBM Tivoli Monitoring V6.2.

This behavior changes based on the Tmw2kProfile configuration:

- Broadcast

  In this case, you have an entry like server1,server2 in your profile. The migration of the profile creates an event destination for each server in the broadcast list.

- Failover

  In this case, you have a single entry in your profile. The migration of the profile creates a single event destination.

The event destination is called “EIF Server List ID”, where ID is the internal ID of the event destination, as created in the IBM Tivoli Monitoring V6.2 infrastructure.

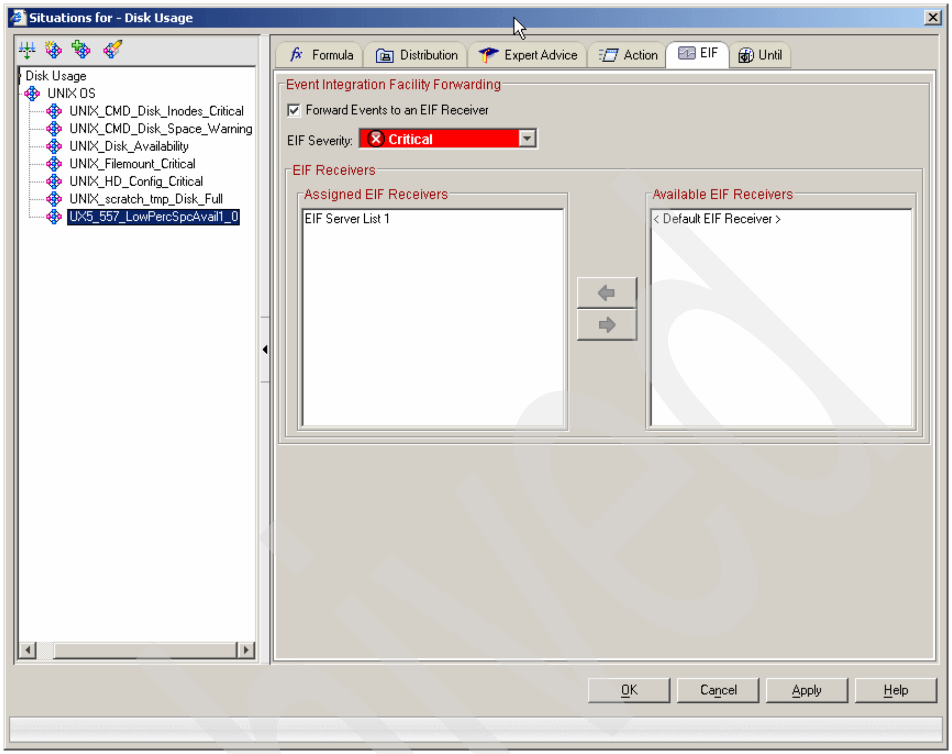
Example 4-23 shows the result of the mapping for the AIX.xml profile that we migrated for this example.

Example 4-23 TEC server to event destination mapping

```
Our AIX.xml profile assess file contains the following TECEventServers
stanza:

<TECEventServers status="DEPLOYED">
    <TECEventServer name="9.3.5.205" port="0"/>
  </TECEventServers>
</ProfileAssess>

The migration of the profile creates an event destination for the
TECEventServer name 9.3.5.205.

To list the event destination on the HUB TEMS, login to the TEMS first
with this command:

[root@edinburgh ~]# tacmd login -s localhost -u root -t 1440

 Password?
Validating user...
```

```
KUIC00007I: User root logged into server on https://localhost:41120.

Then use the listeventdest option of the tacmd command as shown below:

[root@edinburgh ~]# tacmd listeventdest
Server Id Server Name          Server Type
0         Default EIF Receiver TEC
1         EIF Server List 1    TEC

The ID 0 represents the Default EIF Receiver, the one that is specified
at HUB TEMS configuration time.

The below command lists the detail of the event destination created:

[root@edinburgh ~]# tacmd vieweventdest -i 1
Server Id  : 1
Server Name: EIF Server List 1
Server Type: TEC
Description:
Default    :
Host1      : 9.3.5.205:0
Host2      : Not set
Host3      : Not set
Host4      : Not set
Host5      : Not set
Host6      : Not set
Host7      : Not set
Host8      : Not set

The mapped event destinations are only created of "T" type.
```

Figure 4-15 on page 255 shows a migrated situation and its association to the migrated event destination. As you can see, the default EIF Receiver is listed under “Available EIF Receivers”, while the migrated one is listed under “Assigned EIF Receivers”.



Disk Usage
- UNIX OS
  - UNIX_CMD_Disk_Inodes_Critical
  - UNIX_CMD_Disk_Space_Warning
  - UNIX_Disk_Availability
  - UNIX_Filemount_Critical
  - UNIX_HD_Config_Critical
  - UNIX_scratch_tmp_Disk_Full
  - UX5_557_LowPercSpcAvail1_0

Event Integration Facility Forwarding

☑ Forward Events to an EIF Receiver

EIF Severity: Critical

EIF Receivers

Assigned EIF Receivers: EIF Server List 1

Available EIF Receivers: < Default EIF Receiver >

Figure 4-15 Migrated TEC server

4.4.5 Phase D: Migrating the profile managers

As with the other phases in the migration process, this one is made of four steps: assess, analyze, migrate, and status check.

In this case, the resources to be migrated are profile managers.

Step 13: Migrate profile managers – assess

This step results in the creation of an XML file for each profile manager that determines which endpoints (managed systems) will be included in which managed system list.

The full mapping logic is:

- The subscribers to the profile manager become managed system lists. There is one managed system list for each profile and agent type.
- The distribution relationship between profiles and subscribers is applied to situations and managed systems.

- It assesses all profiles contained in the profile manager (unless the –p filter is specified or the profile has already been assessed).
- It assesses all endpoint contained in the profile manager (unless the –e filter is specified or the endpoint has already been assessed).
- If there are subscribed profile managers, they and their profiles and endpoints are similarly assessed.
- The -o flatten option can be used to avoid running the assess recursively in environments with nested profile managers.

Example 4-24 shows the execution of the steps in our environment.

Example 4-24 Migrate profile managers - assess step

```
We started from the profiles managers list in our environment:

C:\Tivoli\db\cairo.db\AMK\analyze\profiles>wlookup -ar ProfileManager
|grep ITM
ITM_AIX_PM      1713357986.1.1359#TMF_CCMS::ProfileManager#
ITM_CUSTOM_PM   1713357986.1.1374#TMF_CCMS::ProfileManager#
ITM_HPUX_PM     1713357986.1.1379#TMF_CCMS::ProfileManager#
ITM_LINUX_PM    1713357986.1.1368#TMF_CCMS::ProfileManager#
ITM_WINDOWS_PM  1713357986.1.1371#TMF_CCMS::ProfileManager#

Whit the below command we assessed the profile manager called
ITM_AIX_PM:

C:\Tivoli\db\cairo.db\AMK\analyze\profilemanagers>witmmtk assess -pm
ITM_AIX_PM

AMKUT0016I Processing the request.
.
AMKUT5003I Loading the resource snapshot for the assessment.
AMKUT0057I Loading the infrastructure baseline file:
"C:\Tivoli\db\cairo.db\AMK\analyze\scans\1713357986.xml".
AMKUT5006I Starting the resource assessment.
AMKUT5080I Converting profile manager ITM_AIX_PM.
AMKUT5007I All resources are assessed. Processing is complete.
.
AMKUT0008I The command completed successfully. See log
"C:\Tivoli\db\cairo.db\AMK\logs\log_wmtkassess_20071010_16_24_46.log"fo
r more information.
```

The generated XML file for the above profile manager is listed in Example 4-25 on page 257.

Example 4-25 XML file for the profile manager ITM_AIX_PM

```
<?xml version="1.0" encoding="UTF-8"?>
<!--Copyright IBM Corporation 2006-->
<?xml-stylesheet type="text/xsl"
href="../../data/stylesheet/ProfileManagerAssess.xsl"?>
<ProfileManagerAssess aggregateStatus="0" comment="" name="ITM_AIX_PM"
xmlns="http://www.ibm.com/tivoli/itm/assess/profilemanager"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="http://www.ibm.com/tivoli/itm/assess/profilemanager
ProfileManagerAssess.xsd">
  <ManagedSystemList
affinity="00f20000000000000000000000000000#m000000000" comment=""
name="557_KUX" product="KUX" profile="AIX" status="NOT_DEPLOYED">
    <ManagedSystem hostname="server2.itsc.austin.ibm.com"
name="server2.itsc.austin.ibm.com:KUX" source="server2-ep"/>
    <ManagedSystem hostname="paris.itsc.austin.ibm.com"
name="paris.itsc.austin.ibm.com:KUX" source="paris-ep"/>
  </ManagedSystemList>
</ProfileManagerAssess>
```

Step 14: Migrate profile managers – analyze

After creating the assess files, you should check that the number of files created corresponds with your expectations, given the input to the command.

Each profile manager assess file contains elements that describe the managed system lists that will be created. You may decide you want to check this information.

For further details, refer to Chapter 18, “Assess data file XML reference” in *Upgrading from IBM Tivoli Monitoring V5.1.2*, GC32-1976, which describes the assess file, and gives details on how you can view it. It also explains the naming convention for managed system lists.

Step 15: Migrate profile managers – migrate

The migrate tool is used to:

- Create the V6 managed system lists.
- Create the distribution relationship between situations and managed systems.
- Distribute situations to the appropriate managed systems and activate them.
- Associate navigation items using the association class for the Tivoli Enterprise Portal.
- Update the profile manager assess file status.

Attention: You must not migrate a profile manager until the profiles and endpoints it references have been migrated.

The following is an example of how to migrate a profile manager called myPM1:

1. Log on to the Tivoli server and source the Tivoli environment.
2. Run the Migrate tool with the –x option to create just the managed system lists for the profile manager myPM1, but to not migrate any other assess files:

   ```
   witmmtk migrate –x $DBDIR/AMK/analyze/profilemanagers/myPM1.xml –u
   ```

   where:

   – –x $DBDIR/AMK/analyze/profilemanagers/myPM1.xml specifies the profile manager to migrate.

   – –u specifies that you are using the **witmmtk migrate** command to perform a migration. See 4.5.3, “Migrate” on page 277 for a full description of the command and its options. The assess file is updated to show the deployed status.

Example 4-26 shows the steps to migrate the profile managers of our environment.

Example 4-26 Profile managers migration

```
The -d option migrates all the profile managers contained in the
specified directory. If you want to migrate only one profile manager,
use the -x option followed by the XML file name for the profile manager
you want to migrate.

The below example migrates all the profiles managers contained in the
“%DBDIR%\AMK\analyze\profilemanagers” directory:

C:\Tivoli\db\cairo.db\AMK\analyze\profilemanagers>witmmtk migrate -d
"%DBDIR%\AMK\analyze\profilemanagers" -u
.
AMKUT0016I Processing the request.

AMKUT0057I Loading the infrastructure baseline file:
"C:\Tivoli\db\cairo.db\AMK\analyze\scans\1713357986.xml".
AMKUT7002E The file
"C:\Tivoli\db\cairo.db\AMK\analyze\profilemanagers\pm.txt" is not a
valid file.
AMKUT7077I Processing profile manager: "ITM_AIX_PM".
AMKUT7080I Creating managed system list "557_KUX" for hub monitoring
server "HUB_TEMS".
```

```
AMKUT7617I The managed system list "557_KUX" was added.
AMKUT7621I Associating situations for resource model "DMXCpu" to
managed systems in the managed system list "557_KUX".
AMKUT7621I Associating situations for resource model "DMXFileSystem" to
managed systems in the managed system list "557_KUX".
AMKUT7621I Associating situations for resource model "DMXMemory" to
managed systems in the managed system list "557_KUX".
AMKUT7621I Associating situations for resource model "DMXPhysicalDisk"
to managed systems in the managed system list "557_KUX".
AMKUT7622I All the situations were successfully associated to the
managed systems in the managed system list "557_KUX".
AMKUT7077I Processing profile manager: "ITM_HPUX_PM".
AMKUT7080I Creating managed system list "564_KUX" for hub monitoring
server "HUB_TEMS".
AMKUT7010W The agent "rx2620:KUX" has already been deployed, but with a
different name "rx2620.itsc.austin.ibm.com:KUX" than that us
ed in the endpoint assess file. The assess file and infrastructure
baseline (if appropriate) have been updated with the new name.
AMKUT7617I The managed system list "564_KUX" was added.
AMKUT7621I Associating situations for resource model "DMXCpu" to
managed systems in the managed system list "564_KUX".
AMKUT7621I Associating situations for resource model "DMXFileSystem" to
managed systems in the managed system list "564_KUX".
AMKUT7621I Associating situations for resource model "DMXMemory" to
managed systems in the managed system list "564_KUX".
AMKUT7621I Associating situations for resource model "DMXPhysicalDisk"
to managed systems in the managed system list "564_KUX".
AMKUT7622I All the situations were successfully associated to the
managed systems in the managed system list "564_KUX".
AMKUT7077I Processing profile manager: "ITM_LINUX_PM".
AMKUT7080I Creating managed system list "55a_KLZ" for hub monitoring
server "HUB_TEMS".
AMKUT7010W The agent "edinburgh:LZ" has already been deployed, but with
a different name "edinburgh.itsc.austin.ibm.com:LZ" than tha
t used in the endpoint assess file. The assess file and infrastructure
baseline (if appropriate) have been updated with the new name
.
AMKUT7617I The managed system list "55a_KLZ" was added.
AMKUT7621I Associating situations for resource model "DMXCpu" to
managed systems in the managed system list "55a_KLZ".
AMKUT7627W The target situation "LZ5_55a_HIGH_WAITCPUUSE_0" could not
be associated with the navigator items of objects in the manag
ed system list "55a_KLZ".
AMKUT7627W The target situation "LZ5_55a_LOW_IDLECPUUSE_0" could not be
associated with the navigator items of objects in the manage
```

```
d system list "55a_KLZ".
AMKUT7627W The target situation "LZ5_55a_HIGH_SYSCPUUSE_O" could not be
associated with the navigator items of objects in the manage
d system list "55a_KLZ".
AMKUT7621I Associating situations for resource model "DMXFileSystem" to
managed systems in the managed system list "55a_KLZ".
AMKUT7621I Associating situations for resource model "DMXMemory" to
managed systems in the managed system list "55a_KLZ".
AMKUT7627W The target situation "LZ5_55a_LOWSTORAGE_O" could not be
associated with the navigator items of objects in the managed sy
stem list "55a_KLZ".
AMKUT7627W The target situation "LZ5_55a_THRASHING_O" could not be
associated with the navigator items of objects in the managed sys
tem list "55a_KLZ".
AMKUT7627W The target situation "LZ5_55a_LOWSWAP_O" could not be
associated with the navigator items of objects in the managed syste
m list "55a_KLZ".
AMKUT7621I Associating situations for resource model "DMXPhysicalDisk"
to managed systems in the managed system list "55a_KLZ".
AMKUT7077I Processing profile manager: "ITM_WINDOWS_PM".
AMKUT7080I Creating managed system list "55d_KNT" for hub monitoring
server "HUB_TEMS".
AMKUT7617I The managed system list "55d_KNT" was added.
AMKUT7621I Associating situations for resource model "TMW_Processor" to
managed systems in the managed system list "55d_KNT".
AMKUT7621I Associating situations for resource model "TMW_LogicalDisk"
to managed systems in the managed system list "55d_KNT".
AMKUT7621I Associating situations for resource model "TMW_MemoryModel"
to managed systems in the managed system list "55d_KNT".
AMKUT7622I All the situations were successfully associated to the
managed systems in the managed system list "55d_KNT".
.

AMKUT0010W The command completed with warnings. See log
"C:\Tivoli\db\cairo.db\AMK\logs\log_wmtkmigrate_20071010_16_32_50.log"
for more information.

The warning message is simply caused by the presence of the
“C:\Tivoli\db\cairo.db\AMK\analyze\profilemanagers\pm.txt” file in the
profiles directory: this is not a valid XML file so tool identify it is
not valid.
```

The status of the XML file for the profiles is updated, as shown in Example 4-27 on page 261.

Example 4-27 Updated XML file for the migrated profile managers

```
The below file is for the migrated profile manager called ITM_AIX_PM:

<?xml version="1.0" encoding="UTF-8"?>
<!--Copyright IBM Corporation 2006-->
<?xml-stylesheet type="text/xsl"
href="../../data/stylesheet/ProfileManagerAssess.xsl"?>
<ProfileManagerAssess aggregateStatus="100" comment=""
name="ITM_AIX_PM"
xmlns="http://www.ibm.com/tivoli/itm/assess/profilemanager"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="http://www.ibm.com/tivoli/itm/assess/profilemanager
ProfileManagerAssess.xsd">
  <ManagedSystemList
affinity="00f20000000000000000000000000000#m000000000" comment=""
name="557_KUX" product="KUX" profile="AIX" status="DEPLOYED">
    <ManagedSystem hostname="server2.itsc.austin.ibm.com"
name="server2.itsc.austin.ibm.com:KUX" source="server2-ep"/>
    <ManagedSystem hostname="paris.itsc.austin.ibm.com"
name="paris.itsc.austin.ibm.com:KUX" source="paris-ep"/>
  </ManagedSystemList>
</ProfileManagerAssess>
```

Step 16: Migrate profile managers – status check

After the migration has completed, there are no obligatory tasks to be performed. However, you might want to verify the results of the migration for one or more profile managers, or examine in detail one or more managed system lists.

The managed system lists are not indicated in the infrastructure file, so you will not need to recalculate the overall status.

If you want to verify the migration operation, open the output file from the **`witmmtk migrate`** command and verify that the situation was created. The aggregateStatus tag for the profile manager should specify "100" to indicate that the migration of the profile manager is 100% complete.

You can also check on the hub Tivoli Enterprise Monitoring Server if the situations have been successfully updated and the managed system lists have been created.

Example 4-28 on page 262 shows you how to perform these checks on the hub monitoring server.

Example 4-28 Checking managed system lists on the hub Tivoli Enterprise Monitoring Server

```
You can either use the Tivoli Enterprise Portal to check that the
situations are associated to the right managed system list, or the
tacmd listsystemlist CLI. Before using this command you must login into
the hub monitoring server using this command:

[root@edinburgh /]# tacmd login -s localhost -u root -t 1440

 Password?
Validating user...

KUIC00007I: User root logged into server on https://localhost:41120.

To list the newly created managed system lists use this command:

[root@edinburgh 1]# tacmd listsystemlist |grep 5
557_KUX                  UNIX OS
55a_KLZ                  Linux OS
55d_KNT                  Windows OS
564_KUX                  UNIX OS

The below command provides details on a specific managed system list,
showing the belonging agents:

[root@edinburgh ~]# tacmd viewsystemlist -l 557_KUX
Name                  : 557_KUX
Type                  : UNIX OS
Assigned Managed List : paris.itsc.austin.ibm.com:KUX
Available Managed List:
rp3410.itsc.austin.ibm.com:KUX,rx2620.itsc.austin.ibm.com:KUX,server2.i
tsc.austin.ibm.com:KUX

To check that the situations has been updated to include to correct
managed system list in its distribution you can run this command:

[root@edinburgh 1]# tacmd viewsit -s UX5_557_HIGH_SYSCPUUSE_0
Name                      : UX5_557_HIGH_SYSCPUUSE_0
Description               : High_SysCPUUsage AIX ITM5 RM:DMXCpu
Type                      : UNIX OS
Formula                   : *IF ( *VALUE System.System_CPU *GT 80 )
Sampling Interval         : 0/0:1:0
Run At Start Up           : Yes
Distribution              : 557_KUX
```

```
Text                      :
Action Location           : Agent
Action Selection          : System Command
Universal Message Category:
Universal Message Severity:
Universal Message         :
True For Multiple Items   : Action on First item only
TEC Severity              : Warning
TEC Forwarding            : Y
TEC Destination           : 1
```

4.4.6 Viewing the results and cleaning up

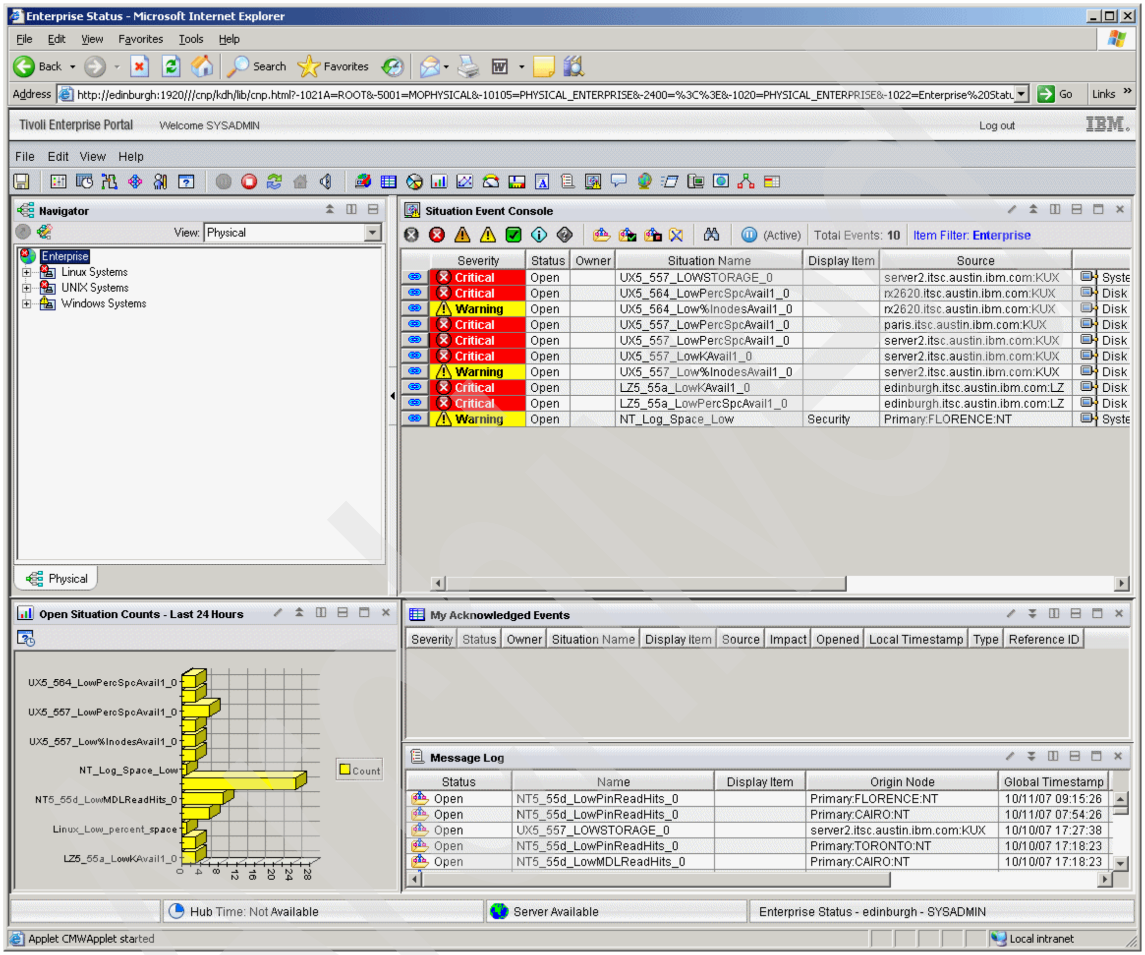
This is the last step of the migration process.

Step 17: Viewing results in the Tivoli Enterprise Portal

If the migration is successful, the new situations, managed systems, and managed system lists are displayed in the Tivoli Enterprise Portal.

The following figures show sample checks that you can perform to check that the migration is successful.

Figure 4-16 shows the Tivoli Enterprise Portal after the migration. As you can see, the Situation Event Console already contains some situation events coming from the new situations that has been migrated and distributed to the endpoints migrated to OS agents.


Enterprise Status - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://edinburgh:1920///cnp/kdh/lib/cnp.html?-1021A=ROOT&-5001=MOPHYSICAL&-10105=PHYSICAL_ENTERPRISE&-2400=%3C%3E&-1020=PHYSICAL_ENTERPRISE&-1022=Enterprise%20Statu
Go Links
Tivoli Enterprise Portal Welcome SYSADMIN Log out IBM.
File Edit View Help
Navigator
View: Physical
Enterprise
Linux Systems
UNIX Systems
Windows Systems
Physical
Situation Event Console
(Active) Total Events: 10 Item Filter: Enterprise

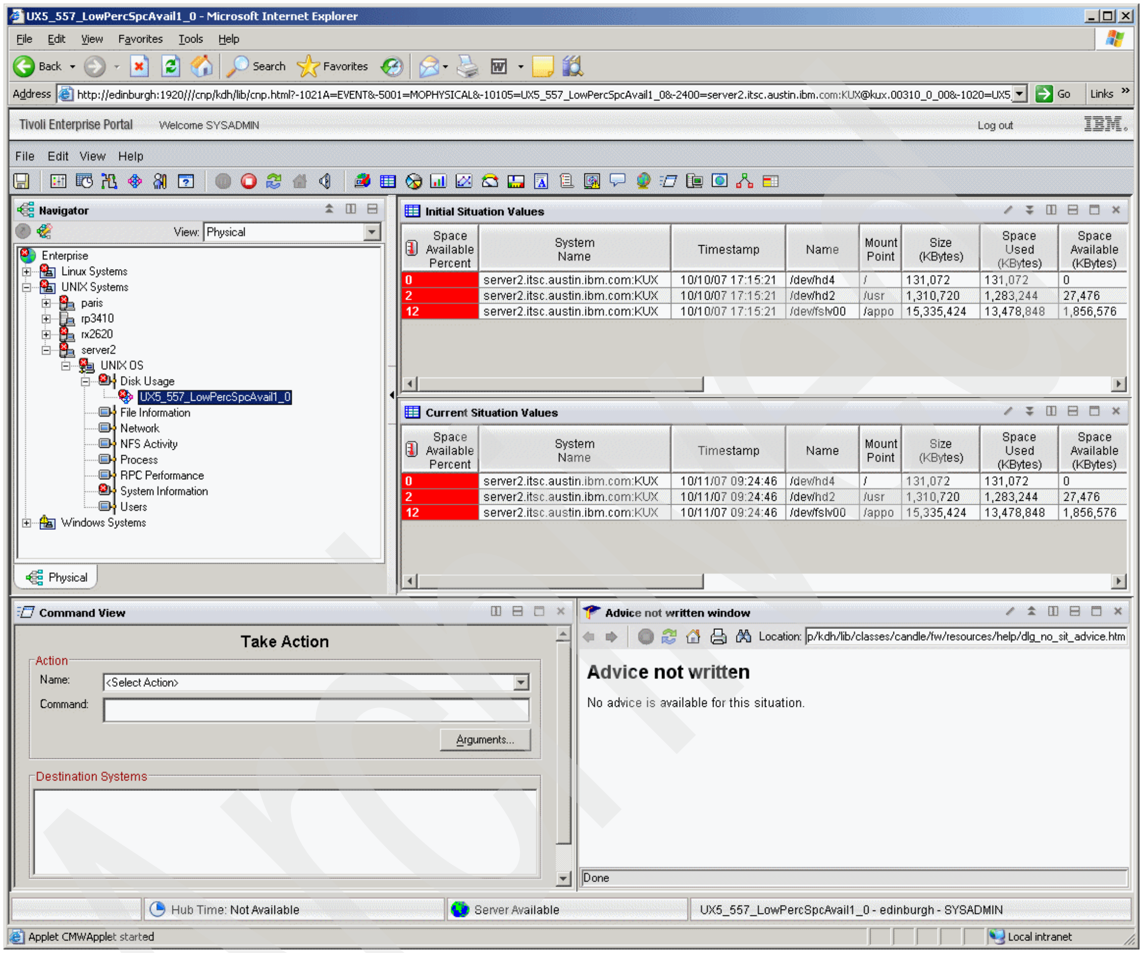
	Severity	Status	Owner	Situation Name	Display Item	Source	
	Critical	Open		UX5_557_LOWSTORAGE_0		server2.itsc.austin.ibm.com:KUX	Syste
	Critical	Open		UX5_564_LowPercSpcAvail1_0		rx2620.itsc.austin.ibm.com:KUX	Disk
	Warning	Open		UX5_564_Low%InodesAvail1_0		rx2620.itsc.austin.ibm.com:KUX	Disk
	Critical	Open		UX5_557_LowPercSpcAvail1_0		paris.itsc.austin.ibm.com:KUX	Disk
	Critical	Open		UX5_557_LowPercSpcAvail1_0		server2.itsc.austin.ibm.com:KUX	Disk
	Critical	Open		UX5_557_LowKAvail1_0		server2.itsc.austin.ibm.com:KUX	Disk
	Warning	Open		UX5_557_Low%InodesAvail1_0		server2.itsc.austin.ibm.com:KUX	Disk
	Critical	Open		LZ5_55a_LowKAvail1_0		edinburgh.itsc.austin.ibm.com:LZ	Disk
	Critical	Open		LZ5_55a_LowPercSpcAvail1_0		edinburgh.itsc.austin.ibm.com:LZ	Disk
	Warning	Open		NT_Log_Space_Low	Security	Primary:FLORENCE:NT	Syste

Severity	Status	Owner	Situation Name	Display Item	Source	Impact	Opened	Local Timestamp	Type	Reference ID

Status	Name	Display Item	Origin Node	Global Timestamp
Open	NT5_55d_LowPinReadHits_0		Primary:FLORENCE:NT	10/11/07 09:15:26
Open	NT5_55d_LowPinReadHits_0		Primary:CAIRO:NT	10/11/07 07:54:26
Open	UX5_557_LOWSTORAGE_0		server2.itsc.austin.ibm.com:KUX	10/10/07 17:27:38
Open	NT5_55d_LowPinReadHits_0		Primary:TORONTO:NT	10/10/07 17:18:23
Open	NT5_55d_LowMDLReadHits_0		Primary:CAIRO:NT	10/10/07 17:18:23

Figure 4-16 Tivoli Enterprise Portal view after the migration

Figure 4-17 shows the details of one situation evaluated to true. In this case, the situation is called UX5_557_LowPercSpcAvail1_0. It is set to run if the Space Available Percent is less than 15%.



Address: http://edinburgh:1920///cnp/kdh/lib/cnp.html?-1021A=EVENT&-5001=MOPHYSICAL&-10105=UX5_557_LowPercSpcAvail1_0&-2400=server2.itsc.austin.ibm.com:KUX@kux.00310_0_00&-1020=UX5

Initial Situation Values

Space Available Percent	System Name	Timestamp	Name	Mount Point	Size (KBytes)	Space Used (KBytes)	Space Available (KBytes)
0	server2.itsc.austin.ibm.com:KUX	10/10/07 17:15:21	/dev/hd4	/	131,072	131,072	0
2	server2.itsc.austin.ibm.com:KUX	10/10/07 17:15:21	/dev/hd2	/usr	1,310,720	1,283,244	27,476
12	server2.itsc.austin.ibm.com:KUX	10/10/07 17:15:21	/dev/fslv00	/appo	15,335,424	13,478,848	1,856,576

Current Situation Values

Space Available Percent	System Name	Timestamp	Name	Mount Point	Size (KBytes)	Space Used (KBytes)	Space Available (KBytes)
0	server2.itsc.austin.ibm.com:KUX	10/11/07 09:24:46	/dev/hd4	/	131,072	131,072	0
2	server2.itsc.austin.ibm.com:KUX	10/11/07 09:24:46	/dev/hd2	/usr	1,310,720	1,283,244	27,476
12	server2.itsc.austin.ibm.com:KUX	10/11/07 09:24:46	/dev/fslv00	/appo	15,335,424	13,478,848	1,856,576

Name: <Select Action>

Command:

Location: p/kdh/lib/classes/candle/fw/resources/help/dlg_no_sit_advice.htm

Advice not written

No advice is available for this situation.

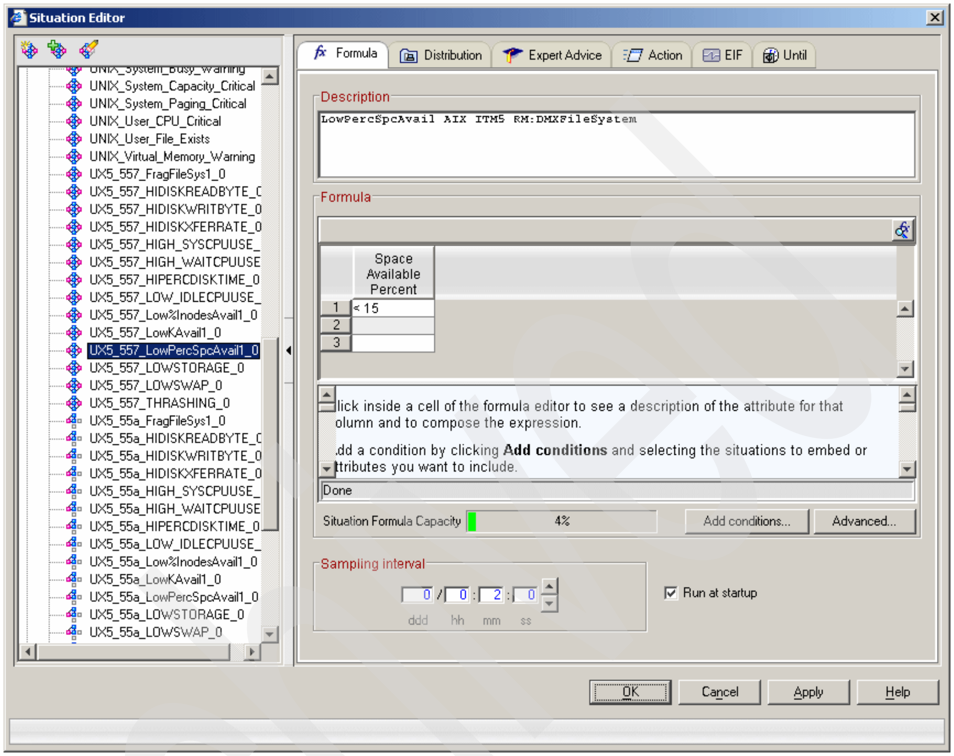
Done

UX5_557_LowPercSpcAvail1_0 - edinburgh - SYSADMIN

Applet CMWApplet started

Figure 4-17 UX5_557_LowPercSpcAvail1_0 details in Tivoli Enterprise Portal

Figure 4-18 shows the formula, the description, the sampling interval, and the run at startup setting for the situation.



Description: LowPercSpcAvail AIX ITM5 RM:DMXFileSystem

Formula:

	Space Available Percent
1	< 15
2	
3	

lick inside a cell of the formula editor to see a description of the attribute for that olumn and to compose the expression.

.dd a condition by clicking **Add conditions** and selecting the situations to embed or ttributes you want to include.

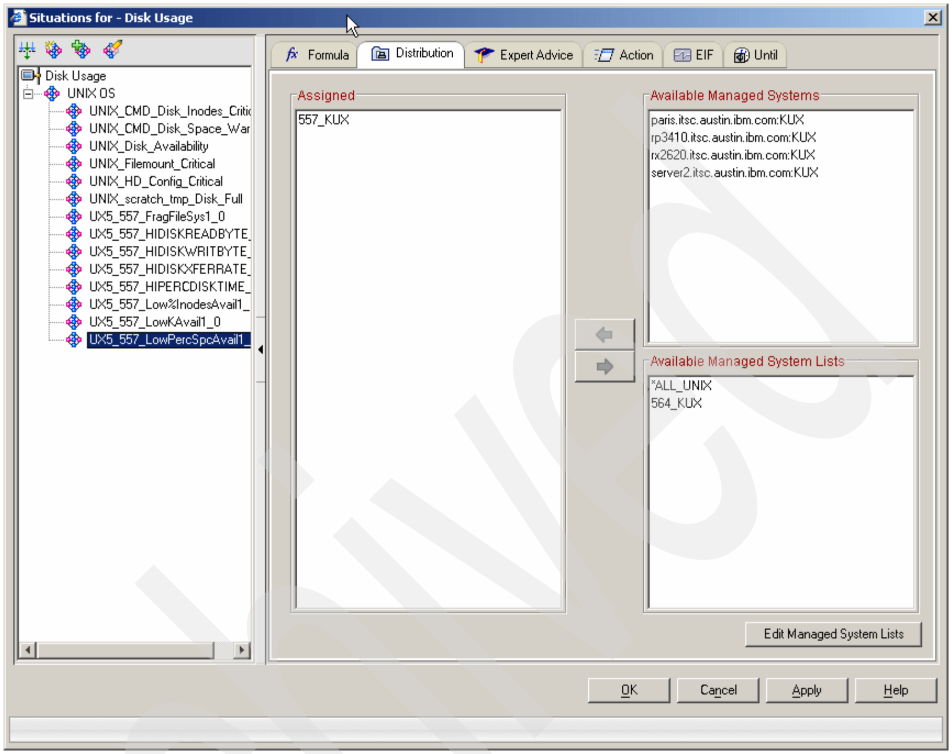
Done

Sampling interval: 0 / 0 : 2 : 0 (ddd hh mm ss)

☑ Run at startup

Figure 4-18 UX5_557_LowPercSpcAvail1_0 situation formula

Figure 4-19 shows the Distribution tab for the situation, where you can see the new managed system list correctly assigned to the situation.


Situations for - Disk Usage
Formula
Distribution
Expert Advice
Action
EIF
Until
Assigned
Available Managed Systems
Available Managed System Lists
Edit Managed System Lists
OK
Cancel
Apply
Help

Disk Usage
UNIX OS
UNIX_CMD_Disk_Inodes_Critic
UNIX_CMD_Disk_Space_War
UNIX_Disk_Availability
UNIX_Filemount_Critical
UNIX_HD_Config_Critical
UNIX_scratch_tmp_Disk_Full
UX5_557_FragFileSys1_0
UX5_557_HIDISKREADBYTE_
UX5_557_HIDISKWRITBYTE_
UX5_557_HIDISKXFERRATE_
UX5_557_HIPERCDISKTIME_
UX5_557_Low%InodesAvail1_
UX5_557_LowKAvail1_0
UX5_557_LowPercSpcAvail1_

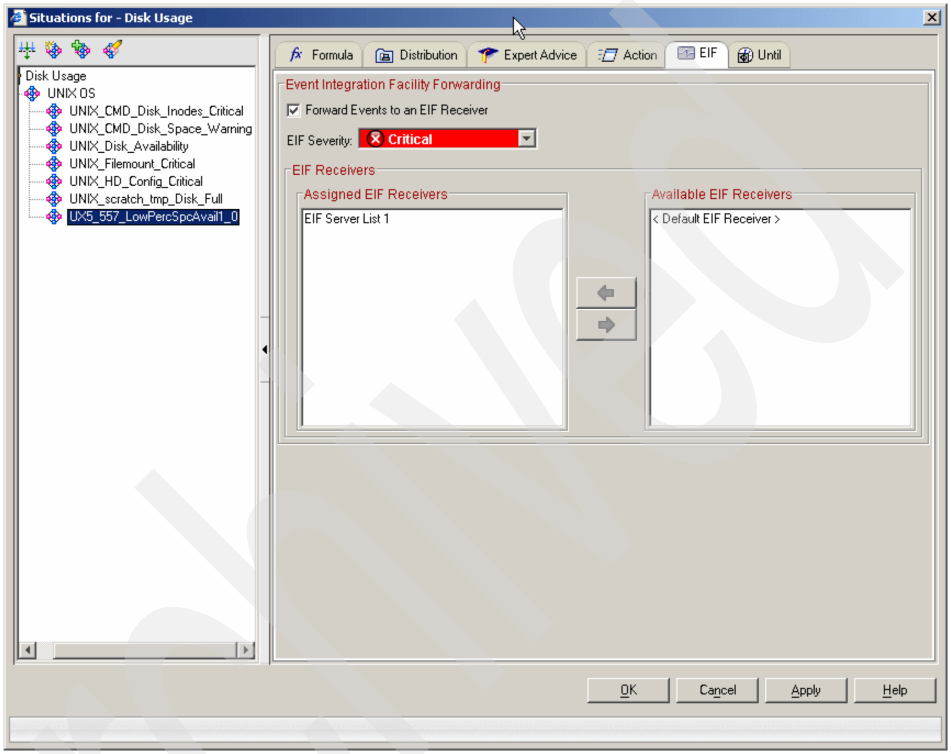
Assigned: 557_KUX

Available Managed Systems:
paris.itsc.austin.ibm.com:KUX
rp3410.itsc.austin.ibm.com:KUX
rx2620.itsc.austin.ibm.com:KUX
server2.itsc.austin.ibm.com:KUX

Available Managed System Lists:
*ALL_UNIX
564_KUX

Figure 4-19 UX5_557_LowPercSpcAvail1_0 Distribution tab

Figure 4-20 shows the EIF tab for the situation. This tab is new in IBM Tivoli Monitoring V6.2 and can be used to specify an event destination for a situation that is different from the Default EIF Receiver that is made at Tivoli Enterprise Monitoring Server configuration time. At this stage, you can also define in advance the severity that the event should have at the destination.



Event Integration Facility Forwarding

☑ Forward Events to an EIF Receiver

EIF Severity: Critical

EIF Receivers

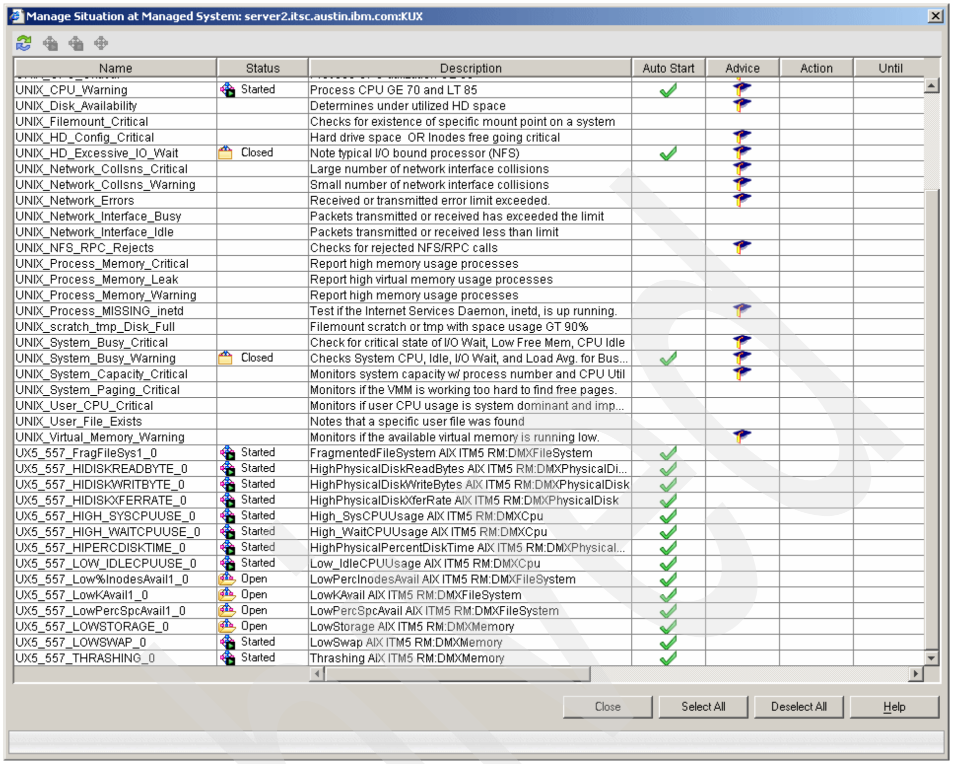
Assigned EIF Receivers: EIF Server List 1

Available EIF Receivers: < Default EIF Receiver >

Figure 4-20 UX5_557_LowPercSpcAvail1_0 EIF tab

Figure 4-21 on page 269 shows the Manage Situation dialog. In this dialog, you can see the new situations, the Auto Start parameter, and the current status of each situation.

All the migrated situations as set to run at startup.



Manage Situation at Managed System: server2.itsc.austin.ibm.com:KUX

Name	Status	Description	Auto Start	Advice	Action	Until
UNIX_CPU_Warning	Started	Process CPU GE 70 and LT 85	✓	🎓		
UNIX_Disk_Availability		Determines under utilized HD space		🎓		
UNIX_Filemount_Critical		Checks for existence of specific mount point on a system				
UNIX_HD_Config_Critical		Hard drive space OR Inodes free going critical		🎓		
UNIX_HD_Excessive_IO_Wait	Closed	Note typical I/O bound processor (NFS)	✓	🎓		
UNIX_Network_Collsns_Critical		Large number of network interface collisions		🎓		
UNIX_Network_Collsns_Warning		Small number of network interface collisions		🎓		
UNIX_Network_Errors		Received or transmitted error limit exceeded.		🎓		
UNIX_Network_Interface_Busy		Packets transmitted or received has exceeded the limit				
UNIX_Network_Interface_Idle		Packets transmitted or received less than limit				
UNIX_NFS_RPC_Rejects		Checks for rejected NFS/RPC calls		🎓		
UNIX_Process_Memory_Critical		Report high memory usage processes				
UNIX_Process_Memory_Leak		Report high virtual memory usage processes				
UNIX_Process_Memory_Warning		Report high memory usage processes				
UNIX_Process_MISSING_inetd		Test if the Internet Services Daemon, inetd, is up running.		🎓		
UNIX_scratch_tmp_Disk_Full		Filemount scratch or tmp with space usage GT 90%				
UNIX_System_Busy_Critical		Check for critical state of I/O Wait, Low Free Mem, CPU Idle		🎓		
UNIX_System_Busy_Warning	Closed	Checks System CPU, Idle, I/O Wait, and Load Avg. for Bus...	✓	🎓		
UNIX_System_Capacity_Critical		Monitors system capacity w/ process number and CPU Util		🎓		
UNIX_System_Paging_Critical		Monitors if the VMM is working too hard to find free pages.				
UNIX_User_CPU_Critical		Monitors if user CPU usage is system dominant and imp...				
UNIX_User_File_Exists		Notes that a specific user file was found				
UNIX_Virtual_Memory_Warning		Monitors if the available virtual memory is running low.		🎓		
UX5_557_FragFileSys1_0	Started	FragmentedFileSystem AIX ITM5 RM:DMXFileSystem	✓			
UX5_557_HIDISKREADBYTE_0	Started	HighPhysicalDiskReadBytes AIX ITM5 RM:DMXPhysicalDi...	✓			
UX5_557_HIDISKWRITBYTE_0	Started	HighPhysicalDiskWriteBytes AIX ITM5 RM:DMXPhysicalDisk	✓			
UX5_557_HIDISKXFERRATE_0	Started	HighPhysicalDiskXferRate AIX ITM5 RM:DMXPhysicalDisk	✓			
UX5_557_HIGH_SYSCPUUSE_0	Started	High_SysCPUUsage AIX ITM5 RM:DMXCpu	✓			
UX5_557_HIGH_WAITCPUUSE_0	Started	High_WaitCPUUsage AIX ITM5 RM:DMXCpu	✓			
UX5_557_HIPERCDISKTIME_0	Started	HighPhysicalPercentDiskTime AIX ITM5 RM:DMXPhysical...	✓			
UX5_557_LOW_IDLECPUUSE_0	Started	Low_IdleCPUUsage AIX ITM5 RM:DMXCpu	✓			
UX5_557_Low%InodesAvail1_0	Open	LowPercInodesAvail AIX ITM5 RM:DMXFileSystem	✓			
UX5_557_LowKAvail1_0	Open	LowKAvail AIX ITM5 RM:DMXFileSystem	✓			
UX5_557_LowPercSpcAvail1_0	Open	LowPercSpcAvail AIX ITM5 RM:DMXFileSystem	✓			
UX5_557_LOWSTORAGE_0	Open	LowStorage AIX ITM5 RM:DMXMemory	✓			
UX5_557_LOWSWAP_0	Started	LowSwap AIX ITM5 RM:DMXMemory	✓			
UX5_557_THRASHING_0	Started	Thrashing AIX ITM5 RM:DMXMemory	✓			

Figure 4-21   Manage Situations dialog

Step 18: Removing V5 objects after a migration

After you have migrated V5 resource models to V6 situations, the original resource models continue to run on the endpoints. The running V5 resource models do not normally interfere with the collection of monitoring data by V6. Furthermore, the V5 endpoint lcfds and the application objects are still installed on the endpoints. In fact, there is nothing to stop you from running the V5 and V6 monitoring systems side-by-side, except for the following considerations:

- Possible performance problems on the endpoint caused by having two monitoring processes running simultaneously
- Duplicate events being sent to the Tivoli Enterprise Console event server
- Monitored resources that can only provide one set of results in a given time frame, so can be monitored in V5 or V6, but not both (you are warned of this during the migration)

However, the point will come when you want to stop V5 monitoring. To do that, use the –c (cleanup) option of the **`witmmtk migrate`** command, which removes the V5 resource models and their distribution structure. You specify the objects to remove by specifying the assess files used in a preceding migration.

Once the Resource Models are removed, the migration is complete.

The endpoint lcfds and the application objects remain so that the resource models may be redistributed if necessary. Once the migration is completely successful, the V5 endpoint objects may be uninstalled (using the DMEndpointUninstall task). If the endpoint lcfds are only being used for monitoring, and not by any other Tivoli Management Framework process, they too can be uninstalled (see the Tivoli Management Framework documentation at `http://publib.boulder.ibm.com/tividd/td/ManagementFramework4.1.1.html` for details).

The cleanup operation is discussed in the following sections.

Endpoints

For each assess data file that resulted from the assessment of an endpoint, the –c option does the following:

- Removes the V5 resource models and engine (ITM5) from the endpoint.
- Unsubscribes the endpoint from every profile manager to which it is subscribed.

> **Note:** If you need to roll back the –c action, you must redistribute the ITM5 profile to the endpoint.

Example 4-29 on page 271 shows one endpoint cleanup executed in our environment.

Profiles

For each assess data file that resulted from the assessment of a profile, the –c option does the following:

- Removes the profile from the server.
- Removes the profile from every endpoint it is running on (for example, if profiles A and B are running on an endpoint, and you issue the migrate command with the –c option for the assess file for profile A, after the tool has finished, only profile B is left running on the endpoint). If the removal of a profile from an endpoint leaves the endpoint without any profiles, the endpoint is not removed by this action, but must be specifically removed.

Profile managers

For each assess data file that resulted from the assessment of a profile manager, the –c option does the following:

- Cancels every subscription to the profile manager.
- Tries to remove the profile manager. If profiles still remain, the command gives a warning to this effect. This is because profiles of types other than Tmw2kProfile could be defined (for example, the SentryProfile, which is a Tivoli Distributed Monitoring type.)

Sample cleanup procedure execution

Example 4-29 shows the cleanup procedure executed on one endpoint of our environment, called server2-ep.

Example 4-29 Cleanup procedure example

```
XML FILE

We chosen and endpoint called server2-ep with the following XML file
called server2-ep.xml

<?xml version="1.0" encoding="UTF-8"?>
<!--Copyright IBM Corporation 2006-->
<?xml-stylesheet type="text/xsl"
href="../../data/stylesheet/EndpointAssess.xsl"?>
<EndpointAssess aggregateStatus="100" hostname="server2.itsc.austin.ibm.com"
interp="aix4-r1" name="server2-ep"
xmlns="http://www.ibm.com/tivoli/itm/assess/endpoint"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="http://www.ibm.com/tivoli/itm/assess/endpoint
EndpointAssess.xsd">
  <OSTargetAgent name="server2.itsc.austin.ibm.com:KUX" product="KUX"
status="DEPLOYED" truncated="false">
    <SourceApplication sourceClass="Endpoint" sourceObject="server2-ep">
      <RunningProfiles>
        <Profile name="AIX"/>
        <Profile name="CUSTOM_PORT"/>
        <Profile name="CUSTOM_PROCESS"/>
      </RunningProfiles>
    </SourceApplication>
  </OSTargetAgent>
</EndpointAssess>

RUNNING IBM Tivoli Monitoring V5.1.2 PROFILES

The endpoint had these V5 profiles running:
```

```
C:\Tivoli\db\cairo.db\AMK\analyze\endpoints>wdmlseng -e server2-ep

Forwarding the request to the endpoint:
server2-ep  1713357986.16.522+#TMF_Endpoint::Endpoint#

The following profiles are running:

CUSTOM_PROCESS#cairo-region
        ContProcess: Running
AIX#cairo-region
        DMXCpu: Running
        DMXFileSystem: Running
        DMXMemory: Running
        DMXPhysicalDisk: Running
CUSTOM_PORT#cairo-region
        CheckPort: Running

CLEANUP COMMAND

The following command removes the V5 engine from server2-ep endpoint,
unsubscribes the endpoint, removes the profiles and attempts to remove
the profile managers:

The cleanup command sintax is showed below:

C:>witmmtk migrate -x
C:\Tivoli\db\cairo.db\AMK\analyze\endpoints\server2-ep.xml -c
.
AMKUT0016I Processing the request.

AMKUT0057I Loading the infrastructure baseline file:
"C:\Tivoli\db\cairo.db\AMK\analyze\scans\1713357986.xml".
AMKUT7075I Processing endpoint: "server2-ep".
AMKUT7115W Warning in processing endpoint "server2-ep": the endpoint
was cleaned up but at least one profile belonging to it is still
defined on the Tivoli management region server.
.
AMKUT0010W The command completed with warnings. See log
"C:\Tivoli\db\cairo.db\AMK\logs\log_wmtkmigrate_20071103_01_49_27.log"
 for more information.

The above warning message simply means that the same resource model is
distributed to other endpoints not yet cleaned up, therefore the
migration toolkit cannot remove the whole profile and pofile manager
structure, to prevent problems with the other resources using them.
```

```
CHECKS AFTER THE CLEANUP EXECUTION

At cleanup completed we verified that the IBM Tivoli Monitoring V5.1.2
engine was not running anymore one the enpoint.

C:\Tivoli\db\cairo.db\AMK\analyze\endpoints>wdmlseng -e server2-ep

Forwarding the request to the endpoint:
server2-ep  1713357986.16.522+#TMF_Endpoint::Endpoint#

AMW0051E - The engine is not running or is unreachable.

The above message means that the IBM Tivoli Monitoring V5.1.2 engine
has been successfully remove from the Endpoint. This can be verified
running this commands:

C:\>wlookup -ar Endpoint |grep server2-ep
server2-ep      1713357986.16.522+#TMF_Endpoint::Endpoint#

The above command is used to find out the endpoint OID that is used for
the next command:

C:\>wep boot_method list "" 1713357986.16.522+#TMF_Endpoint::Endpoint#
No Boot Method defined for Endpoint
1713357986.16.522+#TMF_Endpoint::Endpoint# and tag ""

The above command lists the boot methods of the endpoints, so all the
processes that start automatically with the endpoint restart. When an
IBM Tivoli Monitoring V5.1.2 profile is distributed for the first time
on an endpoint, the engine is installed, started and the resource model
loaded. Furthermore, the boot method is created.
Running the same command on an endpoint not yet cleaned up will show
the boot method called DMAE_boot_engine:

C:\>wep boot_method list "" 1713357986.7.522+#TMF_Endpoint::Endpoint#
Boot Method(s) for Endpoint 1713357986.7.522+#TMF_Endpoint::Endpoint#
Tag                      Prototype Object     Method Name
tmnt_boot                1713357986.1.993     DMAE_boot_engine

References to the boot method can also be found in the endpoint
lcfd.log file and you can look for messages starting with that method
to troubleshoot problems with the engine.
```

```
A subsequent restart of the IBM Tivoli Monitoring V5.1.2 engine will
cause the engine file to be distributed again to the endpoint, via the
dependecy mechanism, but as expected no profiles are running on the
endpoint cause the cleanup procedure successfully removed them.

C:\Tivoli\db\cairo.db\AMK\analyze\endpoints>wdmlseng -e server2-ep

Forwarding the request to the endpoint:
server2-ep  1713357986.16.522+#TMF_Endpoint::Endpoint#

AMW0250I - No profiles are running on the endpoint.
```

Once you execute the procedure, you can open the Tivoli desktop to check, for example, that the endpoint has been successfully unsubscribed from the profile managers containing the Tmw2kProfile that were previously distributed on it.

Figure 4-22 shows two profile managers, ITM_AIX_PM and ITM_CUSTOM_PM, that contain some Tmw2kProfiles that were previously distributed on the endpoint called server2-ep: AIX, CUSTOM_PROCESS, and CUSTOM_PORT.

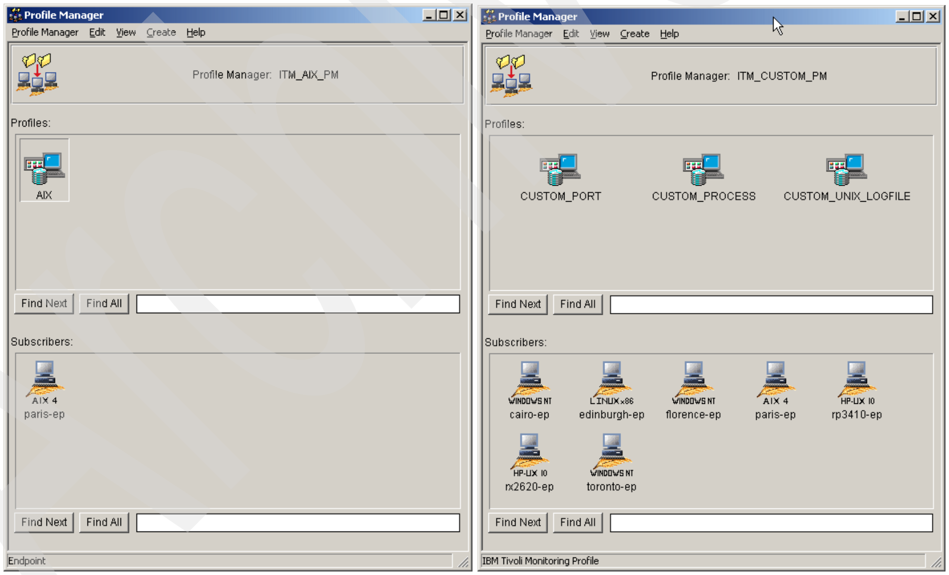


Figure 4-22 AIX and custom profile managers

As you can see, the server2-ep endpoint is no longer in the subscribers list.

The cleanup procedure should perform these steps:

- Remove the IBM Tivoli Monitoring V5.1.2 engine.
- Unsubscribe the endpoint.
- Remove the profiles.
- Attempt to remove the profile manager.

The last two actions has not been executed in our environment cause there are other endpoint that are subscribed to those profile managers and are using the above profiles that are distributed and running on them.

To perform a complete cleanup of the IBM Tivoli Monitoring V5.1.2 environment you should run the command **`witmmtk migrate -c`** without any other parameter.

In that case, the above cleanup steps are executed for all the resources defined in the assess files that reside in the default locations.

4.5 Migration toolkit internal flow

In this section, we describe the internal flow of the migration toolkit steps:

- Use **`scantmr`**.
- Assess.
- Migrate.
- Migrate an OS agent.

For each step, we provide an internal diagram describing all the components involved in the specific operation.

4.5.1 scantmr

Figure 4-23 on page 276 shows the internal flow of the **`scantmr`** step.

This step basically invokes two objects:

- TME® Corba is an implementation of an interface called MigrationITMManager::scanTMR that collects all the ITMv5 infrastructure data in terms of Servers, Gateways, Endpoints, and EventServers.
- JAVA Module provides a class called ScanTMR that is used to analyze ITM V5.1.2 data and produce an ITM V6.2 equivalent infrastructure. The result of the analysis is then saved in the baseline file in the format TMR_OID.xml.

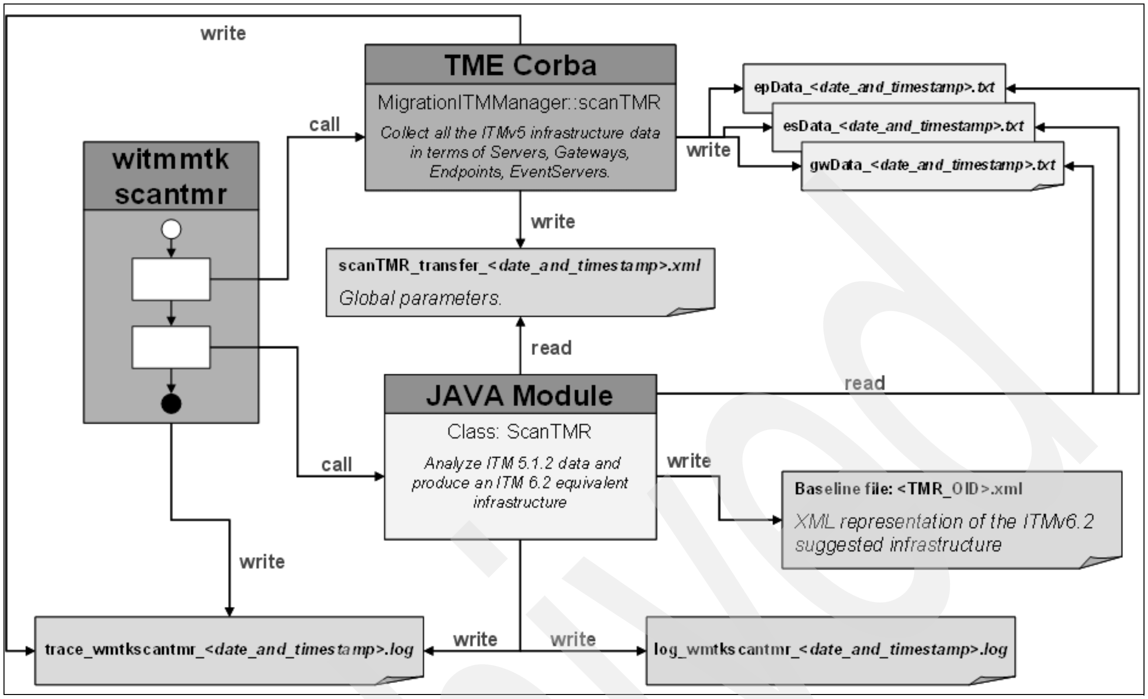

write
TME Corba
MigrationITMManager::scanTMR
Collect all the ITMv5 infrastructure data in terms of Servers, Gateways, Endpoints, EventServers.
call
witmmtk scantmr
write
epData_<date_and_timestamp>.txt
esData_<date_and_timestamp>.txt
gwData_<date_and_timestamp>.txt
write
scanTMR_transfer_<date_and_timestamp>.xml
Global parameters.
read
JAVA Module
Class: ScanTMR
Analyze ITM 5.1.2 data and produce an ITM 6.2 equivalent infrastructure
read
call
write
Baseline file: <TMR_OID>.xml
XML representation of the ITMv6.2 suggested infrastructure
write
trace_wmtkscantmr_<date_and_timestamp>.log
write
write
log_wmtkscantmr_<date_and_timestamp>.log

Figure 4-23 scantmr internal flow

4.5.2 Assess

Figure 4-24 on page 277 shows the internal flow of the assess step.

Two objects are invoked:

- TME Corba is an implementation of an interface called MigrationITMManager::assess that collects all the IBM Tivoli Monitoring V 5 configuration in terms of Endpoints, Profiles, and Profile Managers.
- JAVA Module provides a class called AssessHandler that is used to process ITM V5.1.2 data and produce an IBM Tivoli Monitoring V6.2 equivalent configuration.

The baseline file generated in the previous step is read and updated. Another XML file is generated for the assessed resource. This file represents the IBM Tivoli Monitoring V6.2 suggested configuration for that resource.

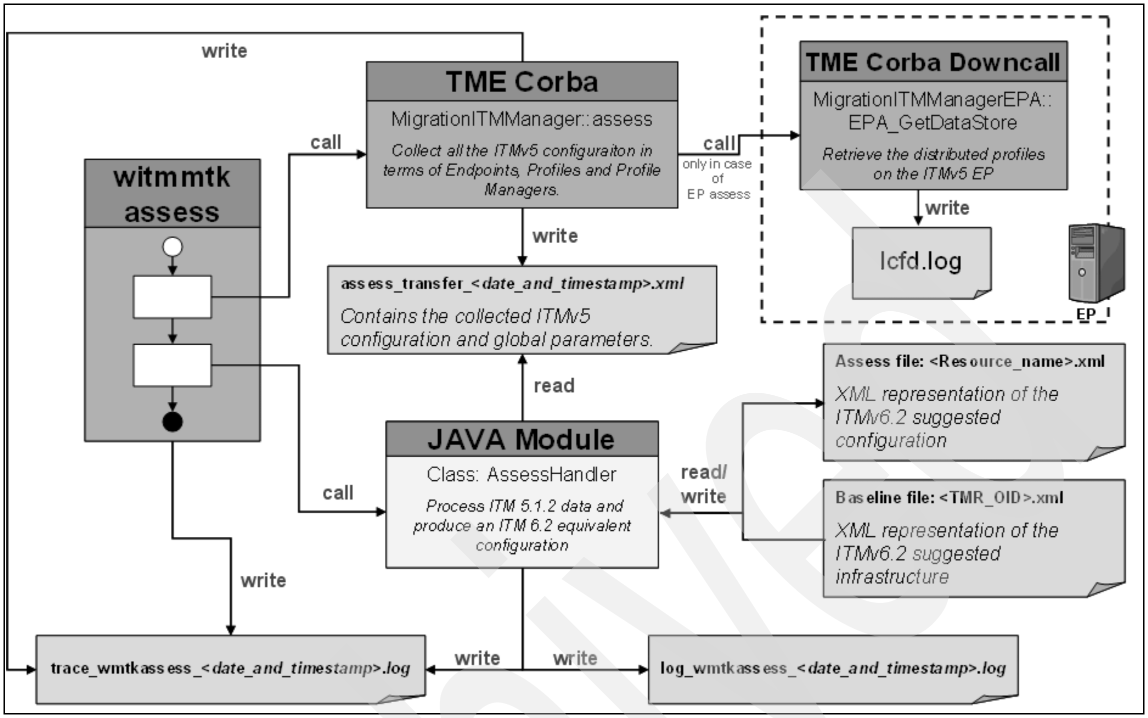

write
TME Corba
MigrationITMManager::assess
Collect all the ITMv5 configuraiton in terms of Endpoints, Profiles and Profile Managers.
call
call
only in case of EP assess
TME Corba Downcall
MigrationITMManagerEPA::
EPA_GetDataStore
Retrieve the distributed profiles on the ITMv5 EP
write
lcfd.log
EP
witmmtk assess
write
assess_transfer_<date_and_timestamp>.xml
Contains the collected ITMv5 configuration and global parameters.
read
Assess file: <Resource_name>.xml
XML representation of the ITMv6.2 suggested configuration
JAVA Module
Class: AssessHandler
Process ITM 5.1.2 data and produce an ITM 6.2 equivalent configuration
call
read/ write
Baseline file: <TMR_OID>.xml
XML representation of the ITMv6.2 suggested infrastructure
write
trace_wmtkassess_<date_and_timestamp>.log
write
write
log_wmtkassess_<date_and_timestamp>.log

Figure 4-24 Assess internal flow

4.5.3 Migrate

Figure 4-25 on page 278 shows the internal flow of the migrate step.

This step uses the XML file for the assessed resource, generated in the previous step, and uses a JAVA Module that provides a class called Migrate, which is responsible for interacting with the IBM Tivoli Monitoring V6.2 monitoring server and portal server to create, update, or remove the IBM Tivoli Monitoring V6.2 entities.

As for the previous steps, both the baseline and interested resource XML files are used.

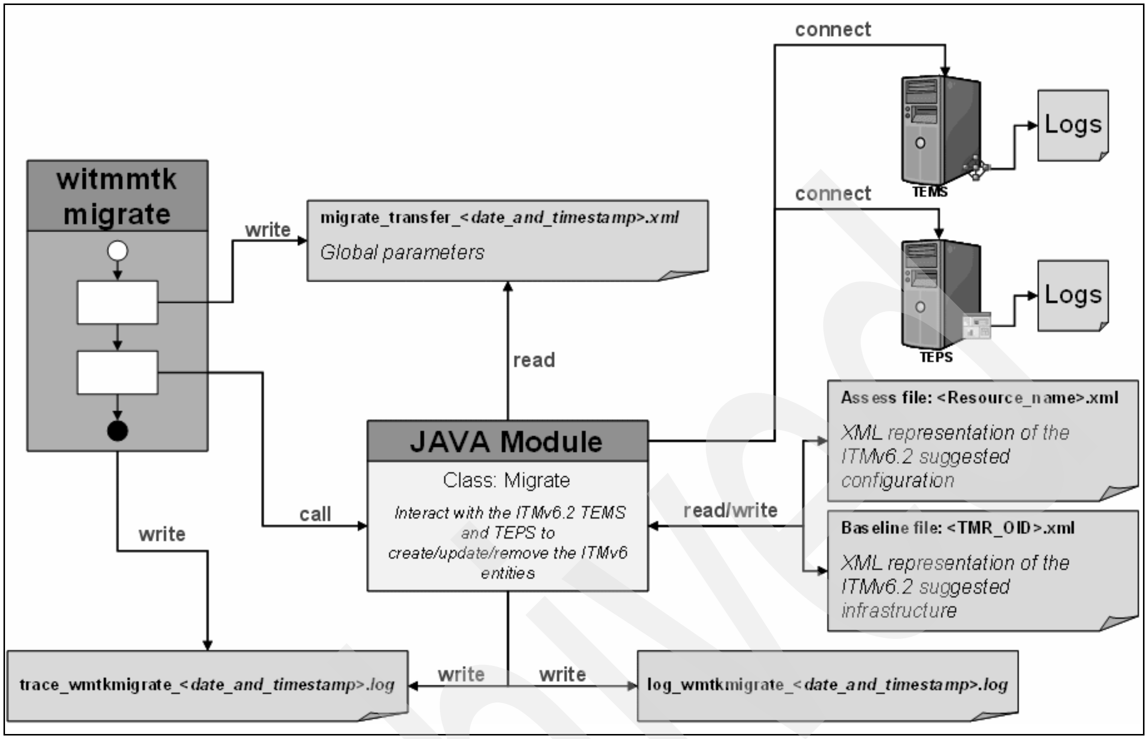

connect
Logs
TEMS
witmmtk migrate
write
migrate_transfer_<date_and_timestamp>.xml
Global parameters
connect
Logs
TEPS
read
Assess file: <Resource_name>.xml
XML representation of the ITMv6.2 suggested configuration
JAVA Module
Class: Migrate
Interact with the ITMv6.2 TEMS and TEPS to create/update/remove the ITMv6 entities
call
read/write
write
Baseline file: <TMR_OID>.xml
XML representation of the ITMv6.2 suggested infrastructure
trace_wmtkmigrate_<date_and_timestamp>.log
write
write
log_wmtkmigrate_<date_and_timestamp>.log

Figure 4-25 Migrate internal flow

4.5.4 Migrate an OS agent

Figure 4-26 on page 279 shows the internal flow of the migration of an OS agent.

This step still uses the Migrate Java class that in this case is responsible for interacting with the Tivoli Management Framework.

A call is made to a Corba object, an interface called MigrationITMManagerEPA::installOSAgent. This interface defines a dependency called ITMMTKInstallOSAgent, which is responsible for downloading a script called createNode.sh to the hub monitoring server endpoint; this script runs the **`tacmd createNode`** command on the monitoring server.

An output file containing the result of the **`tacmd createNode`** command is saved in the monitoring server endpoint directories.

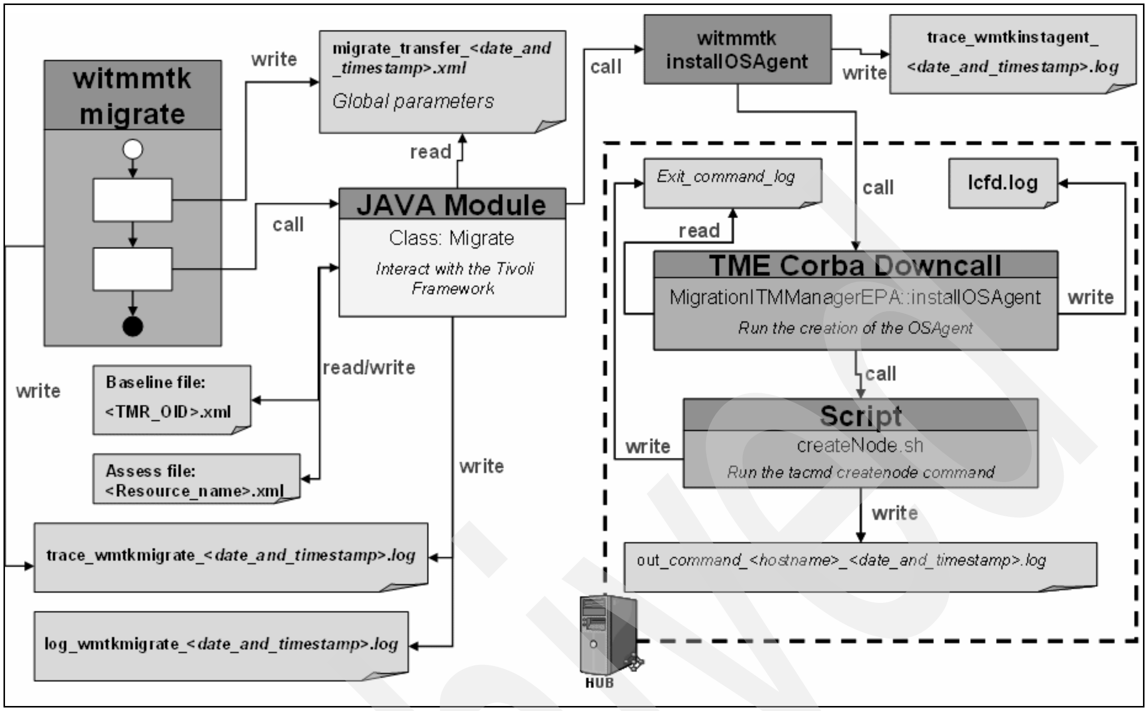

witmmtk migrate
write
migrate_transfer_<date_and _timestamp>.xml
Global parameters
read
call
JAVA Module
Class: Migrate
Interact with the Tivoli Framework
call
witmmtk installOSAgent
write
trace_wmtkinstagent_ <date_and_timestamp>.log
Exit_command_log
call
lcfd.log
read
TME Corba Downcall
MigrationITMManagerEPA::installOSAgent
Run the creation of the OSAgent
write
call
Script
createNode.sh
Run the tacmd createnode command
write
write
out_command_<hostname>_<date_and_timestamp>.log
write
read/write
Baseline file: <TMR_OID>.xml
Assess file: <Resource_name>.xml
write
trace_wmtkmigrate_<date_and_timestamp>.log
log_wmtkmigrate_<date_and_timestamp>.log
HUB

Figure 4-26 Migrate an OS agent internal flow

4.5.5 Files produced by the toolkit

In this section, we provide a summary of the files produced by the toolkit phase by phase. We do not refer to the logs and traces in this section.

Files locations:

- UNIX: $DBDIR/AMK/
- Windows: %DBDIR%\AMK\

These paths are the starting point for the following file locations.

Scantmr

- temp/epData_<date_and_timestamp>.txt
- temp/esData_ <date_and_timestamp>.txt
- temp/gwData_ <date_and_timestamp>.txt
- temp/scanTMR_transfer_<date_and_timestamp>.xml

- analyze/scans/<TMR_OID>.xml (Baseline file: will be updated during the endpoint assess and migrate phases)

Assess

We detail the logs for each resource.

Endpoint

- temp/assess_transfer_<date_and_timestamp>.xml
- analyze/endpoints/epName.xml

Profile

- temp/assess_transfer_<date_and_timestamp>.xml
- analyze/profiles/profileName.xml

ProfileManagers

- temp/assess_transfer_<date_and_timestamp>.xml
- analyze/profilemanagers/profilemanagerName.xml
- analyze/profiles/profileName.xml
- analyze/endpoints/epName.xml

Migrate

- temp/migrate_transfer_<date_and_timestamp>.xml

4.6 Problem determination

In this section, we describe some common scenarios you can encounter while dealing with the migration toolkit.

4.6.1 The scantmr tool

Here we discuss a scenario concerning the **`scantmr`** tool.

Scenario

The infrastructure baseline file could not be saved.

Possible cause:

The baseline file has been locked.

Solution:

If there are no reasons for locking the file, do the following:

- Run the **`unlock`** command.
- Rerun the **`scantmr`** command.
- Rerun the assess tool.

4.6.2 Assess tool

Here we discuss a scenario concerning the assess tool.

Scenario

The assess operation fails with a file creation error.

Possible cause:

The object has a name that is not permitted as a file name, so the creation of the assess file, which uses the object name, fails.

Solution:

- Rename the object in V5 (and propagate the changed object throughout the region, as appropriate).
- Rerun the **`scantmr`** tool.
- Rerun the assess tool.

4.6.3 Agent deployment

Here we discuss scenarios concerning agent deployment.

Scenario 1

The OS Agent deployment fails with the message:

```
A specified authentication package is unknown.
```

Possible causes are:

- No endpoint lcfd is installed on the appropriate hub server.
- The endpoint lcfd installation did not complete correctly.
- The endpoint lcfd correctly installed, but the hub server did not reboot.

Scenario 2

The deployment of the first agent for a hub monitoring server fails with error code 13 (= user credential not correct), but the user credentials are correct.

Possible cause:

An endpoint lcfd was already installed on the computer where the Tivoli Enterprise Monitoring Server is installed and being used as a Hub.

Solution:

- Stop and restart the endpoint lcfd to read the IBM Tivoli Monitoring environment configuration.
- Retry the agent deployment.

Scenario 3

The deployment of the first agent for a hub monitoring server fails with error code 15 (= agent already exists, or not enough temporary space available), but the agent does not exists and there is enough temp space.

Possible cause:

The remote_control_endpoint (the name of the Tivoli endpoint located on the Hub monitoring server) started before the Hub installation.

Solution:

- Recycle the endpoint lcfd.
- Retry the agent deployment.

Scenario 4

The deployment of agents stops because a truncated agent name is found.

Possible cause:

A V6 agent name can be no more than 32 characters long. Names generated by the agent-specific algorithm, longer than 32 characters, are truncated by the V6 module, and the agent is deployed with the truncated name.

Solution:

- Rename the agent (to avoid duplicates).
- In the endpoint assess file:
  - Change the agent name to the new name.
  - Change the value of the attribute "truncated" from "true" to "false".

- If the agent is an OS agent, change the infrastructure baseline for the agent to reflect the new name.

4.7 Migrating custom resource models

The procedure for migrating a custom resource model differs in these possible respects for one for a standard resource model:

- When performing the migration, the resource model mapping file used by the assess command must be created, either by copying and editing an existing mapping file, or by creating it from scratch.
- To evaluate this mapping file, you might need to create a Java resource model plug-in class, which allows you to add your own coding to the standard evaluation used by the toolkit.
- If the resource model data collection is different from that used by the standard resource models, you might also have to create a new agent to collect the data using the agent builder. For this agent, you will also need to create an agent mapping file to enable the migration to work correctly.
- If the data collection in the agent cannot be provided by standard operating system facilities, you might need to create a Java agent plug-in class to do the collection.

When these items have been developed and tested, the actual migration follows exactly the same steps as the migration of standard resource models.

Thus, the procedure for migrating custom resource models requires you take the following steps:

1. Perform a basic analysis of the resource model to determine the level of customization. This should help you to determine whether you require plug-ins or a new agent, or both, in addition to the obligatory resource model mapping file.
2. Analyze the resource model to list the thresholds, parameters, and other entities it uses, and render the logic of the resource model in the boolean expressions required for V6.2.
3. Optionally, use the resource model analyzer tool to create the resource model mapping file.
4. As an alternative to using the tool, use the data you recorded in step 2 and create the resource model mapping file manually. You can create the file from scratch, or base it on an existing mapping file from a standard resource model, or one you have already created yourself.

5. If the resource model mapping file contains any of the following, create a Java resource model plug-in class that the toolkit will run during the migration:
   - Complex parameters that need special coding to be parsed
   - Context variables that need to be manipulated
   - A restriction on the creation of the V6.2 situation that has a condition that requires special coding
6. If the resource model data collection cannot be performed by the standard agent at the appropriate endpoints, create a custom agent using the agent builder tool.
7. If you have created a custom agent, create the corresponding agent mapping file.
8. If the custom agent cannot collect the data you require using the standard operating system facilities, create a Java agent plug-in class that the toolkit will run during the migration.
9. Assess the profile that contains the custom resource model, as described in 4.4.4, “Phase C: Migrating the profiles” on page 231.
10. Check very carefully that the created situations map exactly what you require, paying particular attention that the V6.2 agent attributes have been correctly described.
11. The custom resource model can now be fully migrated.

All the above mentioned steps are described in a very detailed way in Part 3, “Migrating custom resource models”, in *Upgrading from IBM Tivoli Monitoring V5.1.2*, GC32-1976.

4.7.1 Resource model Analyzer tool

For customers that have developed their own resource models on IBM Tivoli Monitoring V5.1.2, the resource model Analyzer Tool (RM Analyzer Tool) offers specific migration assistance.

The RM Analyzer tool is expected to be published shortly in the IBM Tivoli Monitoring section of the IBM Service-Oriented Architecture Business Catalog (OPAL) at:

http://catalog.lotus.com/wps/portal/tm

The RM Analyzer Tool provides a quick start for creating resource model mapping files.

This tool is separate from the migration toolkit, operates independently, and can be used in conjunction with the IBM Tivoli Monitoring Migration Toolkit to prepare the conversion of IBM Tivoli Monitoring V5.1.2 PAC resource model indications into IBM Tivoli Monitoring V6.2 situations.

Note: PAC stands for Proactive Analysis Component. For PAC resource models, we refer to any base IBM Tivoli Monitoring V5.1.2 and IBM Tivoli Monitoring (for Databases, Applications, Messaging, and Collaboration and so on) resource models.

This tool installs easily, is easy to invoke, and executes very quickly on a per resource model basis to analyze one or more resource models.

With the input being a single resource model or any number of resource models combined into a single subdirectory, the RM Analyzer Tool conducts a best-effort analysis of the VisitTree logic in the resource model and writes the output to two XML files:

- One output file contains the XML representation of logic relative to resource model indications.
- A resource model mapping file that can be used as input into the migration toolkit.

The mapping files are not in final form, but can be completed with minimal effort from the user. The analysis output contains information that recommends and assists in completing the mapping file.

The RM Analyzer Tool will not successfully process all types of custom resource models and custom metrics into situations. It supports JavaScript™ resource models only (.dmjsws and .jrm). In those cases where the tool cannot interpret the resource model successfully, it states that and gives information pertaining to why it could not.

It will, however, provide an XML template that can be used to manually create situations that will run in an IBM Tivoli Monitoring V6.2 environment.

Note: The RM Analyzer Tool does not support Visual Basic®. Thus, for resource models that were generated by Visual Basic, the user will be required to generate their own mapping files using the resultant template provided by the RM Analyzer Tool.

Custom resource model categories

Based on direct interaction with several customers and our review of their custom-built resource models, the custom resource models are classified into one of the following categories.

- Level A. The resource model was created by altering a shipped resource model. In this category, only thresholds or parameters were added to the default IBM Tivoli Monitoring V5.1.2 resource model and the VisitTree complexity did not vary from the basic resource model.

  Level A custom resource models are mapped more easily than the other categories only by virtue of their consistency with IBM Tivoli Monitoring V5.1.2 default resource models. The output offers the most assured metric parity in IBM Tivoli Monitoring V6.2 agent situations.

  The VisitTree can be collapsed into one or more Boolean expressions. The user will be required to modify the XML mapping file to prepare input into the migration toolkit, which will complete the IBM Tivoli Monitoring V6.2 situation.

- Level B1. The resource model VisitTree was completely re-written and the metrics were collected using IBM Tivoli Monitoring V5.1.2 pre-built data collectors.

  Level B1 custom resource models are mapped with a consistency similar to Level A. The output is a metric parity that is ensured by IBM Tivoli Monitoring V6.2 infrastructure.

  The VisitTree can again be collapsed into one or more Boolean expressions. The user is required to modify the XML mapping files to map custom resource models by using the RM Analyzer Tool first and then feeding the output into the migration toolkit.

- Level B2. The resource model VisitTree was completely re-written and the metrics were collected using specific scripts directly invoked from the VisitTree.

  These custom scripts are not available in IBM Tivoli Monitoring V6.2. In this case, data providers are implemented using the IBM Tivoli Monitoring V6.2 Agent Builder or the IBM Tivoli Monitoring Universal Agent (ITM UA).

  The VisitTree can be collapsed into one or more Boolean expressions. The user is required to use the IBM Tivoli Monitoring V6.2 Agent Builder or the UA to create a specific IBM Tivoli Monitoring V6.2 agent. These will use the output from the RM Analyzer Tool and the migration toolkit to build the IBM Tivoli Monitoring V6.2 situations.

- Level C. The resource model was completely built from scratch with both VisitTree and data collectors that have been developed by the IBM Tivoli Monitoring V5.1.2 user. The metrics collected by this custom data provider are not available in IBM Tivoli Monitoring V6.2.

Much like Level B2, the data provider can be implemented using the IBM Tivoli Monitoring V6.2 Agent Builder or the Universal Agent.

The VisitTree can be collapsed into one or more Boolean expressions. The user builds the required agent by using the IBM Tivoli Monitoring V6.2 Agent Builder or the Universal Agent. The output from the RM Analyzer Tool and the migration toolkit provides the IBM Tivoli Monitoring V6.2 situations.

The RM Analyzer Tool provides analysis and output based on the complexity of the custom resource models from any level.

Important: In all cases after the RM Analyzer Tool is run, manual intervention is required prior to the invocation of the migration toolkit.

In any cases where the RM Analyzer Tool cannot provide acceptable metric parity, an XML mapping file template is still created for the user to manually alter prior to using the migration toolkit.

Installation

The RM Analyzer Tool can be installed on any workstation running Windows or Linux. We recommend that the workstation where it is installed is separate from the IBM Tivoli Monitoring V5.1.2 Tivoli Management Region, where the migration toolkit will be installed.

Workstation and software specifications required for the RM Analyzer Tool to successfully install and run are discussed in the following sections.

OS versions

- Windows
- Linux

You can use any version of the above operating systems that support Java Version 5.0.

Java version

Java Version 5.0 plus Java plug-ins

Java Version 5.0 must be installed and used to load the plug-ins.
Java Version 5.0 is not included on the RM Analyzer Tool image. It can be accessed through the IBM Tivoli Monitoring V6.2 Agent Builder or IBM Tivoli Monitoring V6.2 or otherwise installed in the customer environment.

The IBM Tivoli Monitoring V6.2 Agent Builder or IBM Tivoli Monitoring V6.2 must be installed first so that the RM Analyzer Tool can use that Java to load the plug-ins (if not otherwise installed in the customer environment).

Eclipse version

Not required, but if you use it, use Version 3.2 or higher.

The RM Analyzer Tool includes Java jar files and Eclipse plug-ins required for customer jar files. There is no requirement for Eclipse to be installed anywhere for the RM Analyzer Tool to run.

Eclipse is therefore not included on the RM Analyzer Tool image and is not required to be accessible from IBM Tivoli Monitoring or otherwise in the customer environment. The plug-ins can be downloaded without Eclipse. However, Eclipse can be used to download the plug-ins required for the RM Analyzer Tool. Furthermore, if Eclipse is installed, the plug-ins might already be available, and it would not be necessary to use those that are shipped on the RM Analyzer Tool image.

The RM Analyzer Tool provided as additional material for this book will come in the form of a zip and tar files. The user needs only to unbundle the file into a single subdirectory. A separate script for Windows and UNIX environments is provided to invoke the RM Analyzer Tool, as shown in Example 4-30.

Example 4-30 RM Analyzer Tools invoke script

```
UNIX environment:

export
CLASSPATH=$CLASSPATH:./IBMTivoliRMAnalyze.jar:./org.eclipse.emf.common_
2.2.0.v200606271057.jar:./org.eclipse.equinox.common_3.2.0.v20060603.ja
r:./org.eclipse.core.runtime_3.2.0.v20060603.jar:./ibmjs.jar:./org.ecli
pse.emf.ecore_2.2.0.v200606271057.jar:./org.eclipse.emf.comon_2.2.0.v20
0606271057.jar
java com.ibm.domo.tivoli.RMAnalyzer $@

Windows environment:

@setlocal
@set
classpath=.\IBMTivoliRMAnalyze.jar;.\org.eclipse.emf.common_2.2.0.v2006
06271057.jar;.\org.eclipse.equinox.common_3.2.0.v20060603.jar;.\org.ecl
ipse.core.runtime_3.2.0.v20060603.jar;.\ibmjs.jar;.\org.eclipse.emf.eco
re_2.2.0.v200606271057.jar;.\org.eclipse.emf.comon_2.2.0.v200606271057.
jar;%CLASSPATH%
@java com.ibm.domo.tivoli.RMAnalyzer %1 %2 %3 %4
@endlocal
```

Note: The execute script assumes one subdirectory is used to contain the jar files. If Eclipse is used, the plug-ins will not be found in a single subdirectory. The script runs with or without Eclipse installed.

You could modify the sample scripts provided in the above example, based on the version of the RM Analyzer Tool you are using. In the case of a later version, the file names can change.

Running the RM Analyzer Tool

The user executes the RM Analyzer Tool by invoking either the Windows script or the UNIX script provided. These are simple CLI scripts that execute the commands necessary for tool operation. The script finds the jar files in the specified subdirectory, puts in a class path, and then calls the RM Analyzer Tool to execute those jar files.

We recommend that the first execution of the RM Analyzer Tool be done without parameters specified so that the usage statement is displayed. This describes the options and their syntax. Example 4-31 shows the script invocation result on a Windows box.

Example 4-31 RM Analyzer Tool invocation

```
First check that the Java version installed on the system is supported
by the tool:

Z:\Templates\addmat\rmanalyzer-d3>java -version
java version "1.5.0"
Java(TM) 2 Runtime Environment, Standard Edition (build
pwi32devifx-20070706 (SR5 + IZ00983))
IBM J9 VM (build 2.3, J2RE 1.5.0 IBM J9 2.3 Windows XP x86-32
j9vmwi3223-2007042
6 (JIT enabled)
J9VM - 20070420_12448_lHdSMR
JIT  - 20070419_1806_r8
GC   - 200704_19)
JCL  - 20070706

Then execute the script:

Z:\Templates\addmat\rmanalyzer-d3>RMAnalyze.bat
ITM v6.2 resource model Analysis tool, v0.6

RMAnalyze [-o outDir] <RMfile | dir>
```

```
Options:
-o   specify the subdirectory where analysis output is written. The
default
     is to put the output in the same directory as the analyzed
resource model.
where:
     RMfile:  is the filename for an ITMv5 resource model source file.
              to be analyzed.
     dir:     is a subdirectory containing ITMv5 resource models. All
              resource models in the subdirectory will be analyzed.
```

So to summarize, an IBM Tivoli Monitoring V5.1.2 resource model is the input to the RM Analyzer Toolkit, and the XML file with indication analysis and XML mapping file are the outputs.

The main input parameter required is the subdirectory where the resource model or resource models are located and to which the analysis is to be written. The subdirectory location is pointed to through the execution parameter.

The RM Analyzer Tool can operate on a single resource model or multiple resource models in batch fashion. If there is more than one resource model in the input subdirectory, the tool will serially process each resource model in the order in which it is listed in the subdirectory. The output will appear in sequential fashion.

Example 4-32 shows the execution of the tool.

Example 4-32 Sample RM Analyzer Tool execution

```
In our example we are using these custom resource model files:

Z:\Templates\addmat\rmanalyzer-d3\shell-examples>dir
 Volume in drive Z is Data
 Volume Serial Number is DODC-B9E1

 Directory of Z:\Templates\addmat\rmanalyzer-d3\shell-examples

10/17/2007  02:45 PM    <DIR>          .
10/17/2007  02:45 PM    <DIR>          ..
10/17/2007  02:41 PM    <DIR>          CVS
11/17/2006  09:39 AM            25,089 UNIX_ITM_CPPM.jrm
11/17/2006  10:10 AM            12,231 UNIX_ITM_DiskError.jrm
11/17/2006  10:07 AM            68,464 UNIX_ITM_Diskmon.jrm
08/03/2006  01:45 AM            11,905 UNIX_ITM_DumpWaiter.jrm
09/14/2006  04:27 AM            14,930 UNIX_ITM_GPFSMon.jrm
05/26/2006  02:53 AM            12,781 UNIX_ITM_Logfile.jrm
```

```
09/12/2006  06:28 AM            28,163 UNIX_Sun_Temperature.jrm
              21 File(s)        285,055 bytes
               3 Dir(s) 12,471,835,007 bytes free

The ouptut of the RM Analyzer Tool execution follows:

Z:\Templates\addmat\rmanalyzer-d3>RMAnalyze.bat
Z:\Templates\addmat\rmanalyzer-d3\shell-examples
ITM v6.2 resource model Analysis tool, v0.6

Processing path[file:/Z:/Templates/addmat/rmanalyzer-d3/shell-examples]
RM[UNIX
_ITM_CPPM.jrm]
scriptDir:    file:/Z:/Templates/addmat/rmanalyzer-d3/shell-examples
oDir:    /Z:/Templates/addmat/rmanalyzer-d3/shell-examples
Processing completed for RM[UNIX_ITM_CPPM.jrm]

Processing path[file:/Z:/Templates/addmat/rmanalyzer-d3/shell-examples]
RM[UNIX
_ITM_DiskError.jrm]
scriptDir:    file:/Z:/Templates/addmat/rmanalyzer-d3/shell-examples
oDir:    /Z:/Templates/addmat/rmanalyzer-d3/shell-examples
Processing completed for RM[UNIX_ITM_DiskError.jrm]

Processing path[file:/Z:/Templates/addmat/rmanalyzer-d3/shell-examples]
RM[UNIX
_ITM_Diskmon.jrm]
scriptDir:    file:/Z:/Templates/addmat/rmanalyzer-d3/shell-examples
oDir:    /Z:/Templates/addmat/rmanalyzer-d3/shell-examples
Processing completed for RM[UNIX_ITM_Diskmon.jrm]

Processing path[file:/Z:/Templates/addmat/rmanalyzer-d3/shell-examples]
RM[UNIX
_ITM_DumpWaiter.jrm]
scriptDir:    file:/Z:/Templates/addmat/rmanalyzer-d3/shell-examples
oDir:    /Z:/Templates/addmat/rmanalyzer-d3/shell-examples
Processing completed for RM[UNIX_ITM_DumpWaiter.jrm]

Processing path[file:/Z:/Templates/addmat/rmanalyzer-d3/shell-examples]
RM[UNIX
_ITM_GPFSMon.jrm]
scriptDir:    file:/Z:/Templates/addmat/rmanalyzer-d3/shell-examples
oDir:    /Z:/Templates/addmat/rmanalyzer-d3/shell-examples
Processing completed for RM[UNIX_ITM_GPFSMon.jrm]
Processing path[file:/Z:/Templates/addmat/rmanalyzer-d3/shell-examples]
RM[UNIX
_ITM_Logfile.jrm]
scriptDir:    file:/Z:/Templates/addmat/rmanalyzer-d3/shell-examples
oDir:    /Z:/Templates/addmat/rmanalyzer-d3/shell-examples
Processing completed for RM[UNIX_ITM_Logfile.jrm]

Processing path[file:/Z:/Templates/addmat/rmanalyzer-d3/shell-examples]
RM[UNIX
_Sun_Temperature.jrm]
scriptDir:    file:/Z:/Templates/addmat/rmanalyzer-d3/shell-examples
oDir:    /Z:/Templates/addmat/rmanalyzer-d3/shell-examples
Processing completed for RM[UNIX_Sun_Temperature.jrm]


7 RMs processed.

The seven resource models have been processes in sequential order, and
the following output files has been created:

Z:\Templates\addmat\rmanalyzer-d3\shell-examples>dir
 Volume in drive Z is Data
 Volume Serial Number is DODC-B9E1

 Directory of Z:\Templates\addmat\rmanalyzer-d3\shell-examples

10/17/2007  02:45 PM    <DIR>          .
10/17/2007  02:45 PM    <DIR>          ..
10/17/2007  02:41 PM    <DIR>          CVS
11/17/2006  09:39 AM            25,089 UNIX_ITM_CPPM.jrm
10/17/2007  02:44 PM            14,918 UNIX_ITM_CPPM.jrm.xml
10/17/2007  02:44 PM             3,574 UNIX_ITM_CPPM_1_1.xml
11/17/2006  10:10 AM            12,231 UNIX_ITM_DiskError.jrm
10/17/2007  02:45 PM             7,228 UNIX_ITM_DiskError.jrm.xml
10/17/2007  02:45 PM             2,051 UNIX_ITM_DiskError_1_1.xml
11/17/2006  10:07 AM            68,464 UNIX_ITM_Diskmon.jrm
10/17/2007  02:45 PM            30,913 UNIX_ITM_Diskmon.jrm.xml
10/17/2007  02:45 PM             8,189 UNIX_ITM_Diskmon_4_13.xml
08/03/2006  01:45 AM            11,905 UNIX_ITM_DumpWaiter.jrm
10/17/2007  02:45 PM             5,307 UNIX_ITM_DumpWaiter.jrm.xml
10/17/2007  02:45 PM             1,740 UNIX_ITM_DumpWaiter_1_9.xml
09/14/2006  04:27 AM            14,930 UNIX_ITM_GPFSMon.jrm
10/17/2007  02:45 PM            14,492 UNIX_ITM_GPFSMon.jrm.xml
10/17/2007  02:45 PM             3,400 UNIX_ITM_GPFSMon_1_14.xml
05/26/2006  02:53 AM            12,781 UNIX_ITM_Logfile.jrm
```

```
10/17/2007  02:45 PM             8,184 UNIX_ITM_Logfile.jrm.xml
10/17/2007  02:45 PM             2,062 UNIX_ITM_Logfile_1_9.xml
09/12/2006  06:28 AM            28,163 UNIX_Sun_Temperature.jrm
10/17/2007  02:45 PM             6,536 UNIX_Sun_Temperature.jrm.xml
10/17/2007  02:45 PM             2,898 UNIX_Sun_Temperature_1_9.xml
              21 File(s)        285,055 bytes
               3 Dir(s)  12,471,549,952 bytes free
```

RM Analyzer Tool Output

Once the RM Analyzer tool is run, the output is one XML file per resource model, metric analysis, an XML mapping file, and a summary of the resource model Level categories found, as shown in Example 4-32 on page 290. If multiple resource models are contained in the in the input subdirectory, the summary also provides a tally for the number of resource models found and processed in each category.

The output XML files and analysis can either be stored into a specified subdirectory or displayed through STDOUT (Standard Output) to a console. In the above example, we did not specify the -o option, so the file has been generated in the same path as the custom resource model location.

Example 4-33 shows the first XML file with the result of the resource model metrics analysis.

Example 4-33   Metric analysis XML file

```
<ITM modelName="UNIX_ITM_Logfile">
  <event name="TMW_UNIXLogfileIsOld">
    <attribute name="rem_assign" kind="string" />
    <attribute name="file_time" kind="string" />
    <attribute name="probe_arg" kind="string" />
    <attribute name="rem_sev" kind="string" />
    <attribute name="email_addr" kind="string" />
    <attribute name="notif_page" kind="string" />
  </event>
  <raise event="TMW_UNIXLogfileIsOld"
         lineNumber="123">
    <condition>
      <PRIMITIVE>
        <constant value="ELEMENT_OF" type="class java.lang.String"/>
        <PRIMITIVE position="[104:31]->[104:56]">
          <constant value="&amp;lt;Code body of function
Lprologue.js/stringSplit&amp;gt;" type="class java.lang.String"/>
          <PRIMITIVE position="[104:31]->[104:44]">
```

```
            <constant value="EACH_ELEMENT_OF" type="class
java.lang.String"/>
            <PRIMITIVE position="[94:21]->[94:48]">
              <constant value="&amp;lt;Code body of function
Lprologue.js/stringSplit&amp;gt;" type="class java.lang.String"/>
              <PRIMITIVE position="[166:26]->[166:53]">
                <constant value="SHELL" type="class java.lang.String"/>
                <constant value="UNIX_logfile.pl" type="class
java.lang.String"/>
              </PRIMITIVE>
            </PRIMITIVE>
          </PRIMITIVE>
        </PRIMITIVE>
        <constant value="0.0" type="class java.lang.Double"/>
      </PRIMITIVE>
    </condition>
    <metric name="probe_arg"
            lineNumber="117">
      <value>
        <PRIMITIVE position="[106:31]->[106:41]">
          <constant value="ELEMENT_OF" type="class java.lang.String"/>
          <PRIMITIVE position="[104:31]->[104:56]">
            <constant value="&amp;lt;Code body of function
Lprologue.js/stringSplit&amp;gt;" type="class java.lang.String"/>
            <PRIMITIVE position="[104:31]->[104:44]">
              <constant value="EACH_ELEMENT_OF" type="class
java.lang.String"/>
              <PRIMITIVE position="[94:21]->[94:48]">
                <constant value="&amp;lt;Code body of function
Lprologue.js/stringSplit&amp;gt;" type="class java.lang.String"/>
                <PRIMITIVE position="[166:26]->[166:53]">
                  <constant value="SHELL" type="class
java.lang.String"/>
                  <constant value="UNIX_logfile.pl" type="class
java.lang.String"/>
                </PRIMITIVE>
              </PRIMITIVE>
            </PRIMITIVE>
          </PRIMITIVE>
          <constant value="0.0" type="class java.lang.Double"/>
        </PRIMITIVE>
      </value>
    </metric>
    <metric name="rem_sev"
            lineNumber="119">
```

```
   <value>
    <PRIMITIVE position="[108:32]->[108:42]">
     <constant value="ELEMENT_OF" type="class java.lang.String"/>
     <PRIMITIVE position="[104:31]->[104:56]">
      <constant value="&amp;lt;Code body of function
Lprologue.js/stringSplit&amp;gt;" type="class java.lang.String"/>
      <PRIMITIVE position="[104:31]->[104:44]">
       <constant value="EACH_ELEMENT_OF" type="class
java.lang.String"/>
       <PRIMITIVE position="[94:21]->[94:48]">
        <constant value="&amp;lt;Code body of function
Lprologue.js/stringSplit&amp;gt;" type="class java.lang.String"/>
        <PRIMITIVE position="[166:26]->[166:53]">
         <constant value="SHELL" type="class
java.lang.String"/>
         <constant value="UNIX_logfile.pl" type="class
java.lang.String"/>
        </PRIMITIVE>
       </PRIMITIVE>
      </PRIMITIVE>
     </PRIMITIVE>
     <constant value="2.0" type="class java.lang.Double"/>
    </PRIMITIVE>
   </value>
  </metric>
  <metric name="email_addr"
      lineNumber="120">
   <value>
    <PRIMITIVE position="[110:29]->[110:39]">
     <constant value="ELEMENT_OF" type="class java.lang.String"/>
     <PRIMITIVE position="[104:31]->[104:56]">
      <constant value="&amp;lt;Code body of function
Lprologue.js/stringSplit&amp;gt;" type="class java.lang.String"/>
      <PRIMITIVE position="[104:31]->[104:44]">
       <constant value="EACH_ELEMENT_OF" type="class
java.lang.String"/>
       <PRIMITIVE position="[94:21]->[94:48]">
        <constant value="&amp;lt;Code body of function
Lprologue.js/stringSplit&amp;gt;" type="class java.lang.String"/>
        <PRIMITIVE position="[166:26]->[166:53]">
         <constant value="SHELL" type="class
java.lang.String"/>
         <constant value="UNIX_logfile.pl" type="class
java.lang.String"/>
        </PRIMITIVE>
```

```
              </PRIMITIVE>
            </PRIMITIVE>
          </PRIMITIVE>
          <constant value="4.0" type="class java.lang.Double"/>
        </PRIMITIVE>
      </value>
    </metric>
    <metric name="notif_page"
            lineNumber="121">
      <value>
        <PRIMITIVE position="[111:34]->[111:45]">
          <constant value="ELEMENT_OF" type="class java.lang.String"/>
          <PRIMITIVE position="[104:31]->[104:56]">
            <constant value="&amp;lt;Code body of function 
Lprologue.js/stringSplit&amp;gt;" type="class java.lang.String"/>
            <PRIMITIVE position="[104:31]->[104:44]">
              <constant value="EACH_ELEMENT_OF" type="class 
java.lang.String"/>
              <PRIMITIVE position="[94:21]->[94:48]">
                <constant value="&amp;lt;Code body of function 
Lprologue.js/stringSplit&amp;gt;" type="class java.lang.String"/>
                <PRIMITIVE position="[166:26]->[166:53]">
                  <constant value="SHELL" type="class 
java.lang.String"/>
                  <constant value="UNIX_logfile.pl" type="class 
java.lang.String"/>
                </PRIMITIVE>
              </PRIMITIVE>
            </PRIMITIVE>
          </PRIMITIVE>
          <constant value="5.0" type="class java.lang.Double"/>
        </PRIMITIVE>
      </value>
    </metric>
    <metric name="file_time"
            lineNumber="122">
      <value>
        <PRIMITIVE position="[107:33]->[107:43]">
          <constant value="ELEMENT_OF" type="class java.lang.String"/>
          <PRIMITIVE position="[104:31]->[104:56]">
            <constant value="&amp;lt;Code body of function 
Lprologue.js/stringSplit&amp;gt;" type="class java.lang.String"/>
            <PRIMITIVE position="[104:31]->[104:44]">
              <constant value="EACH_ELEMENT_OF" type="class 
java.lang.String"/>
```

```
       <PRIMITIVE position="[94:21]->[94:48]">
        <constant value="&amp;lt;Code body of function 
Lprologue.js/stringSplit&amp;gt;" type="class java.lang.String"/>
        <PRIMITIVE position="[166:26]->[166:53]">
         <constant value="SHELL" type="class 
java.lang.String"/>
         <constant value="UNIX_logfile.pl" type="class 
java.lang.String"/>
        </PRIMITIVE>
       </PRIMITIVE>
      </PRIMITIVE>
     </PRIMITIVE>
     <constant value="1.0" type="class java.lang.Double"/>
    </PRIMITIVE>
   </value>
  </metric>
  <metric name="rem_assign"
      lineNumber="118">
   <value>
    <PRIMITIVE position="[109:35]->[109:45]">
     <constant value="ELEMENT_OF" type="class java.lang.String"/>
     <PRIMITIVE position="[104:31]->[104:56]">
      <constant value="&amp;lt;Code body of function 
Lprologue.js/stringSplit&amp;gt;" type="class java.lang.String"/>
      <PRIMITIVE position="[104:31]->[104:44]">
       <constant value="EACH_ELEMENT_OF" type="class 
java.lang.String"/>
       <PRIMITIVE position="[94:21]->[94:48]">
        <constant value="&amp;lt;Code body of function 
Lprologue.js/stringSplit&amp;gt;" type="class java.lang.String"/>
        <PRIMITIVE position="[166:26]->[166:53]">
         <constant value="SHELL" type="class 
java.lang.String"/>
         <constant value="UNIX_logfile.pl" type="class 
java.lang.String"/>
        </PRIMITIVE>
       </PRIMITIVE>
      </PRIMITIVE>
     </PRIMITIVE>
     <constant value="3.0" type="class java.lang.Double"/>
    </PRIMITIVE>
   </value>
  </metric>
 </raise>
```

```
</ITM>
```

Example 4-34 shows the second XML file, the resource model mapping file.

Example 4-34   RM mapping file

```
<?xml version="1.0" encoding="UTF-8"?>
<rmmap:ResourceModelMapping
    xmlns:rmmap="http://www.ibm.com/tivoli/rm/mapping"
    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
    xsi:schemaLocation="http://www.ibm.com/tivoli/rm/mapping 
ResourceModelMapping.xsd"
    version="1.0"
    rmVersion="1.9"
    copyright="TODO: ***Enter Copyright***"
    name="UNIX_ITM_Logfile">

  <!-- ===== -->
  <!-- TODO: Enter 3-char application ID of the target ITMv6 agent for 
this RM mapping. -->
  <rmmap:Application applicationID="???">

    <rmmap:ResourceModelIndications>
      <!--## Indication ##-->
      <rmmap:IndicationMapping name="TMW_UNIXLogfileIsOld" 
supported="true">
        <!-- ===== -->
        <!-- TODO: Enter the 2-char situation prefix from the 
applicationID above. -->
        <!-- ===== -->
        <!-- TODO: Enter the attribute identifier that will be the key 
attribute for this situation. -->
        <rmmap:Situation situationPrefix="??5_$_TMW_UNIXLogflIsOld" 
displayItem="***keyAttribute***">
          <rmmap:Predicate>
            <rmmap:Row>
              <!-- ===== -->
              <!-- TODO: Attribute derived using the following 
operations in resource model:  (see next line) -->
              <!-- TODO: 
ELEMENT_OF[0.0]/<stringSplit>/EACH_ELEMENT_OF/<stringSplit>    -->
              <rmmap:ConstantCondition function="*VALUE" 
attribute="SHELL(UNIX_logfile.pl)" value="" operator="*NE"/>
            </rmmap:Row>
          </rmmap:Predicate>
        </rmmap:Situation>
      </rmmap:IndicationMapping>
```

You should now complete the information with the prefix “TODO”, at a minimum, the copyright and the application ID.

If the custom resource model is of Level A or B1, you do not need a resource model mapping file cause they directly come with the migration toolkit.

The resource model we used is of a B2 Level, cause it uses a script to collect some data, so the logical sequence of steps to deal with these kind of custom resource models would be:

1. Use the RM analyzer tool to make a first analysis of the resource model.
2. Use the IBM Tivoli Monitoring V6.2 Agent Builder or the Universal Agent to create your custom agent and define the attributes that will be used for the migration process. When using the IBM Tivoli Monitoring V6.2 Agent Builder, the agent mapping file is also created. The agent mapping file contains the metric definitions, and the resource model mapping files the logic.
3. Customize the resource model mapping by completing the “TODO” sections before invoking the migration toolkit to create situations based on it.

A B2 resource model also defines new metrics. This can be seen in the resource model mapping file after the first analysis from the RM Analyzer Tool by looking at the following line:

```
<rmmap:ConstantCondition function="*VALUE"
attribute="SHELL(UNIX_logfile.pl)" value="" operator="*NE"/>
```

To simplify this example, we customized our resource model mapping file using the application ID of the UNIX OS agent, KUX; in this case, the agent mapping file is already provided with the migration toolkit.

We used Process.CPU_Utilization as our attribute.

Example 4-35 shows the modified resource model mapping file. The bold text represents the customization.

Example 4-35 Analyzed resource model mapping file

```
<?xml version="1.0" encoding="UTF-8"?>
<rmmap:ResourceModelMapping
    xmlns:rmmap="http://www.ibm.com/tivoli/rm/mapping"
    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
    xsi:schemaLocation="http://www.ibm.com/tivoli/rm/mapping
ResourceModelMapping.xsd"
    version="1.0"
    rmVersion="1.9"
    copyright="ITSO"
    name="UNIX_ITM_Logfile">

  <!-- ===== -->
  <!-- TODO: Enter 3-char application ID of the target ITMv6 agent for
this RM mapping. -->
  <rmmap:Application applicationID="KUX">

    <rmmap:ResourceModelIndications>
      <!--## Indication ##-->
      <rmmap:IndicationMapping name="TMW_UNIXLogfileIsOld"
supported="true">
        <!-- ===== -->
        <!-- TODO: Enter the 2-char situation prefix from the
applicationID above. -->
        <!-- ===== -->
        <!-- TODO: Enter the attribute identifier that will be the key
attribute for this situation. -->
        <rmmap:Situation situationPrefix="UX5_$_TMW_UNIXLogflIsOld"
displayItem="***keyAttribute***">
          <rmmap:Predicate>
            <rmmap:Row>
              <!-- ===== -->
              <!-- TODO: Attribute derived using the following
operations in resource model:  (see next line) -->
              <!-- TODO:
ELEMENT_OF[0.0]/<stringSplit>/EACH_ELEMENT_OF/<stringSplit>    -->
              <rmmap:ConstantCondition function="*VALUE"
attribute="Process.CPU_Utilization" value="85" operator="*NE"/>
            </rmmap:Row>
          </rmmap:Predicate>
        </rmmap:Situation>
      </rmmap:IndicationMapping>
```

The XML mapping files, once completed by the user, are then used as input to the migration toolkit to complete the migration from resource model indication to agent situations.

Additionally, the user may need to set prefixes and alter the attributes depending on the analysis provided. Other user actions vary depending upon the resource model level category and complexity.

For example, if the RM Analyzer Tool cannot provide analysis for a specific metric (it could be any Level), the attribute mappings are not provided and the user must use the analysis and template provided to complete the XML mapping file prior to using it as input to the migration toolkit.

In cases where the RM Analyzer Toolkit cannot provide full analysis, the user will need to open the resource model source and manually fill in the XML mapping file template provided by the tool. The key to completing the XML mapping file is for the user to determine what it takes to generate an IBM Tivoli Monitoring V6.2 agent situation from a resource model indication mapping.

The user then has to synthesize it into the XML mapping file prior to inputting it to the migration toolkit.

In some cases, there are restrictions or predicates that have conditions that require special handling in order to generate mapping input that is similar to out-of-box IBM Tivoli Monitoring V5.1.2 mappings for existing resource models.

Once the XML mapping file is completed, the user then goes to the Tivoli Management Region where the migration toolkit is installed and specifies the subdirectory in BINDIR where the custom resource model directories are located.

The migration toolkit is then executed and the custom resource models are migrated to IBM Tivoli Monitoring V6.2 agent Situations similar to IBM Tivoli Monitoring V5.1.2 provided resource models.

Please refer to *Upgrading from IBM Tivoli Monitoring V5.1.2*, GC32-1976 for specific detailed installation, procedure, and output information.

Example 4-36 shows the import and the distribution of the custom resource model into the IBM Tivoli Monitoring V5.1.2 infrastructure.

Example 4-36 Installing a custom resource model into an ITM V5.1.2 infrastructure

```
The below command has been used to load the custom resource model in
the Tivoli Management Region server:

C:\Tivoli\bin\lcf_bundle.40\Tmw2k\Rm>wdmrm -add UNIX_ITM_Logfile.tar

IBM Tivoli Monitoring - Adding new resource model

Parsing configuration file UNIX_ITM_Logfile.conf ...
Configuration file successfully parsed.
Checking for event redefinition...
Starting resource UNIX_ITM_Logfile registration ...
The resource UNIX_ITM_Logfile has been successfully stored.
Registration completed.

Copying UNIX_ITM_Logfile.cat msgfile ...
Copying UNIX_ITM_Logfile.cat zipfile ...

Installation completed.

Once the resource model has been added in a profile and distributed to
an endpoint, you can run the below command to check if it is running
fine:

C:\WINDOWS>wdmlseng -e rp3410-ep -verbose

Forwarding the request to the endpoint:
rp3410-ep  1713357986.8.522+#TMF_endpoint::endpoint#

The following profiles are running:

CUSTOM_PORT#cairo-region
        CheckPort: Running
                CheckPort_Error 0 %
HPUX#cairo-region
        DMXPhysicalDisk: Running
                HighPhysicalDiskWriteBytes 100 %
                HighPhysicalPercentDiskTime 100 %
                HighPhysicalDiskXferRate 100 %
                HighPhysicalDiskReadBytes 100 %
        DMXFileSystem: Running
```

```
                LowKAvail 100 %
                LowPercSpcAvail 100 %
                LowPercInodesAvail 100 %
                FragmentedFileSystem 100 %
        DMXMemory: Running
                Thrashing 100 %
                LowSwap 100 %
                LowStorage 100 %
        DMXCpu: Running
                High_SysCPUUsage 100 %
                Low_IdleCPUUsage 100 %
                High_WaitCPUUsage 100 %
CUSTOM_PROCESS#cairo-region
        ContProcess: Running
                ContProcess_Error 100 %
CUSTOM_UNIX_LOGFILE#cairo-region
        UNIX_ITM_Logfile: Running
                TMW_UNIXLogfileIsOld 0 %

As you can see in the last part of the above output, the status of the
UNIX_ITM_Logfile resource model is Running.
```

Example 4-37 shows the result of the Tmw2kProfile assessment.

Example 4-37 Assessing the profiles

```
C:\Tivoli\db\cairo.db\AMK\analyze\profiles>witmmtk assess -i
profiles_cus.txt

AMKUT0016I Processing the request.
.
AMKUT5003I Loading the resource snapshot for the assessment.
AMKUT0057I Loading the infrastructure baseline file:
"C:\Tivoli\db\cairo.db\AMK\analyze\scans\1713357986.xml".
AMKUT5006I Starting the resource assessment.
AMKUT5074I Converting profile "CUSTOM_UNIX_LOGFILE".
AMKUT5078I Converting resource model "UNIX_ITM_Logfile".
AMKUT5009I The number of "situations" created for resource model
"UNIX_ITM_Logfile" is 1.
AMKUT5007I All resources are assessed. Processing is complete.
.
AMKUT0008I The command completed successfully. See log
"C:\Tivoli\db\cairo.db\AMK\logs\log_wmtkassess_20071120_17_29_10.log"fo
r more information.
```

The result of the profile assess is the XML file shown in Example 4-38.

Example 4-38 XML file resulting from the profile assess

```
<?xml version="1.0" encoding="UTF-8"?>
<!--Copyright IBM Corporation 2006-->
<?xml-stylesheet type="text/xsl"
href="../../data/stylesheet/ProfileAssess.xsl"?>
<ProfileAssess aggregateStatus="0" comment=""
name="CUSTOM_UNIX_LOGFILE"
xmlns="http://www.ibm.com/tivoli/itm/assess/profile"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="http://www.ibm.com/tivoli/itm/assess/profile
ProfileAssess.xsd">
  <ResourceModelAssess aggregateStatus="0" comment=""
name="UNIX_ITM_Logfile">
    <TargetSituation action="" advice=""
affinity="00f200000000000000000000000000000#m000000000"
applicationID="KUX" association="" autoStart="true"
description="TMW_UNIXLogfileIsOld CUSTOM_UNIX_LOGFILE ITM5
RM:UNIX_ITM_Logfi" displayItem="***keyAttribute***"
displaySeverity="Critical" distribution="" eventSeverity="CRITICAL"
multipleIntervals="NYN" name="UX5_566_TMW_UNIXLogflIsOld_0"
persistence="1" predicate="*IF ( *VALUE Process.CPU_Utilization *NE
'85' )" samplingIntervalDays="0" samplingIntervalTime="0:5:0"
status="NOT_DEPLOYED"/>
  </ResourceModelAssess>
  <TECEventServers status="NOT_DEPLOYED">
    <TECEventServer name="9.3.5.205" port="0"/>
  </TECEventServers>
</ProfileAssess>
```

The status is “NOT_DEPLOYED” cause the migration did not take place yet.

In Example 4-39, you can see the result of the profile migration. It also lists the commands related to the profile manager assess and migration.

Example 4-39 Migrating profiles and profile managers

```
The below command is used to migrate the custom Tmw2kProfile called
CUSTOM_UNIX_LOGFILE:

C:\Tivoli\db\cairo.db\AMK\analyze\profiles>witmmtk migrate -d
"%DBDIR%\AMK\analyze\profiles\custom" -u
.
AMKUT0016I Processing the request.
```

```
AMKUT0057I Loading the infrastructure baseline file:
"C:\Tivoli\db\cairo.db\AMK\analyze\scans\1713357986.xml".
AMKUT7076I Processing profile: "CUSTOM_UNIX_LOGFILE".
AMKUT7078I Migrating resource model "UNIX_ITM_Logfile" for hub
monitoring server "HUB_TEMS".
AMKUT7100I The situation "UX5_566_TMW_UNIXLogflIsOld_0" was added.
.
AMKUT0008I The command completed successfully. See log
"C:\Tivoli\db\cairo.db\AMK\logs\log_wmtkmigrate_20071120_17_33_48.log"f
or more information.
```

The resulting XML file after the migration will looks like:

```
<?xml version="1.0" encoding="UTF-8"?>
<!--Copyright IBM Corporation 2006-->
<?xml-stylesheet type="text/xsl"
href="../../data/stylesheet/ProfileAssess.xsl"?>
<ProfileAssess aggregateStatus="100" comment=""
name="CUSTOM_UNIX_LOGFILE"
xmlns="http://www.ibm.com/tivoli/itm/assess/profile"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="http://www.ibm.com/tivoli/itm/assess/profile
ProfileAssess.xsd">
  <ResourceModelAssess aggregateStatus="100" comment=""
name="UNIX_ITM_Logfile">
    <TargetSituation action="" advice=""
affinity="00f20000000000000000000000000000#m000000000"
applicationID="KUX" association="" autoStart="true"
description="TMW_UNIXLogfileIsOld CUSTOM_UNIX_LOGFILE ITM5
RM:UNIX_ITM_Logfi" displayItem="***keyAttribute***"
displaySeverity="Critical" distribution="" eventSeverity="CRITICAL"
multipleIntervals="NYN" name="UX5_566_TMW_UNIXLogflIsOld_0"
persistence="1" predicate="*IF ( *VALUE Process.CPU_Utilization *NE
'85' )" samplingIntervalDays="0" samplingIntervalTime="0:5:0"
status="DEPLOYED"/>
  </ResourceModelAssess>
  <TECEventServers status="DEPLOYED">
    <TECEventServer name="9.3.5.205" port="0"/>
  </TECEventServers>
</ProfileAssess>
```

Once migrated the profile, we have to migrate the profile managers to create the distribution list. In the below example we used the “-o force” option cause the profile manager has been assessed before.

```
C:\Tivoli\db\cairo.db\AMK\analyze\profilemanagers>witmmtk assess -pm
ITM_CUSTOM_PM -o force

AMKUT0016I Processing the request.
.....
AMKUT5003I Loading the resource snapshot for the assessment.
AMKUT0057I Loading the infrastructure baseline file:
"C:\Tivoli\db\cairo.db\AMK\analyze\scans\1713357986.xml".
AMKUT5006I Starting the resource assessment.
AMKUT5077I The "-o force" option was specified. For any resources that
have previously been assessed, the tool makes a new ass
essment and overwrites the previous one. After this assess has
finished, you must rerun the assess of the Profile Manager or M
anagers to which these resources belong.
AMKUT5075I Converting endpoint "cairo-ep".
AMKUT5073I Converting application object "MDIST2@DB2@cairo-ep".
AMKUT5073I Converting application object "PLANNER@DB2@cairo-ep".
AMKUT5073I Converting application object "cairo-ep".
AMKUT5075I Converting endpoint "edinburgh-ep".
AMKUT5073I Converting application object "edinburgh-ep".
AMKUT5075I Converting endpoint "florence-ep".
AMKUT5073I Converting application object "florence-ep".
AMKUT5075I Converting endpoint "paris-ep".
AMKUT5073I Converting application object "paris-ep".
AMKUT5075I Converting endpoint "rp3410-ep".
AMKUT5073I Converting application object "rp3410-ep".
AMKUT5075I Converting endpoint "rx2620-ep".
AMKUT5073I Converting application object "rx2620-ep".
AMKUT5075I Converting endpoint "toronto-ep".
AMKUT5073I Converting application object "toronto-ep".
AMKUT5074I Converting profile "CUSTOM_UNIX_LOGFILE".
AMKUT5078I Converting resource model "UNIX_ITM_Logfile".
AMKUT5009I The number of "situations" created for resource model
"UNIX_ITM_Logfile" is 1.
AMKUT5080I Converting profile manager ITM_CUSTOM_PM.
AMKUT5007I All resources are assessed. Processing is complete.
.
AMKUT0008I The command completed successfully. See log
"C:\Tivoli\db\cairo.db\AMK\logs\log_wmtkassess_20071120_18_14_19.log"fo
r more information.

Once assessed the profile manager, the migrate will create the Managed
System lists and associate them to the previously created situations.
```

```
C:\Tivoli\db\cairo.db\AMK\analyze\profilemanagers\custom>witmmtk
migrate -d "%DBDIR%\AMK\analyze\profilemanagers\custom" -u
.
AMKUT0016I Processing the request.

AMKUT0057I Loading the infrastructure baseline file:
"C:\Tivoli\db\cairo.db\AMK\analyze\scans\1713357986.xml".
AMKUT7077I Processing profile manager: "ITM_CUSTOM_PM".
AMKUT7080I Creating managed system list "566_KUX" for hub monitoring
server "HUB_TEMS".
AMKUT7010W The agent "rp3410:KUX" has already been deployed, but with a
different name "rp3410.itsc.austin.ibm.com:KUX" than t
hat used in the endpoint assess file. The assess file and
infrastructure baseline (if appropriate) have been updated with the
new name.
AMKUT7617I The managed system list "566_KUX" was added.
AMKUT7621I Associating situations for resource model "UNIX_ITM_Logfile"
to managed systems in the managed system list "566_KUX
".
AMKUT7622I All the situations were successfully associated to the
managed systems in the managed system list "566_KUX".
.
AMKUT0010W The command completed with warnings. See log
"C:\Tivoli\db\cairo.db\AMK\logs\log_wmtkmigrate_20071120_18_17_30.log"
 for more information.
```

To make sure that the migration process completed successfully, you can run some simple commands on the hub monitoring server to make sure the resources have been created, as shown in Example 4-40.

Example 4-40   Checks at migration completed

```
To list the newly created managed system lists use this command:

[root@edinburgh ~]# tacmd listsystemlist|grep 566_KUX
566_KUX                  UNIX OS

The below command provides details on a specific managed system list,
showing the belonging agents:

[root@edinburgh ~]# tacmd viewsystemlist -l 566_KUX
Name                  : 566_KUX
Type                  : UNIX OS
Assigned Managed List : rp3410.itsc.austin.ibm.com:KUX
```

```
Available Managed List:
paris.itsc.austin.ibm.com:KUX,rx2620.itsc.austin.ibm.com:KUX,server2.it
sc.austin.ibm.com:KUX

To check that the situations has been updated to include to correct
managed system list in its distribution you can run this command:

[root@edinburgh ~]# tacmd viewsit -s UX5_566_TMW_UNIXLogflIsOld_0
Name                      : UX5_566_TMW_UNIXLogflIsOld_0
Description               : TMW_UNIXLogfileIsOld CUSTOM_UNIX_LOGFILE
ITM5 RM:UNIX_ITM_Logfi
Type                      : UNIX OS
Formula                   : *IF ( *VALUE Process.CPU_Utilization *NE
'85' )
Sampling Interval         : 0/0:5:0
Run At Start Up           : Yes
Distribution              : 566_KUX
Text                      :
Action Location           : Agent
Action Selection          : System Command
Universal Message Category:
Universal Message Severity:
Universal Message         :
True For Multiple Items   : Action on First item only
TEC Severity              : Critical
TEC Forwarding            : Y
TEC Destination           : 1
```

After completion of this step, you can perform the cleanup procedure described in 4.4.6, “Viewing the results and cleaning up” on page 263.

5

Integrating event management systems

This chapter provides instructions for implementing event integration by forwarding situation events to Tivoli Enterprise Console or Netcool/OMNIbus.

The following topics are discussed:

- “Event integration with Tivoli Enterprise Console” on page 310
- “Event integration with Netcool/OMNIbus” on page 321
- “Configuring connectors for the common event console” on page 331

5.1 Event integration with Tivoli Enterprise Console

If you are using Tivoli Enterprise Console, you can configure the hub monitoring servers to forward situation events to the Tivoli Enterprise Console event server (referred to as the *event server*) for correlation and management. To view updates to the forwarded situation events in the Tivoli Enterprise Portal, you need to install the IBM Tivoli Monitoring Event Synchronization component on the event server. The Event Synchronization component enables changes in the event status made on the Tivoli Enterprise Console to be reflected on the Tivoli Enterprise Portal.

In this section, we show how to configure situation event forwarding and synchronization using Tivoli Enterprise Console running in AIX 5L™ V5.3 and IBM Tivoli Monitoring V6.2, as described in Figure 5-1.

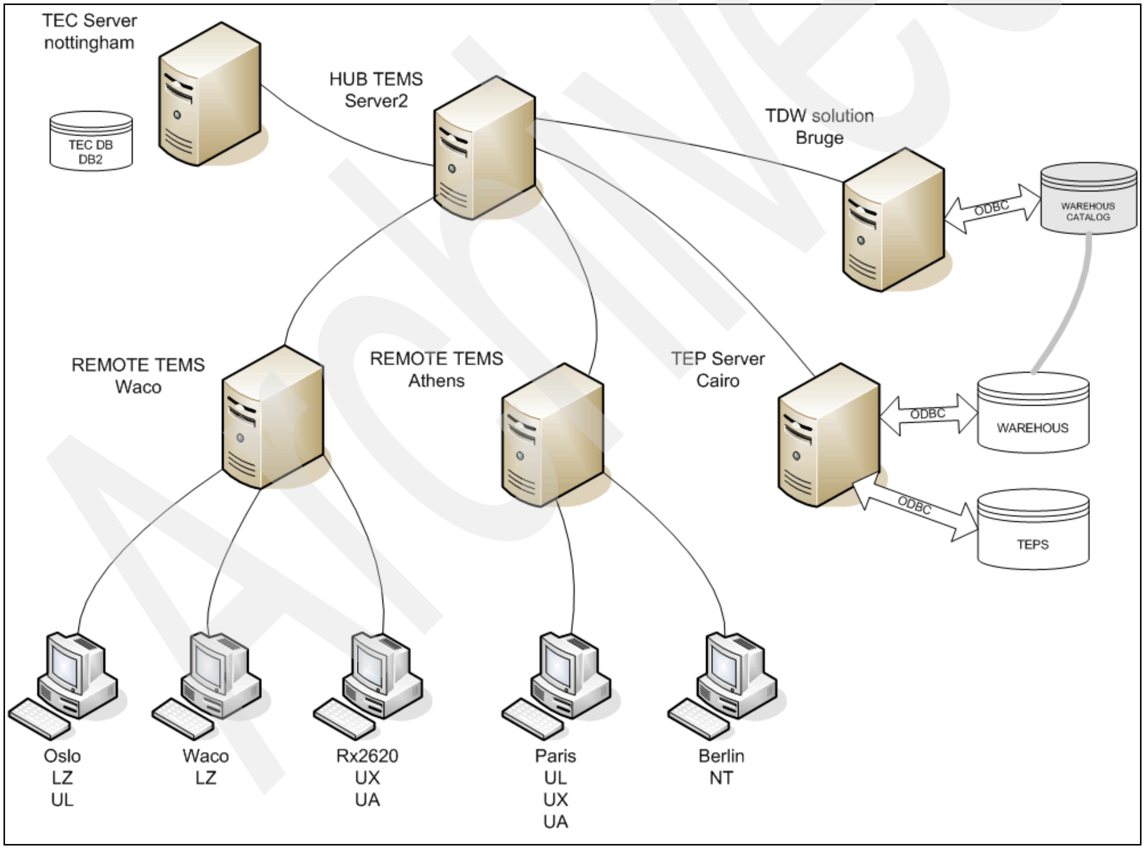


Figure 5-1 Tivoli Enterprise Console integration

5.1.1 Installing Event Synchronization on event server

The installer for the Event Synchronization component is located in the /tec directory of the IBM Tivoli Monitoring V6.2.0 Tools DVD.

There are three methods for installing the component:

- Installing from a wizard
- Installing from the command line
- Installing from the command line using a silent install

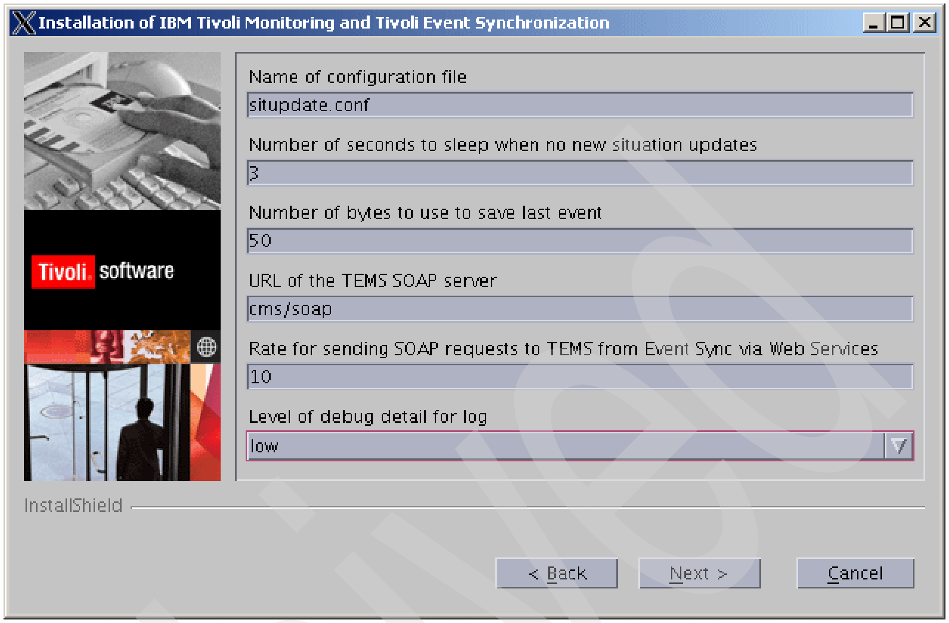
In our test example, we used the Installation wizard as follows:

1. Log on to the host of the event server in an X Window System session, and launch the Event Synchronization installer from the IBM Tivoli Monitoring V6.2.0 Tools DVD media.
2. Change to the \tec subdirectory of the IBM Tivoli Monitoring V6.2.0 Tools DVD and run the following command:

   ```
   ESync2000Aix.bin
   ```

3. Click **Next** on the Welcome window.
4. Select **I accept the terms in the license agreement** and click **Next**.

5. Complete the fields in Figure 5-2and click **Next**.


Installation of IBM Tivoli Monitoring and Tivoli Event Synchronization
Tivoli. software
InstallShield
< Back
Next >
Cancel

Name of configuration file
situpdate.conf

Number of seconds to sleep when no new situation updates
3

Number of bytes to use to save last event
50

URL of the TEMS SOAP server
cms/soap

Rate for sending SOAP requests to TEMS from Event Sync via Web Services
10

Level of debug detail for log
low

Figure 5-2 Tivoli Event Synchronization installation

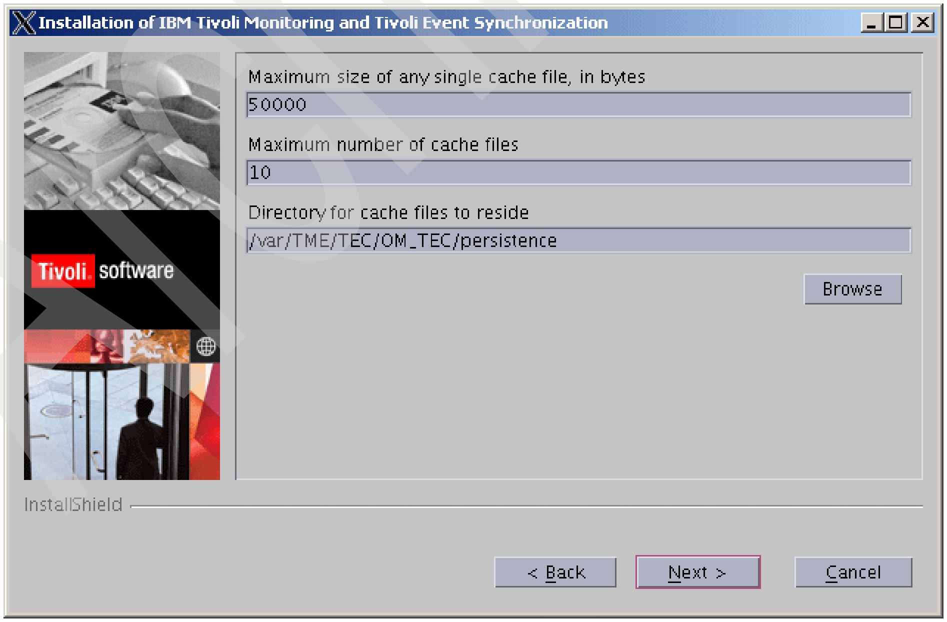
Use Table 5-1 as a reference.

Table 5-1 The IBM Tivoli Enterprise Console Event Synchronization configuration fields

Field	**Description**
Name of configuration file	The name of the file where the Event Synchronization configuration information is stored. The default name is situpdate.conf.
Number of seconds to sleep when no new situation updates	The polling interval in seconds. The minimum value is 1, while the default value is 3. If there are no situation events, the Situation Update Forwarder rests for three seconds.
Number of bytes to use to save last event.	Number of bytes that the long running process will use when it saves the location of the last event it processes. This value must be an integer. The minimum (and default) is 50.

Field	Description
URL of the CMS SOAP Server	The URL for the SOAP Server configured on the computer where the monitoring server is running. The default value is cms/soap. This value is used to create the URL to which IBM Tivoli Enterprise Console sends event information. For example, `http://`*`hostname`*`:`*`port`*`///cms/soap`, where hostname is the host name of the monitoring server and port is the port.
Rate for sending SOAP requests to CMS from Tivoli Enterprise Console via Web Services	The maximum number of event updates sent to the monitoring server at one time. The minimum (and default) value is 10 events.
Level of debug detail for log	The level of information for Event Synchronization that will be logged. You have the following choices: ▸ Low (default) ▸ Medium ▸ Verbose

6. Complete the information about the files where events will be written (Figure 5-3) and click **Next**.



Installation of IBM Tivoli Monitoring and Tivoli Event Synchronization

Maximum size of any single cache file, in bytes

50000

Maximum number of cache files

10

Directory for cache files to reside

/var/TME/TEC/OM_TEC/persistence

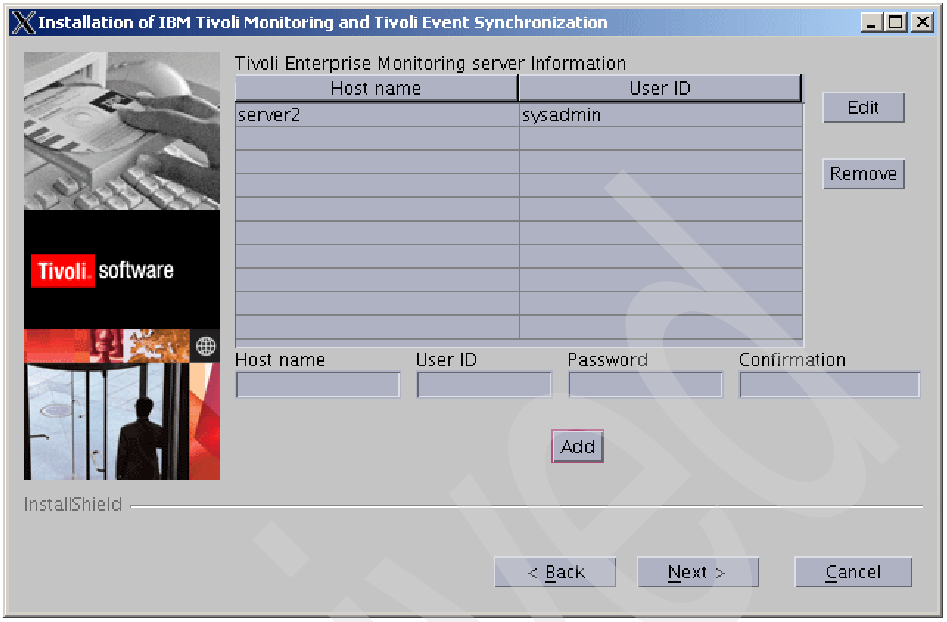
Figure 5-3 Tivoli Event Synchronization installation

Use Table 5-2 as a reference.

Table 5-2 The IBM Tivoli Enterprise Console Event Synchronization configuration fields

Field	**Description**
Maximum size of any single cache file, in bytes	The maximum permitted size, in bytes, for any one event cache file. The minimum (and default) value is 50000. Do not use commas when specifying this value (specify 50000 instead of 50,000).
Maximum number of caches files	The maximum number of event caches files at any given time. The minimum value is 2, while the default value is 10. When this value is reached, the oldest file is deleted to make room for a new file.
Directory for cache files to 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. Use the information from Figure 5-4 on page 315 for each monitoring server with which you want to synchronize events and click **Add**. You must specify information for at least one monitoring server.


Installation of IBM Tivoli Monitoring and Tivoli Event Synchronization
Tivoli software
Edit
Remove
Add
InstallShield
< Back
Next >
Cancel

Tivoli Enterprise Monitoring server Information

Host name	User ID
server2	sysadmin

Host name:
User ID:
Password:
Confirmation:

Figure 5-4 Tivoli Monitoring Server Information

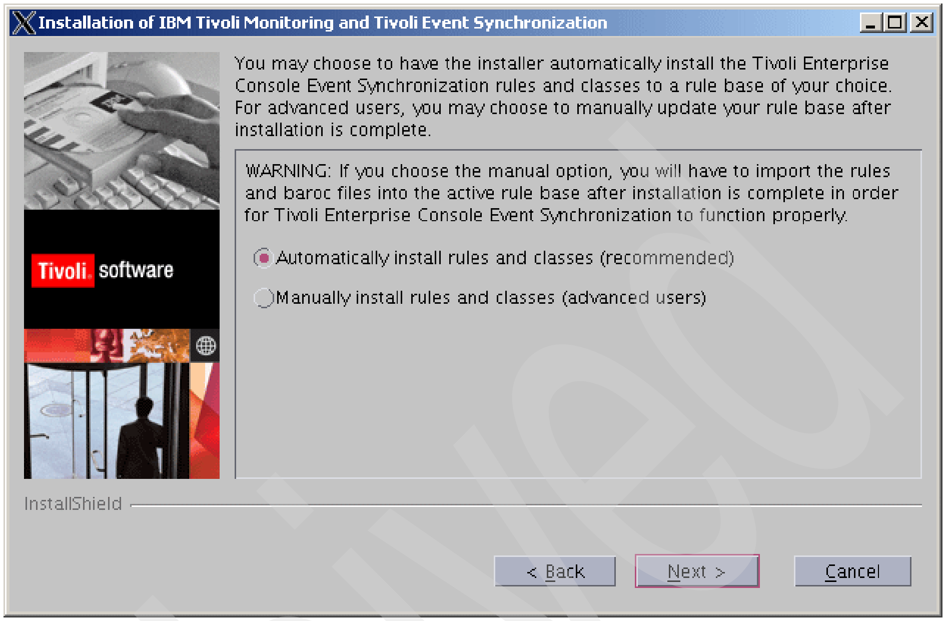
Use Table 5-3 as a reference.

Table 5-3 Tivoli Monitoring Server Information

Field	**Description**
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 again.

8. When you have provided information about all of the monitoring servers, click **Next**.

9. Select **Automatically install rules** and classes and click **Next** (Figure 5-5).



Installation of IBM Tivoli Monitoring and Tivoli Event Synchronization

You may choose to have the installer automatically install the Tivoli Enterprise Console Event Synchronization rules and classes to a rule base of your choice. For advanced users, you may choose to manually update your rule base after installation is complete.

WARNING: If you choose the manual option, you will have to import the rules and baroc files into the active rule base after installation is complete in order for Tivoli Enterprise Console Event Synchronization to function properly.

● Automatically install rules and classes (recommended)

○ Manually install rules and classes (advanced users)

Figure 5-5 Rules and classes configuration

10. Specify **Use Existing rule base (path is optional)** and input the Rule base name and rule base path. Click **Next**.
11. Input the name for backing up the rule base before updating it, and specify both the backup rule base name and backup rule base path. If you leave these fields blank, no backup is made. Click **Next** to proceed to the pre-installation summary window.
12. When the installation and configuration steps are finished, a message telling you to stop and restart the event server is displayed. If you want the installer to restart the event server for you, check the box. If you want to restart the event server yourself, leave the box unchecked.
13. Click **OK**.
14. Click **Finish** in the Summary Information window.

Perform the following tasks after the installation is finished:

- Stop and restart the event server for the configuration changes to take effect.
- Install the monitoring agent .baroc files on the event server, as described in 5.1.2, “Installing monitoring agent .baroc files on the event server” on page 317.

- Configure the monitoring server to forward events to the event server, as described in 5.1.3, “Configuring your monitoring server to forward events” on page 318.

5.1.2 Installing monitoring agent .baroc files on the event server

The monitoring server generates Tivoli Enterprise Console events with classes that are unique to each monitoring agent. Each monitoring agent provides a .baroc file with the Tivoli Enterprise Console classes that are generated by IBM Tivoli Monitoring V6.2. In order to view this event data in the event console, you must install these monitoring agent .baroc files on the event server.

After you have added application support for each agent to the monitoring server, the monitoring agent .baroc files are located in the following directory:

- On Windows, in the *<itm_installdir>*\cms\TECLIB directory, where <itm_installdir> is the directory where you installed IBM Tivoli Monitoring V6.2.
- On Linux and UNIX, in the *<itm_installdir>*/tables/*<ms_name>*/TECLIB directory, where <itm_installdir> is the directory where you installed IBM Tivoli Monitoring V6.2 and <ms_name> is the name of the monitoring server.

Use the following steps to install the monitoring agent .baroc files on the event server:

1. Copy the monitoring agent .baroc files from the computer where the monitoring server is installed to a temporary directory on the event server computer (for example, /tmp). The location of the agent .baroc files is described above. *Do not* copy the om_tec.baroc file; this file contains classes that are duplicates of classes in the omegamon.baroc file.
2. Set up the Tivoli Management Framework environment by running the following command:
   - On Windows:

     ```
     C:\WINDOWS\system32\drivers\etc\Tivoli\setup_env.cmd
     ```

   - On Linux and UNIX, run the following command from a shell environment:

     ```
     . /etc/Tivoli/setup_env.sh
     ```

3. For each monitoring agent .baroc file to load into the rule base, run the following command from the same command prompt:

   ```
   wrb -imprbclass /tmp/<agent_baroc_file> <rb_name>
   ```

where:

- /tmp/<agent_baroc_file> specifies the location and name of the monitoring agent .baroc file. The example above uses the /tmp directory as the location.
- <rb_name> is the name of the rule base that you are using for Event Synchronization.

4. Compile and load the rule base by running the following commands:

```
wrb -comprules <rb_name>
wrb -loadrb <rb_name>
```

5. Stop and restart the event server by running the following commands:

```
wstopesvr
wstartesvr
```

When you have loaded each of the agent .baroc files into the rule base and restarted the event server, the event server is ready to receive and correctly parse any events it receives from the monitoring server from one of the installed monitoring agents.

5.1.3 Configuring your monitoring server to forward events

Before the monitoring server forwards any situation events to Tivoli Enterprise Console, you have to enable the forwarding of events.

Configuring Windows monitoring servers

Use the following steps to enable event forwarding on your monitoring server:

1. Select **Start** → **Programs** → **IBM Tivoli Monitoring** → **Manage Tivoli Monitoring Services**. The Manage Tivoli Enterprise Monitoring Services window is displayed.
2. Right-click the monitoring server and click **Reconfigure**.
3. In the configuration options window, select **Tivoli Event Integration Facility**.
4. Click **OK** and **OK**.
5. Complete the fields as described in Table 5-4 on page 319.

Table 5-4 Tivoli Monitoring Server Information

Field	Description
Server or EIF Probe Location	Type the host name or IP address for the computer where the IBM Tivoli Enterprise Console event server is installed.
Port Number	Type the port number for the event server. If the event server is using port mapping, set this value to 0. If the event server was configured to use a specific port number, specify that number.

6. Click **OK**.

Configuring UNIX monitoring servers

If you installed the monitoring server using the configuration instructions in this chapter, you probably have already configured the TEC Server and TEC Port information for the UNIX monitoring server during installation. However, if you did not configure this information, see “Hub monitoring server configuration on a Linux or UNIX server” on page 74. Example 5-1 describes the TEC Server configuration.

Example 5-1 TEC Server configuration

```
[root@server2][/opt/IBM/ITM/bin]-> ./itmcmd config -S -t HUB_TEMS
Configuring TEMS...

Hub or Remote [1=*LOCAL, 2=*REMOTE] (Default is: 1):
TEMS Host Name (Default is: server2):

Network Protocol 1 [ip, sna, ip.pipe or ip.spipe] (Default is:
ip.pipe):
Now choose the next protocol number from one of these:
     - ip
     - sna
     - ip.spipe
     - 0 for none
Network Protocol 2 (Default is: ip):
Now choose the next protocol number from one of these:
     - sna
     - ip.spipe
     - 0 for none
Network Protocol 3(Default is: ip.spipe):
IP Port Number (Default is: 1918):
IP.PIPE Port Number (Default is: 1918):
```

```
Enter name of KDC_PARTITION (Default is: null):
Enter path and name of KDC_PARTITIONFILE (Default is:
/opt/IBM/ITM/tables/HUB_TE
MS/partition.txt):
IP.SPIPE Port Number (Default is: 3660):
Configuration Auditing? [1=YES, 2=NO] (Default is: 1):
Hot Standby TEMS Host Name or type 0 for "none" (Default is: 0):
Enter Optional Primary Network Name or type 0 for "none" :(Default is:
0):
Security: Validate User ? [1=YES, 2=NO] (Default is: 1):
LDAP Security: Validate User with LDAP ? [1=YES, 2=NO](Default is: 2):

Tivoli Event Integration Facility? [1=YES, 2=NO] (Default is: 2): 1
EIF Server?(Default is: none): nottingham
EIF Port? (Default is: 5529):
Disable Workflow Policy/Tivoli Emitter Agent Event Forwarding? [1=YES,
2=NO] (De
fault is: 2):
 ... Writing to database file for ms.

Hubs
##      CMS_Name
1       ip.pipe:HUB_TEMS[1918]

1)Add, 2)Remove ##, 3)Modify Hub ##, 4)UserAccess ##, 5)Cancel,
6)Save/exit: 6
... creating config file
"/opt/IBM/ITM/config/server2_ms_HUB_TEMS.config"
... creating file "/opt/IBM/ITM/tables/HUB_TEMS/glb_site.txt."
... updating "/opt/IBM/ITM/config/kbbenv"
... verifying Hot Standby.
Info - Checking TEMS User Authentication requirements.
Info - OK, TEMS User Authentication requirements complete.
TEMS configuration completed...
```

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

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

5.2 Event integration with Netcool/OMNIbus

If you are already using Netcool/OMNIbus to monitor events from other sources in your enterprise, you can also view and manage situation events from a Tivoli Enterprise Monitoring Server in the Netcool/OMNIbus console. Event integration requires Netcool/OMNIbus V7.x and Netcool/OMNIbus V7.x probe for Tivoli EIF.

Setting up event integration for Netcool/OMNIbus involves three steps:

- Event Synchronization installation
- Configuring OMNIbus Server
- Tivoli Event Integration Facility (EIF) Interface

Before you begin setting up event integration, refer to 2.2.2, “Required software for event integration with Netcool/OMNIbus” on page 30.

5.2.1 Installing Event Synchronization

You install Event Synchronization on the host of the Netcool/OMNIbus ObjectServer using the IBM Tivoli Monitoring V6.2.0 Tools DVD or DVD image. Installing Event Synchronization installs a new process, Situation Update Forwarder, and its supporting binary and configuration files. This process is used to forward updates to the situation events back to the monitoring server. On Windows, a Situation Update Forwarder service is also created.

There are three methods for installing the component:

- Installing from a wizard
- Installing from the command line
- Installing from the command line using a silent install

In our test environment, the EIF probe and Netcool/OMNIbus are installed on a machine running the Red Hat V4.0 operating system. The Event Synchronization component will be installed on the same machine.

The installation steps will now be discussed in detail:

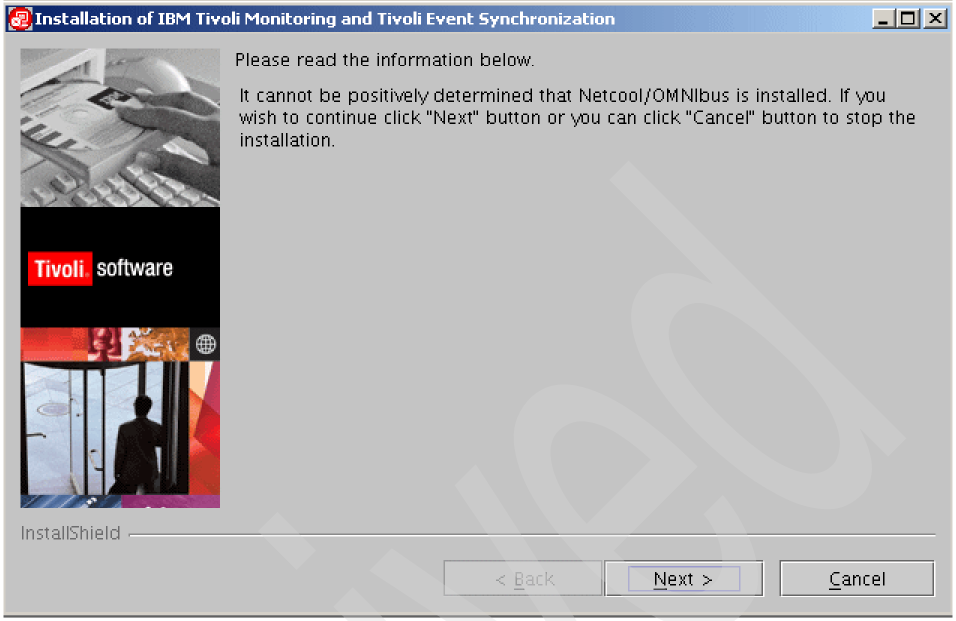
1. On the computer where the ObjectServer is installed, launch the Event Synchronization installation.
2. Change to the tec subdirectory on the IBM Tivoli Monitoring V6.2.0 Tools DVD or DVD image and run the following command to initialize the installation wizard:

   ```
   ESync2000<xxx>.bin
   ```

   where <xxx> indicates the appropriate operating system.

   > **Note:** There are another two ways to install Event Synchronization: from the command line or the command line using a silent install mode.

3. If the installer cannot locate OMNIbus in its usual place, Figure 5-6 on page 323 is displayed. Click **Next** to continue the installation process.



Installation of IBM Tivoli Monitoring and Tivoli Event Synchronization
Tivoli. software
InstallShield
< Back
Next >
Cancel

Please read the information below.

It cannot be positively determined that Netcool/OMNIbus is installed. If you wish to continue click "Next" button or you can click "Cancel" button to stop the installation.

Figure 5-6 Installation of Netcool/OMNIbus not determined

4. Click **Next** on the Welcome window.
5. Review the license agreement, select **I accept the terms in the license agreement**, and click **Next**.
6. Click **Next** to install the synchronization component in the default location, or use the **Browse** button to select another location and then click **Next** to continue.
7. Complete the configuration fields, using Table 5-1 on page 312 as a reference.
8. Click **Next**.
9. Complete the information about the files where events will be written using Table 5-2 on page 314 as a reference.
10. Click **Next**.
11. Type the information from Table 5-3 on page 315 for each hub monitoring server with which you want to synchronize events and click **Add**. You must specify information for at least one hub monitoring server.
12. Click **Next** to proceed.
13. When the installation is completed, a message is displayed telling you that the installation has been successful. Click **Finish** to exit the wizard.

5.2.2 Configuring the OMNIbus server

In this step, you configure the OMNIbus ObjectServer to receive and map the situation event information forwarded by a monitoring server and to reflect the events to the OMNIbus console. You also configure the OMNIbus server to send Event Synchronization information back to the originating monitoring server and configure the EIF probe to map the situation event attributes to OMNIbus event attributes.

In this section, we will describe the UNIX procedure to customize the integration. For Windows configuration, please see the procedure in the *IBM Tivoli Monitoring Version 6.2.0 Installation and Setup Guide,* GC32-9407.

Configuring OMNIbus server for scripts program execution

To run the Event Synchronization program from SQL automation scripts to send synchronization events to ITM, the OMNIbus server must be running under a process control and the properties *PA.Username* and *PA.Password* must be set in $OMNIHOME/etc/NCOMS.props file, where $OMNIHOME is the system defined variable defining the installation location of OMNIbus.

By default, the process control grants access to the members of the default group ncoadmin. For the default configuration, create a ncoadmin group and add root as a user to this group. The *PA.Username* property must be set to the user name used to connect to the process control agent. On UNIX, the default value is root. The *PA.Password* property must be set to the password for the user connecting to the process control agent. For the default setting, specify the password of the root user.

Updating the OMNIbus db schema

The command to configure OMNIbus pipes the SQL command set into the SQL command-line tool and performs the updates to the ObjectServer.

> **Note:** The original procedure described in a draft of the *IBM Tivoli Monitoring Version 6.2.0 Installation and Setup Guide,* GC32-9407 instructs us to run the **`itm_proc.sql`** before **`itm_db_update.sql`**, but as some tables are required to run the procedure tasks, the correct order is update database, run procedure tasks, and then the synchronization task.

Updating the OMNIbus db schema on UNIX

1. Update the ObjectServer database with the following commands:

```
$OMNIHOME/bin/nco_sql -user <username> -password <password> -server
<server_name> < <path_to_file>/itm_db_update.sql
```

```
$OMNIHOME/bin/nco_sql -user <username> -password <password> -server
<server_name> < <path_to_file>/itm_proc.sql
$OMNIHOME/bin/nco_sql -user <username> -password <password> -server
<server_name> < <path_to_file>/itm_sync.sql
```

where:

- $OMNIHOME is the system defined variable defining the install location of OMNIbus.
- <username> is the OMNIbus Object Server user name.
- <password> is the OMNIbus Object Server password.
- <path_to_file> is the fully qualified path to specified SQL file.

2. Stop the OMNIbus server.

   Issue the following command from command line:

   ```
   $OMNIHOME/bin/nco_pa_stop -process <server_name>
   ```

   where:

   - $OMNIHOME is the system defined variable defining the install location of OMNIbus.
   - <server_name> is the OMNIbus ObjectServer name defined for process control.

3. Start the OMNIbus server.

   Issue the following command from the command line:

   ```
   $OMNIHOME/bin/nco_pa_start -process <server_name>
   ```

   where

   - $OMNIHOME is the system defined variable defining the install location of OMNIbus.
   - <server_name> is the OMNIbus ObjectServer name defined for process control.

Updating the OMNIbus db schema on Windows

1. Update the ObjectServer database with the following commands:

   ```
   %OMNIHOME%\..\bin\redist\isql -U <username> -P <password> -S
   <server_name> <path_to_file>\itm_db_update.sql
   %OMNIHOME%\..\bin\redist\isql -U <username> -P <password> -S
   <server_name> <path_to_file>\itm_proc.sql
   %OMNIHOME%\..\bin\redist\isql -U <username> -P <password> -S
   <server_name> <path_to_file>\itm_sync.sql
   ```

where:

- %OMNIHOME% is the system defined variable defining the install location of OMNIbus.
- <username> is the OMNIbus Object Server user name.
- <password> is the OMNIbus Object Server password.
- <path_to_file> is the fully qualified path to the specified SQL file.

2. Stop the OMNIbus server by running **Start** → **Settings** → **Control Panel open Administrative Tools**, and then select **Services**. In the list of services, double-click **OMNIbus server**, and then click **Stop**.
3. Start the OMNIbus server. In OMNIbus services properties, click **Start**.

Configuring the Tivoli EIF Probe

This step configures the probe with the rules for mapping situation events to OMNIbus events. Configuring the mapping involves updating the tivoli_eif.rules file installed with the probe with the contents of the tivoli_eif.rules file shipped with the synchronization component. You must resynchronize the probe after you update the file.

> **Note:** Be careful with this procedure. If you have previous customization, the contents of this rules (tivoli_eif.rules) should be adapted to your rules.

Configure the EIF probe on UNIX

1. Copy the contents of <event_sync_install_dir>/OMNIbus/tivoli_eif.rules to the following file:

   $OMNIHOME/probes/<os_dir>/tivoli_eif.rules

   where:

   - $OMNIHOME is a system defined variable defining the install location of OMNIbus.
   - <os_dir> is the operating system, such as Windows or AIX.

2. Stop the EIF probe by running:

   ```
   $OMNIHOME/bin/nco_pa_stop -process <probe_name>
   ```

   where:

   - $OMNIHOME is the system defined variable defining the install location of OMNIbus.
   - <probe_name> is the OMNIbus EIF probe name defined for process control.

3. Start the EIF probe by running:

   ```
   $OMNIHOME/bin/nco_pa_start -process <probe_name>
   ```

   where:

   – $OMNIHOME is the system defined variable defining the install location of OMNIbus.

   – <probe_name> is the OMNIbus EIF probe name defined for process control.

Configure the EIF probe on Windows

Do the following steps to update the rules file:

1. Copy the contents of <event_sync_install_dir>\OMNIbus\tivoli_eif.rules to the following file:

   %OMNIHOME%\probes\<os_dir>\tivoli_eif.rules

   where:

   – %OMNIHOME% is a system defined variable defining the install location of OMNIbus.

   – <os_dir> is the operating system, such as Windows or AIX.

2. Stop the EIF probe by selecting **Start** → **Settings** → **Control Panel open Administrative Tools**, and then click **Services**. In the list of services, double-click **EIF probe**, and then click **Stop**.
3. Start the EIF probe.In EIF probe services properties, click **Start**.

5.2.3 Configuring the monitor server

Before the monitoring server forwards any situation events to Tivoli Enterprise Console, you have to enable forwarding of events.

Configuring a Windows monitoring server

Use the following steps to enable event forwarding on your monitoring server:

1. Select **Start** → **Programs** → **IBM Tivoli Monitoring** → **Manage Tivoli Monitoring Services**. The Manage Tivoli Enterprise Monitoring Services window is displayed.
2. Right-click the monitoring server and click **Reconfigure**.
3. In the configuration options window, select **Tivoli Event Integration Facility**.
4. Click **OK** and **OK**.

5. Complete the fields as described in Table 5-5.

Table 5-5 Tivoli Monitoring Server Information

Field	Description
Server or EIF Probe Location	Type the host name or IP address for the computer where the EIF probe is installed.
Port Number	Type the port number on which the probe is listening.

6. Click **OK**.

Configuring UNIX monitoring servers

You configured the EIF probe and port information for the UNIX monitoring server during installation if you installed the monitoring server using the configuration instructions in this book. However, if you did not configure this information, refer to "Hub monitoring server configuration on a Linux or UNIX server" on page 74.

Example 5-2 describes an EIF configuration.

Example 5-2 EIF configuration

```
[root@server2][/opt/IBM/ITM/bin]-> ./itmcmd config -S -t HUB_TEMS
Configuring TEMS...

Hub or Remote [1=*LOCAL, 2=*REMOTE] (Default is: 1):
TEMS Host Name (Default is: server2):

Network Protocol 1 [ip, sna, ip.pipe or ip.spipe] (Default is:
ip.pipe):
   Now choose the next protocol number from one of these:
     - ip
     - sna
     - ip.spipe
     - 0 for none
Network Protocol 2 (Default is: ip):
   Now choose the next protocol number from one of these:
     - sna
     - ip.spipe
     - 0 for none
Network Protocol 3(Default is: ip.spipe):
IP Port Number (Default is: 1918):
IP.PIPE Port Number (Default is: 1918):
Enter name of KDC_PARTITION (Default is: null):
```

```
Enter path and name of KDC_PARTITIONFILE (Default is:
/opt/IBM/ITM/tables/HUB_TEMS/partition.txt):
IP.SPIPE Port Number (Default is: 3660):

Configuration Auditing? [1=YES, 2=NO] (Default is: 1):
Hot Standby TEMS Host Name or type 0 for "none" (Default is: 0):
Enter Optional Primary Network Name or type 0 for "none" :(Default is:
0):
Security: Validate User ? [1=YES, 2=NO] (Default is: 1):
LDAP Security: Validate User with LDAP ? [1=YES, 2=NO](Default is: 2):

Tivoli Event Integration Facility? [1=YES, 2=NO] (Default is: 2): 1
EIF Server?(Default is: none): weimar
EIF Port? (Default is: 5529): 9999
Disable Workflow Policy/Tivoli Emitter Agent Event Forwarding? [1=YES,
2=NO] (Default is: 2):
 ... Writing to database file for ms.

Hubs
##      CMS_Name
1       ip.pipe:HUB_TEMS[1918]

1)Add, 2)Remove ##, 3)Modify Hub ##, 4)UserAccess ##, 5)Cancel,
6)Save/exit: 6
... creating config file
"/opt/IBM/ITM/config/server2_ms_HUB_TEMS.config"
... creating file "/opt/IBM/ITM/tables/HUB_TEMS/glb_site.txt."
... updating "/opt/IBM/ITM/config/kbbenv"
... verifying Hot Standby.
Info - Checking TEMS User Authentication requirements.
Info - OK, TEMS User Authentication requirements complete.
TEMS configuration
completed...
```

5.2.4 Customizing the OMNIbus configuration

The procedure get_config_parms in the <event_sync_install_dir>/OMNIbus/itm_proc.sql file defines three configuration parameters:

```
set sit_ack_expired_def_action = 'REJECT'
set sit_resurface_def_action = 'ACCEPT'
set situpdate_conf_file = 'situpdate.conf'
```

The variable *sit_ack_expired_def_action* defines the action to be taken for an event by the OMNIbus server when acknowledgement expiration information is received for an event from a monitoring server. The default action is to Reject the request. OMNIbus sends information to change the state of the event to Acknowledge back to the monitoring server. If you would like to change the action taken by the OMNIbus server to Accept the acknowledgement expiration, modify the statement to `set sit_ack_expired_def_action = 'ACCEPT'`.

The variable *sit_resurface_def_action* defines the action to be taken by the OMNIbus server when a situation event has resurfaced. The default action of the OMNIbus server is to Accept this request and Deacknowledge the event. If you would like to change the action taken by OMNIbus server to Reject the resurface of the event, modify the statement to `set sit_resurface_def_action = 'REJECT'`. OMNIbus then sends information back to the monitoring server to change the state of the event back to Acknowledge.

The variable *situpdate_conf_file* specifies the name of the configuration file to be used by the SitUpdate Forwarder. If you would like to change the name of the configuration file, modify the statement to `set situpdate_conf_file = 'newname.conf'`.

After modifying **itm_proc.sql**, issue the following command:

- For UNIX:

  ```
  $OMNIHOME/bin/nco_sql -user <username> -password <password> -server
  <server_name> < <path_to_file>/itm_proc.sql
  ```

  where:

  – $OMNIHOME is the system defined variable defining the install location of OMNIbus.

  – <username> is the OMNIbus Object Server user name.

  – <password> is the OMNIbus Object Server password.

  – <path_to_file> is the fully qualified path to specified SQL file.

- For Windows:

  ```
  %OMNIHOME%\..\bin\redist\isql -U <username> -P <password> -S
  <server_name> <path_to_file>\itm_proc.sql
  ```

  where:

  %OMNIHOME% is the system defined variable defining the install location of OMNIbus.

  <username> is the OMNIbus Object Server user name.

  <password> is the OMNIbus Object Server password.

<path_to_file> is the fully qualified path to specified SQL file.

5.3 Starting and stopping the situation update forwarder

To send event updates to a monitoring server, you must start the Situation Update Forwarder. This process is started automatically when the event server starts. To start the process manually, change to the <install_esynch>/bin directory and run the following command:

- On Windows:

  ```
  startSUF.cmd
  ```

- On UNIX:

  ```
  startSUF.sh
  ```

To stop the process, run the following command:

- On Windows:

  ```
  stopSUF.cmd
  ```

- On UNIX:

  ```
  stopSUF.sh
  ```

On Windows, you can also start and stop the Tivoli Situation Update Forwarder service to start or stop the forwarding of event updates. You can start and stop this service either by selecting **Windows Administrative Tools** → **Services** or by running the following commands:

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

5.4 Configuring connectors for the common event console

The *common event console* is a Tivoli Enterprise Portal view that provides a single, integrated display of events from multiple event systems. In one table, the common event console presents events from the event systems, and users can sort, filter, and perform actions on these events. The following event systems are supported:

- IBM Tivoli Monitoring V6.2
- IBM Tivoli Enterprise Console
- IBM Tivoli Netcool/OMNIbus

A *common event connector* (frequently called a connector) is software that enables the integrated display of events from multiple event systems in the common event console. A connector retrieves event data from an event system and sends user-initiated actions to be run in that event system. For example, if you perform an action on a Tivoli Enterprise Console or Netcool/OMNIbus event in the common event console, the associated common event console connector sends that action to the originating event system (Tivoli Enterprise Console or Netcool/OMNIbus) for execution. To have the events from a specific event system displayed in the common event console, you must configure a connector for that event system.

5.4.1 Common Event Console Configuration window

Use the Common Event Console Configuration window to configure a common event console connector for each of your event system instances. Because the connector for the IBM Tivoli Monitoring V6.2 product is preconfigured when you install the product, the common event console includes the IBM Tivoli Monitoring V6.2 events by default. However, to have IBM Tivoli Enterprise Console or IBM Tivoli Netcool/OMNIbus events included in the common event console, you must configure a connector for each of these event systems after you install the IBM Tivoli Monitoring V6.2 product. This configuration includes specifying which Tivoli Enterprise Console and Netcool/OMNIbus event systems are used to obtain events for display in the common event console. You might also want to change some of the configuration values for the IBM Tivoli Monitoring V6.2 connector.

To configure connectors, open the Common Event Console Configuration window by performing the following steps according to your operating system.

When you reconfigure/configure the portal server stops, the Common Event Console Configuration window opens after a moment, and it has the following four tabs:

- ITM Connector
- TEC Connector
- OMNIbus Connector
- Names of Extra Columns

Opening CEC Console configuration on Windows

Perform the following steps to open the CEC Console configuration on Windows:

1. Select **Start** → **Programs** → **IBM Tivoli Monitoring** → **Manage Tivoli Monitoring Services**. The Manage Tivoli Enterprise Monitoring Services window is displayed.

2. Right-click the **Tivoli Enterprise Portal Server**.
3. In the menu, click **Reconfigure.**
4. In the first TEP Server Configuration window, click **OK**.
5. In the second TEP Server Configuration window, click **OK**.
6. Click **No** in answer to the question “Do you want to reconfigure the warehouse connection information for the Tivoli Enterprise Portal Server?”

Opening a CEC Console configuration on AIX or Linux

1. Open the Manage Tivoli Enterprise Monitoring Services window. Change the directory to install_dir/bin and enter `./itmcmd manage`.
2. In the Manage Tivoli Enterprise Monitoring Services window, click **Tivoli Enterprise Portal Server**.
3. In the Manage Tivoli Enterprise Monitoring Services window, right-click **Tivoli Enterprise Portal Server**.
4. In the pop-up window, click **Configure**.

ITM Connector

Click the **ITM Connector** tab to view or change the information for the IBM Tivoli Monitoring V6.2 connector. Because you have only the hub Tivoli Enterprise Monitoring Server in the Tivoli Monitoring event system, you configure only one IBM Tivoli Monitoring V6.2 connector. Table 5-6 defines the IBM Tivoli Monitoring V6.2 connector.

Table 5-6 IBM Tivoli Monitoring connector tab

Field	Description
Enable this connector	You can choose Yes or No. A value of Yes means that IBM Tivoli Monitoring events are available in the common event console.
Connector name	The name that is to be displayed in the common event console for this connector.
Maximum number of events for this connector	The maximum number of events that are to be available in the common event console for this connector.
View closed events	You can choose Yes or No. A value of Yes means that closed events for this connector are available in the common event console.

TEC Connector

Click the **TEC Connector** tab to view or change the information for an IBM Tivoli Enterprise Console connector. To have the events from a Tivoli Enterprise Console server displayed in the common event console, you must configure an IBM Tivoli Enterprise Console connector. To configure a connector, click **New**. Table 5-7 defines the TEC connector.

Table 5-7 TEC Connector tab

Field	**Description**
Connector name	The name that is to be displayed in the common event console for this connector.
Maximum number of events for this connector	The maximum number of events that will be available in the common event console for this connector.
Computer name of event system	The computer name of the event system that is associated with this connector.
Port number of event system	The object dispatcher (oserv) port number (usually 94), which this connector uses to retrieve events from the Tivoli Enterprise Console event system.
User name for accessing event system	The user name that is used when accessing the event system that is associated with this connector.
Password	The password that is associated with the user name.
Event group that defines events for common event console	The Tivoli Enterprise Console event group that defines which events are available in the common event console. If you do not specify an event group, all Tivoli Enterprise Console events are available in the common event console. If you want to restrict events further, you can also define a clause in the SQL WHERE clause that restricts events for the common event console field.
SQL WHERE clause that restricts events for common event console	This clause can be applied only to the part of an event that is built from the Tivoli Enterprise Console base attribute table. For example, status <> 30 causes all events with a status that is not equal to 30 to be available in the common event console. If you do not define a clause, all Tivoli Enterprise Console events are available in the common event console, unless they are excluded by an event group that you specified in the Event group that defines events for the common event console field.
View closed events	You can choose Yes or No. A value of Yes means that closed events for this connector are available in the common event console.

Field	Description
Time interval (in minutes) for polling event system	The number of minutes between each poll of the event system for new or changed events.
Time interval (in minutes) for synchronizing events	The number of minutes between each poll of the event system to determine which events have been deleted.
Time interval (in seconds) between reconnection attempts	The number of seconds of delay between reconnection attempts when the connector loses its connection to the event system.
Number of reconnection attempts	The maximum number of consecutive reconnection attempts to make if the connector loses its connection to the event system. If this value is set to -1 and the connector loses its connection, the connector attempts to reconnect indefinitely.
Information for extra table columns	The common event console includes five extra table columns that you can customize. In the remaining fields on this TEC Connector page, you can define the Tivoli Enterprise Console attribute type and attribute name that identify the attribute that is to be mapped to each of these customized columns.

For the attribute type, you can choose one of the following values:

- Base, which means that the attribute is from the Tivoli Enterprise Console base attribute table.
- Extended, which means that the attribute is from the Tivoli Enterprise Console extended attribute table.

OMNIbus Connector

Click the **OMNIbus Connector** tab to view or change the information for an IBM Tivoli Netcool/OMNIbus connector. To have the events from a Tivoli Netcool/OMNIbus ObjectServer displayed in the common event console, you must configure an IBM Tivoli Netcool/OMNIbus connector. To configure a connector, click **New**. Table 5-8 defines the OMNIbus Connector fields.

Table 5-8 OMNIbus Connector tab

Field	Description
Connector name	The name that is to be displayed in the common event console for this connector.
Maximum number of events for this connector	The maximum number of events that will be available in the common event console for this connector.

Field	Description
Computer name of event system	The computer name of the event system that is associated with this connector.
Port number of event system	The ObjectServer port number (usually 4100), which this connector uses to retrieve events from the Tivoli Netcool/OMNIbus event system.
User name for accessing event system	The user name that is used when accessing the event system that is associated with this connector.
Password	The password that is associated with the user name.
SQL WHERE clause that restricts events for common event console	This clause can be applied only to the part of an event that is built from the Tivoli Netcool/OMNIbus alerts.status table. For example, Severity <> 0 causes all events with a severity that is not equal to 0 to be available in the common event console. If you do not define a clause, all Tivoli Netcool/OMNIbus events are available in the common event console.
View cleared events	You can choose Yes or No. A value of Yes means that cleared events for this connector are available in the common event console.
Time interval (in minutes) for polling event system	The number of minutes between each poll of the event system for new or changed events. The Tivoli Netcool/OMNIbus ObjectServer automatically sends new or changed events to the common event console as they become available. Therefore, the primary purpose of this checking is to ensure that the server and the connection to the server are functioning properly.
Time interval (in seconds) between reconnection attempts	The number of seconds of delay between reconnection attempts when the connector loses its connection to the event system.
Number of reconnection attempts	The maximum number of consecutive reconnection attempts to make if the connector loses its connection to the event system. If this value is set to 0 and the connector loses its connection, the connector remains inoperable indefinitely. If this value is set to -1 and the connector loses its connection, the connector attempts to reconnect indefinitely.

Field	Description
Information for extra table columns	The common event console includes five extra table columns that you can customize. In the remaining fields on this page, you can define the Tivoli Netcool/OMNIbus field type and field name that identify the field that is to be mapped to each of these customized columns. For the field type, you can choose one of the following values: ► `alerts.status`, which means that the field contains data from the alerts.status table in the Tivoli Netcool/OMNIbus ObjectServer. ► `alerts.details`, which means that the field contains data from the alerts.details table in the Tivoli Netcool/OMNIbus ObjectServer. ► `Extended`, which means that the field contains extended attributes from a Tivoli Enterprise Console event that has been forwarded to the Tivoli Netcool/OMNIbus event system.

Names of extra columns

The common event console displays only a basic set of information from the Tivoli Enterprise Console base attribute table and the Tivoli Netcool/OMNIbus `alerts.status` and `alerts.details` tables. If, for example, you want to see an additional attribute named "origin" from a Tivoli Enterprise Console event, you can perform the following steps:

1. In the Attribute type for extra column 1 field on the TEC Connector page, choose the attribute type, for example, base.
2. In the Attribute name for extra column 1 field on the TEC Connector page, enter the attribute name, for example, origin.
3. In the Name of extra column 1 field on the Names of Extra Columns page, enter the name that you want to use for the column that you have customized. For example, you might enter Origin.

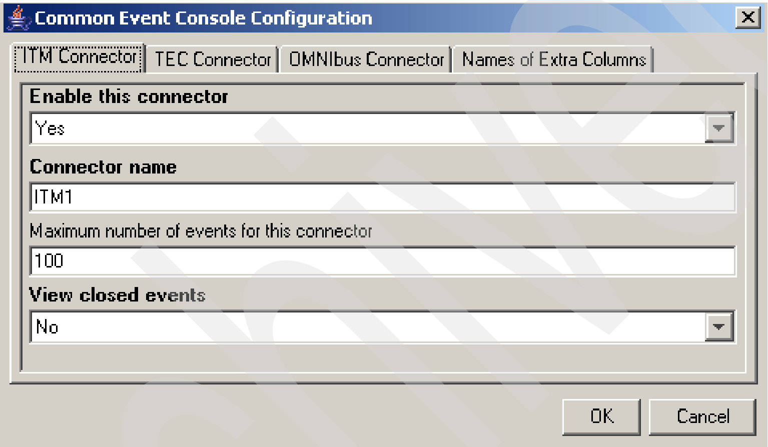
In the "Origin" column for each row that is a Tivoli Enterprise Console event, the common event console displays the value of the origin attribute.

5.5 Integrating the Netcool and OMNIbus events to the Common Event Console example

This section describes an example of IBM Tivoli Monitoring V6.2 event integration.

First, we configure the Common Event Console to concentrate events from IBM Tivoli Monitoring itself, Tivoli Enterprise Console, and Netcool/OMNIbus in the same workspace. To achieve this target, some customization has been made.

TEMS has a default ITM connector configuration, as you can see in Figure 5-7.



Enable this connector: Yes

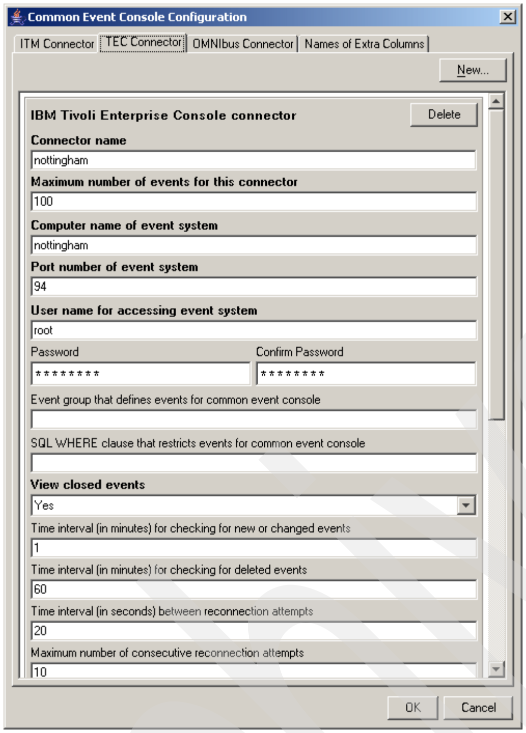
Connector name: ITM1

Maximum number of events for this connector: 100

View closed events: No

Figure 5-7 ITM Connector configuration

To configure TEC Connector, select the respective folder, click **New**, and complete the parameters, as shown in Figure 5-8.



IBM Tivoli Enterprise Console connector

Connector name: nottingham

Maximum number of events for this connector: 100

Computer name of event system: nottingham

Port number of event system: 94

User name for accessing event system: root

Password: ********

Confirm Password: ********

Event group that defines events for common event console:

SQL WHERE clause that restricts events for common event console:

View closed events: Yes

Time interval (in minutes) for checking for new or changed events: 1

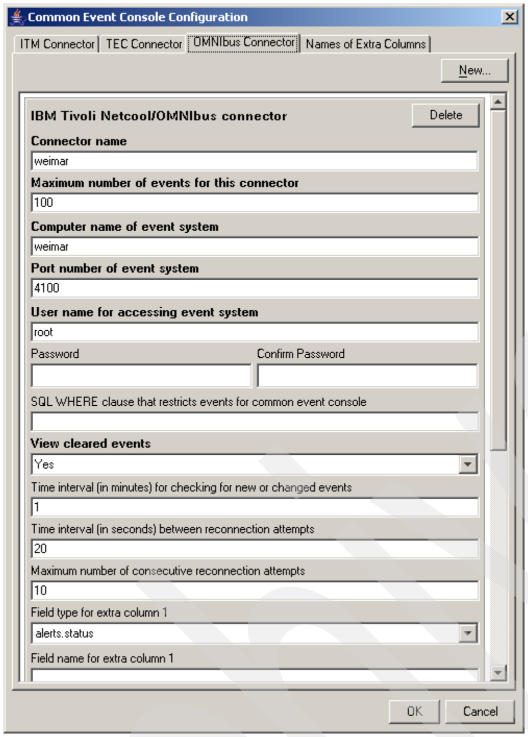
Time interval (in minutes) for checking for deleted events: 60

Time interval (in seconds) between reconnection attempts: 20

Maximum number of consecutive reconnection attempts: 10

Figure 5-8 Tec Connector Tab

To configure the OMNIbus Connector, select the respective folder, click **New**, and complete the parameters, as shown in Figure 5-9.



IBM Tivoli Netcool/OMNIbus connector

Connector name: weimar

Maximum number of events for this connector: 100

Computer name of event system: weimar

Port number of event system: 4100

User name for accessing event system: root

Password:

Confirm Password:

SQL WHERE clause that restricts events for common event console:

View cleared events: Yes

Time interval (in minutes) for checking for new or changed events: 1

Time interval (in seconds) between reconnection attempts: 20

Maximum number of consecutive reconnection attempts: 10

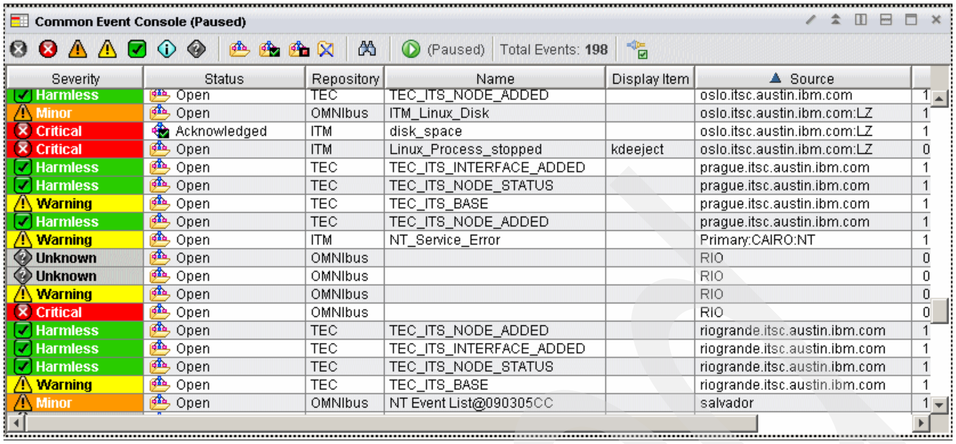
Field type for extra column 1: alerts.status

Field name for extra column 1:

Figure 5-9 OMNIbus connector tab

Note: The other parameters that are not shown above were left with the default values.

In Figure 5-10 on page 341, there is a sample of the Common Enterprise Console with three connectors: ITM, TEC, and Netcool/OMNIbus.



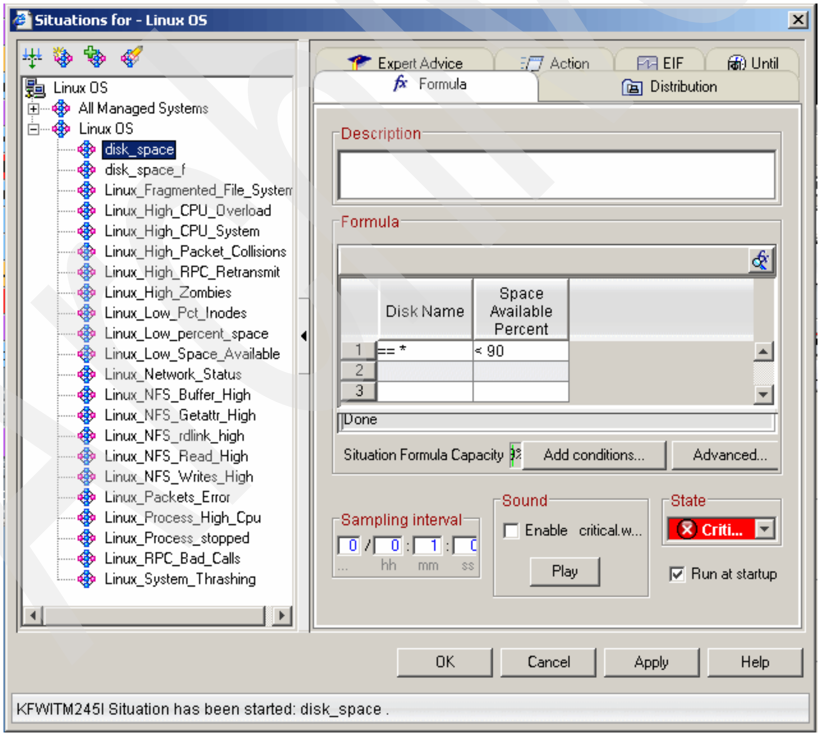
Common Event Console (Paused)

(Paused) Total Events: 198

Severity	Status	Repository	Name	Display Item	Source	
Harmless	Open	TEC	TEC_ITS_NODE_ADDED		oslo.itsc.austin.ibm.com	1
Minor	Open	OMNIbus	ITM_Linux_Disk		oslo.itsc.austin.ibm.com:LZ	1
Critical	Acknowledged	ITM	disk_space		oslo.itsc.austin.ibm.com:LZ	1
Critical	Open	ITM	Linux_Process_stopped	kdeeject	oslo.itsc.austin.ibm.com:LZ	0
Harmless	Open	TEC	TEC_ITS_INTERFACE_ADDED		prague.itsc.austin.ibm.com	1
Harmless	Open	TEC	TEC_ITS_NODE_STATUS		prague.itsc.austin.ibm.com	1
Warning	Open	TEC	TEC_ITS_BASE		prague.itsc.austin.ibm.com	1
Harmless	Open	TEC	TEC_ITS_NODE_ADDED		prague.itsc.austin.ibm.com	1
Warning	Open	ITM	NT_Service_Error		Primary:CAIRO:NT	1
Unknown	Open	OMNIbus			RIO	0
Unknown	Open	OMNIbus			RIO	0
Warning	Open	OMNIbus			RIO	0
Critical	Open	OMNIbus			RIO	0
Harmless	Open	TEC	TEC_ITS_NODE_ADDED		riogrande.itsc.austin.ibm.com	1
Harmless	Open	TEC	TEC_ITS_INTERFACE_ADDED		riogrande.itsc.austin.ibm.com	1
Harmless	Open	TEC	TEC_ITS_NODE_STATUS		riogrande.itsc.austin.ibm.com	1
Warning	Open	TEC	TEC_ITS_BASE		riogrande.itsc.austin.ibm.com	1
Minor	Open	OMNIbus	NT Event List@090305CC		salvador	1

Figure 5-10 Common Event Console

For example, one situation was created to reconfigure disk space when *Space Available Percent* was less than 90. Figure 5-11 shows the basic configuration.



Situations for - Linux OS

- Linux OS
  - All Managed Systems
  - Linux OS
    - disk_space
    - disk_space_f
    - Linux_Fragmented_File_Systen
    - Linux_High_CPU_Overload
    - Linux_High_CPU_System
    - Linux_High_Packet_Collisions
    - Linux_High_RPC_Retransmit
    - Linux_High_Zombies
    - Linux_Low_Pct_Inodes
    - Linux_Low_percent_space
    - Linux_Low_Space_Available
    - Linux_Network_Status
    - Linux_NFS_Buffer_High
    - Linux_NFS_Getattr_High
    - Linux_NFS_rdlink_high
    - Linux_NFS_Read_High
    - Linux_NFS_Writes_High
    - Linux_Packets_Error
    - Linux_Process_High_Cpu
    - Linux_Process_stopped
    - Linux_RPC_Bad_Calls
    - Linux_System_Thrashing

Description

Formula

	Disk Name	Space Available Percent
1	== *	< 90
2		
3		

Done

Situation Formula Capacity

Sampling interval: 0 / 0 : 1 : 0 (... hh mm ss)

Sound: □ Enable critical.w...

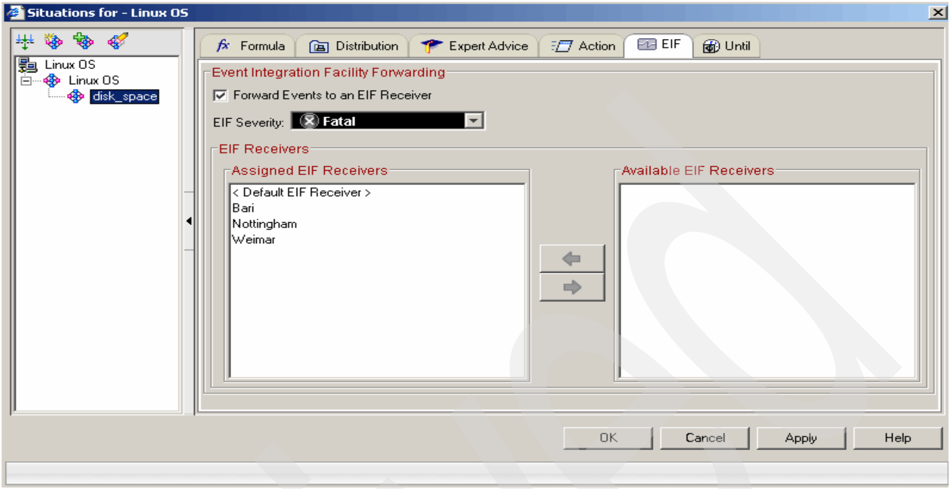
State: Criti...

☑ Run at startup

KFWITM245I Situation has been started: disk_space .

Figure 5-11 Situation configuration

In the situation configuration, click the EIF folder to select the EIF Receiver for the situation alert, as shown in Figure 5-12.



Event Integration Facility Forwarding

☑ Forward Events to an EIF Receiver

EIF Severity: Fatal

EIF Receivers

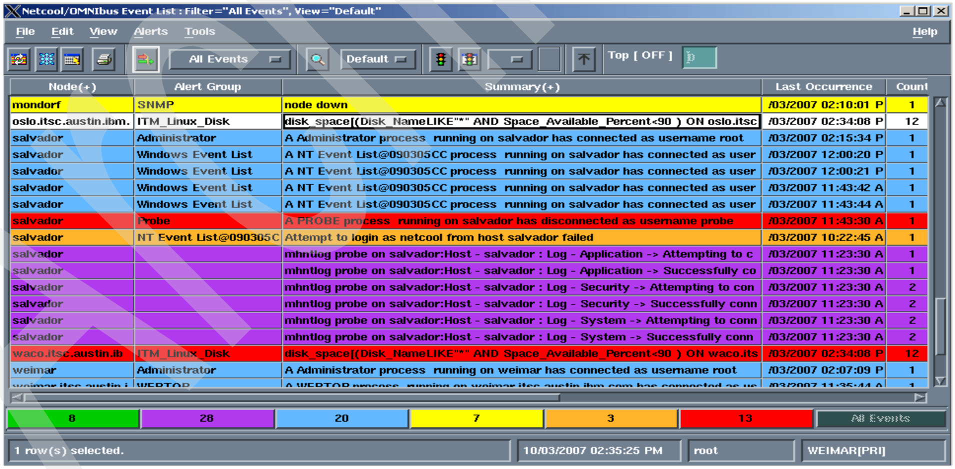
Assigned EIF Receivers

< Default EIF Receiver >
Bari
Nottingham
Weimar

Available EIF Receivers

Figure 5-12 EIF receivers

This example of a situation was used to generate an event to Netcool/OMNIbus. An alert where Alert Group has the value of ITM_Linux_Disk was received by Netcool/OMNIbus. Figure 5-13 shows the native Netcool/OMNIbus console.


Netcool/OMNIbus Event List : Filter="All Events", View="Default"
File
Edit
View
Alerts
Tools
Help
All Events
Default
Top [OFF]

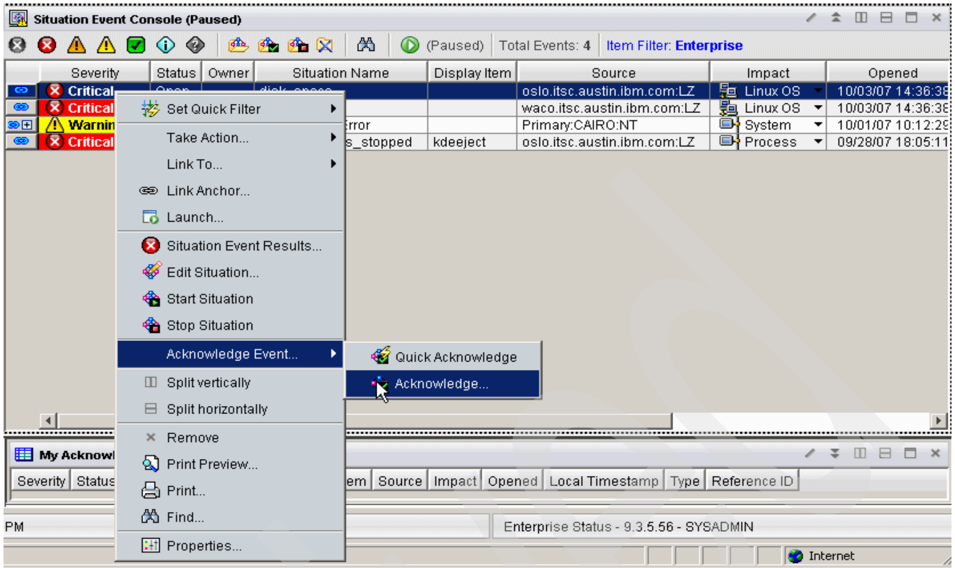
Node(+)	Alert Group	Summary(+)	Last Occurrence	Count
mondorf	SNMP	node down	/03/2007 02:10:01 P	1
oslo.itsc.austin.ibm.	ITM_Linux_Disk	disk_space[(Disk_NameLIKE"*" AND Space_Available_Percent<90) ON oslo.itsc	/03/2007 02:34:08 P	12
salvador	Administrator	A Administrator process running on salvador has connected as username root	/03/2007 02:15:34 P	1
salvador	Windows Event List	A NT Event List@090305CC process running on salvador has connected as user	/03/2007 12:00:20 P	1
salvador	Windows Event List	A NT Event List@090305CC process running on salvador has connected as user	/03/2007 12:00:21 P	1
salvador	Windows Event List	A NT Event List@090305CC process running on salvador has connected as user	/03/2007 11:43:42 A	1
salvador	Windows Event List	A NT Event List@090305CC process running on salvador has connected as user	/03/2007 11:43:44 A	1
salvador	Probe	A PROBE process running on salvador has disconnected as username probe	/03/2007 11:43:30 A	1
salvador	NT Event List@090305C	Attempt to login as netcool from host salvador failed	/03/2007 10:22:45 A	1
salvador		mhntlog probe on salvador:Host - salvador : Log - Application -> Attempting to c	/03/2007 11:23:30 A	1
salvador		mhntlog probe on salvador:Host - salvador : Log - Application -> Successfully co	/03/2007 11:23:30 A	1
salvador		mhntlog probe on salvador:Host - salvador : Log - Security -> Attempting to con	/03/2007 11:23:30 A	2
salvador		mhntlog probe on salvador:Host - salvador : Log - Security -> Successfully conn	/03/2007 11:23:30 A	2
salvador		mhntlog probe on salvador:Host - salvador : Log - System -> Attempting to conn	/03/2007 11:23:30 A	2
salvador		mhntlog probe on salvador:Host - salvador : Log - System -> Successfully conn	/03/2007 11:23:30 A	2
waco.itsc.austin.ib	ITM_Linux_Disk	disk_space[(Disk_NameLIKE"*" AND Space_Available_Percent<90) ON waco.its	/03/2007 02:34:08 P	12
weimar	Administrator	A Administrator process running on weimar has connected as username root	/03/2007 02:07:09 P	1
weimar.itsc.austin.i	WEBTOP	A WEBTOP process running on weimar.itsc.austin.ibm.com has connected as us	/03/2007 11:35:44 A	1

8	28	20	7	3	13	All Events

1 row(s) selected. | 10/03/2007 02:35:25 PM | root | WEIMAR[PRI]

Figure 5-13 Netcool/OMNIbus event list

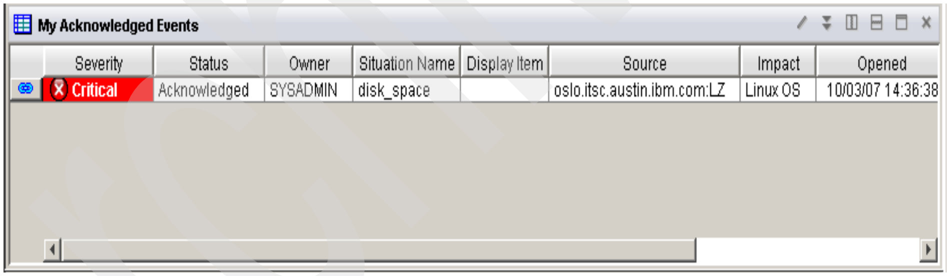
The user can acknowledge the event on the TEP workspace, as shown in Figure 5-14 on page 343.



Severity	Status	Owner	Situation Name	Display Item	Source	Impact	Opened
Critical	Open		disk_space		oslo.itsc.austin.ibm.com:LZ	Linux OS	10/03/07 14:36:38
Critical					waco.itsc.austin.ibm.com:LZ	Linux OS	10/03/07 14:36:38
Warnin			rror		Primary:CAIRO:NT	System	10/01/07 10:12:29
Critical			s_stopped	kdeeject	oslo.itsc.austin.ibm.com:LZ	Process	09/28/07 18:05:11

Figure 5-14 Acknowledging event

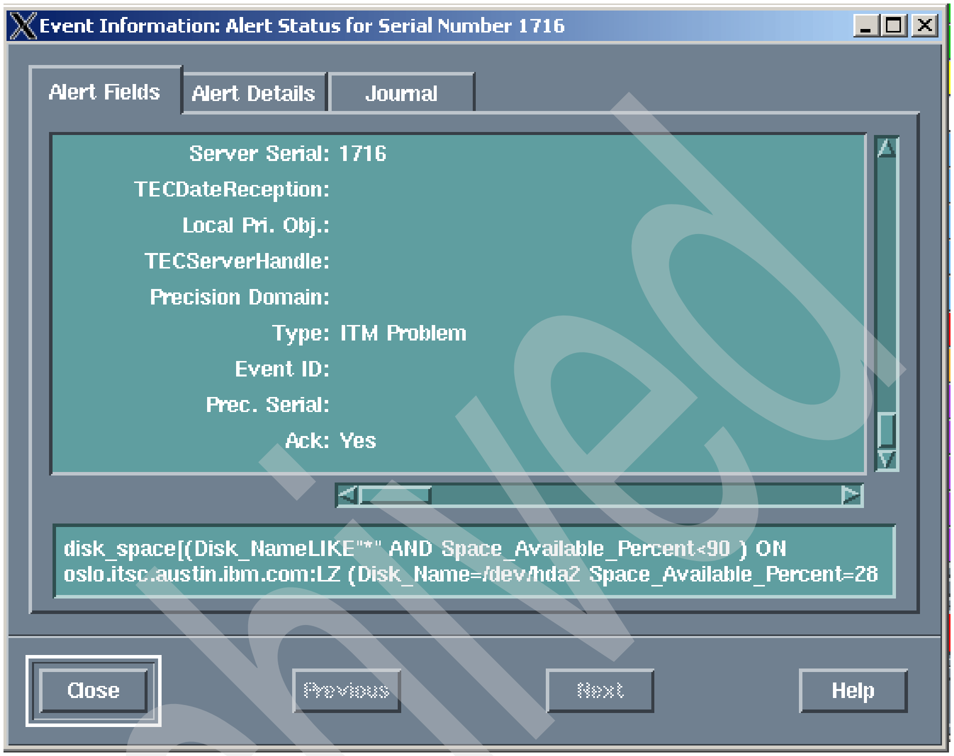
Then the event is acknowledged in the TEP workspace, as shown in Figure 5-15.



Severity	Status	Owner	Situation Name	Display Item	Source	Impact	Opened
Critical	Acknowledged	SYSADMIN	disk_space		oslo.itsc.austin.ibm.com:LZ	Linux OS	10/03/07 14:36:38

Figure 5-15 Event acknowledged

In the Netcool/OMNIbus Event list, we can see that the event has been acknowledged by looking into the Information details, as shown in Figure 5-16.

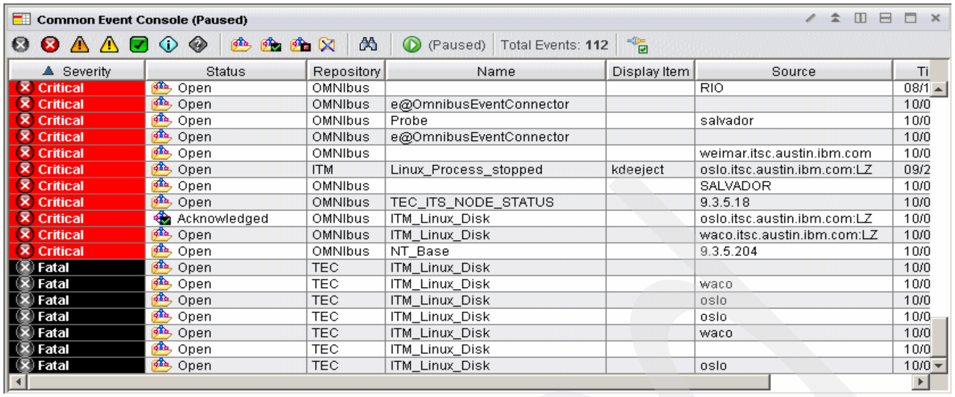


Server Serial: 1716
TECDateReception:
Local Pri. Obj.:
TECServerHandle:
Precision Domain:
Type: ITM Problem
Event ID:
Prec. Serial:
Ack: Yes

disk_space[(Disk_NameLIKE"*" AND Space_Available_Percent<90) ON oslo.itsc.austin.ibm.com:LZ (Disk_Name=/dev/hda2 Space_Available_Percent=28

Figure 5-16 Alert fields updated

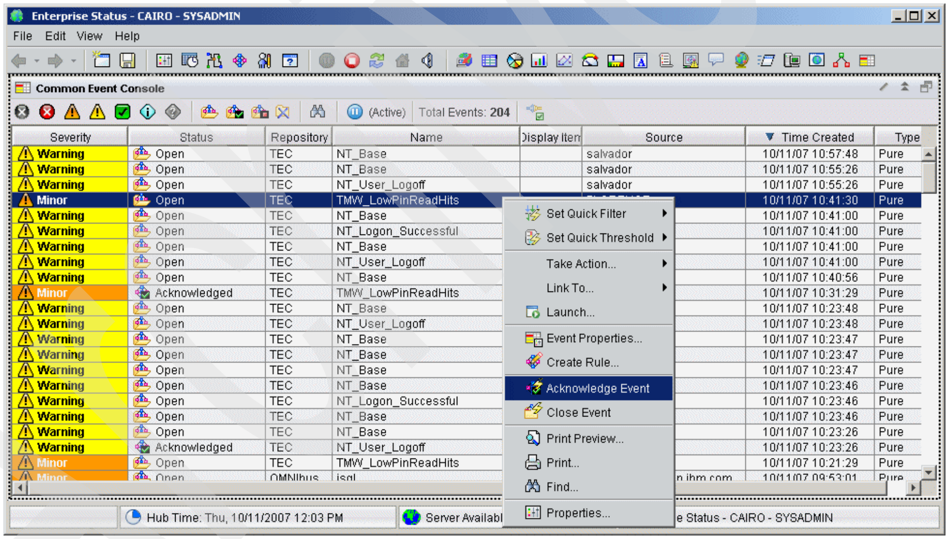
Figure 5-17 on page 345 shows the acknowledged status from the Netcool/OMNIbus connector interface.



Severity	Status	Repository	Name	Display Item	Source	Ti
Critical	Open	OMNIbus			RIO	08/1
Critical	Open	OMNIbus	e@OmnibusEventConnector			10/0
Critical	Open	OMNIbus	Probe		salvador	10/0
Critical	Open	OMNIbus	e@OmnibusEventConnector			10/0
Critical	Open	OMNIbus			weimar.itsc.austin.ibm.com	10/0
Critical	Open	ITM	Linux_Process_stopped	kdeeject	oslo.itsc.austin.ibm.com:LZ	09/2
Critical	Open	OMNIbus			SALVADOR	10/0
Critical	Open	OMNIbus	TEC_ITS_NODE_STATUS		9.3.5.18	10/0
Critical	Acknowledged	OMNIbus	ITM_Linux_Disk		oslo.itsc.austin.ibm.com:LZ	10/0
Critical	Open	OMNIbus	ITM_Linux_Disk		waco.itsc.austin.ibm.com:LZ	10/0
Critical	Open	OMNIbus	NT_Base		9.3.5.204	10/0
Fatal	Open	TEC	ITM_Linux_Disk			10/0
Fatal	Open	TEC	ITM_Linux_Disk		waco	10/0
Fatal	Open	TEC	ITM_Linux_Disk		oslo	10/0
Fatal	Open	TEC	ITM_Linux_Disk		oslo	10/0
Fatal	Open	TEC	ITM_Linux_Disk		waco	10/0
Fatal	Open	TEC	ITM_Linux_Disk			10/0
Fatal	Open	TEC	ITM_Linux_Disk		oslo	10/0

Figure 5-17 Common Enterprise Console

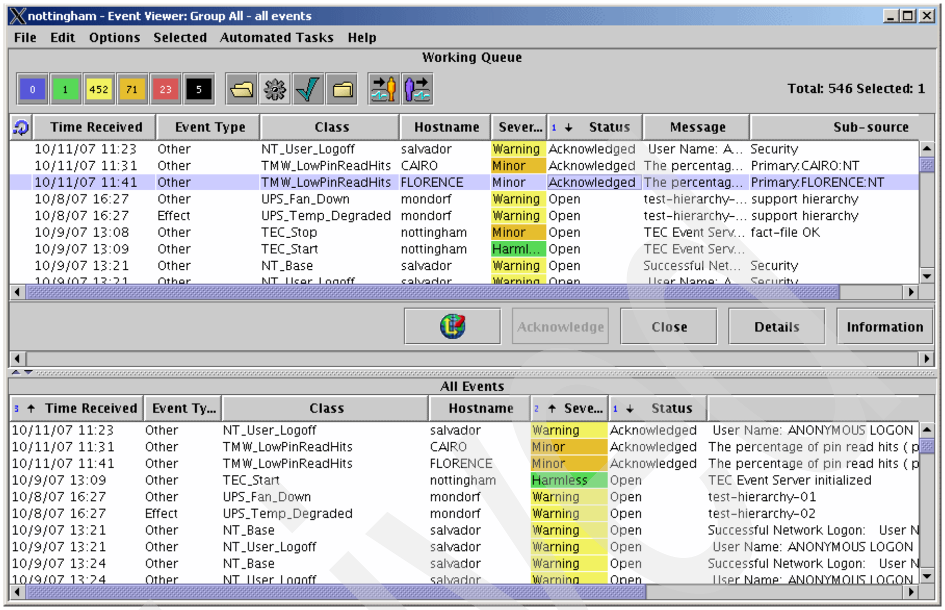
Here we show an example of working with Tivoli Enterprise Console events; right-click **TMW_LowPinReadHits** to acknowledge the event (Figure 5-18).



Severity	Status	Repository	Name	Display Item	Source	Time Created	Type
Warning	Open	TEC	NT_Base		salvador	10/11/07 10:57:48	Pure
Warning	Open	TEC	NT_Base		salvador	10/11/07 10:55:26	Pure
Warning	Open	TEC	NT_User_Logoff		salvador	10/11/07 10:55:26	Pure
Minor	Open	TEC	TMW_LowPinReadHits			10/11/07 10:41:30	Pure
Warning	Open	TEC	NT_Base			10/11/07 10:41:00	Pure
Warning	Open	TEC	NT_Logon_Successful			10/11/07 10:41:00	Pure
Warning	Open	TEC	NT_Base			10/11/07 10:41:00	Pure
Warning	Open	TEC	NT_User_Logoff			10/11/07 10:41:00	Pure
Warning	Open	TEC	NT_Base			10/11/07 10:40:56	Pure
Minor	Acknowledged	TEC	TMW_LowPinReadHits			10/11/07 10:31:29	Pure
Warning	Open	TEC	NT_Base			10/11/07 10:23:48	Pure
Warning	Open	TEC	NT_User_Logoff			10/11/07 10:23:48	Pure
Warning	Open	TEC	NT_Base			10/11/07 10:23:47	Pure
Warning	Open	TEC	NT_Base			10/11/07 10:23:47	Pure
Warning	Open	TEC	NT_Base			10/11/07 10:23:47	Pure
Warning	Open	TEC	NT_Base			10/11/07 10:23:46	Pure
Warning	Open	TEC	NT_Logon_Successful			10/11/07 10:23:46	Pure
Warning	Open	TEC	NT_Base			10/11/07 10:23:46	Pure
Warning	Open	TEC	NT_Base			10/11/07 10:23:26	Pure
Warning	Acknowledged	TEC	NT_User_Logoff			10/11/07 10:23:26	Pure
Minor	Open	TEC	TMW_LowPinReadHits			10/11/07 10:21:29	Pure
Minor	Open	OMNIbus	isql		n.ibm.com	10/11/07 09:53:01	Pure

Figure 5-18 Acknowledging a Tivoli Enterprise Console event

Figure 5-19 show this event as acknowledged in TEC Console as well.



nottingham - Event Viewer: Group All - all events

Total: 546 Selected: 1

Time Received	Event Type	Class	Hostname	Sever...	1 ↓ Status	Message	Sub-source
10/11/07 11:23	Other	NT_User_Logoff	salvador	Warning	Acknowledged	User Name: A...	Security
10/11/07 11:31	Other	TMW_LowPinReadHits	CAIRO	Minor	Acknowledged	The percentag...	Primary:CAIRO:NT
10/11/07 11:41	Other	TMW_LowPinReadHits	FLORENCE	Minor	Acknowledged	The percentag...	Primary:FLORENCE:NT
10/8/07 16:27	Other	UPS_Fan_Down	mondorf	Warning	Open	test-hierarchy-...	support hierarchy
10/8/07 16:27	Effect	UPS_Temp_Degraded	mondorf	Warning	Open	test-hierarchy-...	support hierarchy
10/9/07 13:08	Other	TEC_Stop	nottingham	Minor	Open	TEC Event Serv...	fact-file OK
10/9/07 13:09	Other	TEC_Start	nottingham	Harml...	Open	TEC Event Serv...	
10/9/07 13:21	Other	NT_Base	salvador	Warning	Open	Successful Net...	Security
10/9/07 13:21	Other	NT_User_Logoff	salvador	Warning	Open	User Name: A...	Security

3 ↑ Time Received	Event Ty...	Class	Hostname	2 ↑ Seve...	1 ↓ Status	
10/11/07 11:23	Other	NT_User_Logoff	salvador	Warning	Acknowledged	User Name: ANONYMOUS LOGON
10/11/07 11:31	Other	TMW_LowPinReadHits	CAIRO	Minor	Acknowledged	The percentage of pin read hits (p
10/11/07 11:41	Other	TMW_LowPinReadHits	FLORENCE	Minor	Acknowledged	The percentage of pin read hits (p
10/9/07 13:09	Other	TEC_Start	nottingham	Harmless	Open	TEC Event Server initialized
10/8/07 16:27	Other	UPS_Fan_Down	mondorf	Warning	Open	test-hierarchy-01
10/8/07 16:27	Effect	UPS_Temp_Degraded	mondorf	Warning	Open	test-hierarchy-02
10/9/07 13:21	Other	NT_Base	salvador	Warning	Open	Successful Network Logon: User N
10/9/07 13:21	Other	NT_User_Logoff	salvador	Warning	Open	User Name: ANONYMOUS LOGON
10/9/07 13:24	Other	NT_Base	salvador	Warning	Open	Successful Network Logon: User N
10/9/07 13:24	Other	NT_User_Logoff	salvador	Warning	Open	User Name: ANONYMOUS LOGON

Figure 5-19 TEC Console

6

Agent Builder

This chapter will provide a brief overview of the IBM Tivoli Monitoring V6.2 Agent Builder and provide an overview of a video demonstration using the new Agent Builder.

The following topics are discussed:

- "Agent Builder overview" on page 348
- "Common data manipulation" on page 349
- "Installing the Agent Builder" on page 353
- "Testing and debugging your agent" on page 354
- "Environment variables on the agent" on page 354
- "Agent Builder Demonstration Video" on page 356

6.1 Agent Builder overview

IBM Tivoli Monitoring Agent Builder is a set of tools used for creating agents, installation packages for the created agents and value-add solutions for existing agents. Using the IBM Tivoli Monitoring Agent Builder, you can quickly create, modify, and test an agent. Agents collect and analyze data about the state and performance of different resources, such as disks, memory, CPU, or applications. Agent Builder is based on Eclipse and runs on Windows, AIX, and Linux platforms.

Note: The IBM Tivoli Monitoring Agent Builder is a plug-in for the Eclipse 3.2 platform, an open source framework for the construction of powerful software development tools and rich desktop applications. Leveraging the Eclipse plug-in framework to integrate technology on the desktop can save technology providers time and money for focusing effort on delivering differentiation and value for their offerings. Eclipse is a multi-language, multi-platform, and multivendor supported environment that an open source community of developers built and provided royalty-free through the Eclipse Foundation. Written in the Java language, Eclipse includes extensive plug-in construction toolkits and examples, and can be extended and run on a range of desktop operating systems, including Windows, Linux, QNX, and Macintosh OS X. To see the full details about Eclipse and the Eclipse Foundation, go to `http://www.eclipse.org`.

Agent Builder creates stand-alone agents that can run on Windows, AIX, Linux, Solaris, and HP platforms. It can incorporate queries, situations and workspaces with the agent. Agent Builder creates local or remotely installed images at the end of the customization process.

The Agent Builder creates agents that have encapsulated data providers, unlike the Universal Agent, where all the data providers are exposed. The Agent Builder creates a number of XML files that are used to direct the built-in data providers. The deployed agents are fully integrated into the Enterprise Information Base (EIB). The EIB is the infrastructure of all collected data by the IBM Tivoli Monitoring product. Since data provided by the Agent Builder built agents is integrated into the EIB, it provides seamless integration into the Tivoli Portal real time and historical query interface. It also allows administrators to create monitoring situations for the Agent Builder data providers. Finally, it also provides a common portal interface to turn data warehousing on.

The Agent Builder created agents contain three common data providers as follows:

- Availability

  The Availability provider provides a common provider for gathering process and service data. The Availability provider will gather process performance data: CPU Usage (Total, Privileged, and User Mode), Thread Count, Virtual Size Working Set Size, Page Fault Rate, and Command Line information. It will also provide functionality tests for status and specific failure types. The Availability provider will also check the status of a Windows' service (up, down, or not installed).

- Standard Data Collection interfaces

  The Standard Data Collection provider is a catch all for collection interfaces such as Windows Management Instrumentation (WMI), Perfmon, Windows Event Log, and SNMP V1. An Agent Builder created agent can select or create derived attributes that can integrated into the EIB.

- Extensions

  The third kind of Agent Builder data provider is called the extensions provider. The extensions provide a way to launch scripts or read generic logs.

6.2 Common data manipulation

Attributes gathered from the common Agent Builder data providers can be modified to describe how the attributes are displayed in the Tivoli Enterprise Portal. The following is a list of attribute types that can be defined:

- Counter

  A positive integer value containing values that generally increase over time. Data aggregation in the warehouse displays the total, high, low, and latest values.

- Delta

  An integer value representing the difference between the current value and the previous value for this attribute. Because this attribute is represented as a gauge in the warehouse, data aggregation in the warehouse produces minimum, maximum, and average values.

- Display string

  A string value that can contain any UTF-8 characters. The length that is defined is the total length of the buffer allocated to contain the string. In non-ASCII characters, this attribute may take more than 1 byte per character. Data aggregation in the warehouse displays the latest value collected during the period.

- Enumeration

  An integer value with strings associated with identified values. The string values are displayed in the Tivoli Enterprise Portal. This attribute is used for a set of specific values with identified meanings (for example, 1=UP, 2=DOWN). Data aggregation in the warehouse displays the latest value collected during the period.

- Gauge

  Integer values where the values returned are higher and lower than previous values. Negative values are supported. This type should be the default type for integers. Data aggregation in the warehouse produces minimum, maximum, and average values.

- Percent change

  An integer value that represents the percent change between the current value and the previous value. This type is calculated as: ((new -old)*100)/old. Because this type is represented as a Gauge in the warehouse, data aggregation in the warehouse produces minimum, maximum, and average values.

- Rate of change

  An integer value representing the difference between the current value and the previous value divided by the number of seconds between the samples. It converts a value (such as bytes) to the value per second (bytes per second). Because this type is represented as a Gauge in the warehouse, data aggregation in the warehouse produces minimum, maximum, and average values.

- Timestamp

  A string attribute whose format conforms to the format CYYMMDDHHMMSSmmm (where C=1 for the 21st century). When displayed in the Tivoli Enterprise Portal, a time stamp attribute type is displayed in the correct format for the locale. When using the browse feature for WMI, the Agent Builder automatically marks attributes whose CIM type is CIM_DATETIME as timestamps. The data provider automatically converts WMI attributes to this format.

Attributes can also be derived. The value for a derived attribute is the result of evaluating an expression based on constants and the values of other attributes in the same data source. The expression grammar is the normal mathematical expression: *operand operator operand* with parentheses used for grouping. Integer attributes may be combined with other integer attributes or constants using the normal mathematical operators: +, -, *, /, and %. String attributes can be combined with other string attributes or constants with +. An attribute is represented by its name (the same name you see in the Data Source Information tree). Integer constants are specified as numbers. String contestants are surrounded by quotes; an example is shown in Example 6-1.

Example 6-1 String contestants

```
Myattr1 + Myattr2
Myattr1 - Myattr2
Myattr * Myattr2
Myattr / Myattr2
Myattr1 % Myattr2 (percentage of)
```

6.3 Agent Builder features

Here we discuss some of the features of the Agent Builder.

6.3.1 Full function agents

The agents built by the Agent Builder are full function agents that act just like the agents shipped with IBM Tivoli Monitoring. They do not use the Universal Agent. Therefore, agents created by Agent Builder will function similarly to IBM provided agents. They can be started, stopped, and configured remotely or locally, just like any other agent.

6.3.2 Remote deployment

Agent Builder agents use exactly the same system for remote deployment as other IBM Tivoli Monitoring agents. Anything that works for them will work for an Agent Builder agent.

6.3.3 Versioning

The Agent Builder agents do not use the Universal Agent versioning system. They use the same versioning system used by all other IBM Tivoli Monitoring agents. The developer of the agent assigns a version and determines when a new version is created. This means that you can have multiple versions of an Agent Builder agent in an IBM Tivoli Monitoring deployment at the same time and the monitoring server, portal server, and portal will be able to correctly handle each of the agents according to its version. You can upgrade a system from one version to another just like other IBM Tivoli Monitoring agents.

6.3.4 Support of scripts

If you create an Agent Builder agent and put scripts into its project, they will become part of the agent image and they will be pushed out with the agent when it is pushed out to a system using remote deployment.

6.3.5 Log file monitoring

The Agent Builder built agents use the same code base as the Universal Agent File Data Provider. All of the options included in the IBM Tivoli Monitoring V6.2 Universal Agent are also supported in the Agent Builder Agent. Most of the options can be created using the Eclipse wizard.

6.3.6 Remote browsing

From the Eclipse based Agent Builder, you can remotely browse processes and services on remote computers. You can also browse WMI, Perfmon, and SNMP. The remote browser uses native Windows for WMI, Perfmon, and Services. For all other options, it connects to a Tivoli Enterprise Management Server (TEMS) to gather data from the remote systems OS agent (process, WMI, and Perfmon). For SNMP, it browses a local MIB that has been loaded on the Agent Builder machine.

6.3.7 Generate Migration Agent Mapping file

You can ease the IBM Tivoli Monitoring V5 migration by generating the Agent Mapping file for Custom Resource Model migration.

6.4 Installing the Agent Builder

The Agent Builder can be installed on the following platforms:

- Windows 2003 Server SE (32-bit) with Service Pack 1
- Windows 2003 Server EE (32-bit) with Service Pack 1
- Windows 2003 Data Center
- Windows XP Professional
- Windows 2000 Server
- Windows 2000 Advanced Server
- Red Hat Enterprise Linux V4.0 + U2
- Red Hat Desktop Linux V4.0 + U2
- SUSE Linux Enterprise Server V9 Sp1
- AIX 5L V5.2 ML10 or higher
- AIX 5L V5.3 ML5 or higher

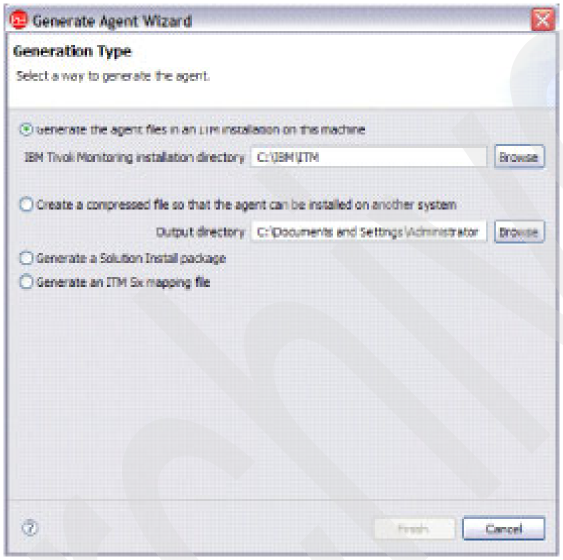
The Agent Builder has three install images for Windows, AIX, and Linux, platforms respectively:

- setup.exe
- setupaix.bin
- setuplinux.bin

See the *IBM Tivoli Monitoring Version 6.2.0 Agent Builder User's Guide*, SC32-1921 for more information.

6.5 Testing and debugging your agent

After the agent is created, you can install the agent on an IBM Tivoli Monitoring system to test and debug the agent. The best methodology for doing this is to install a single system image of IBM Tivoli Monitoring V6.2 and then also install the Agent Builder on the same system. For example, on a Windows system, you would install the monitoring server, portal server, OS Agent, and the Agent Builder on the single Windows system. When you have completed the first phase of your development, you would generate the agent and select the local install option, as seen in Figure 6-1.



Generate Agent Wizard

Generation Type

Select a way to generate the agent.

● Generate the agent files in an ITM installation on this machine

IBM Tivoli Monitoring installation directory: C:\IBM\ITM

○ Create a compressed file so that the agent can be installed on another system

Output directory: C:\Documents and Settings\Administrator

○ Generate a Solution Install package

○ Generate an ITM 5x mapping file

Figure 6-1 Generate Agent Wizard

6.6 Environment variables on the agent

Environment variables can be configured on the agent to affect the agent's runtime behavior. The variables can be set in the KXXENV file on Windows or the $CANDLEHOME/config/XX.ini file, where XX is the product code number defined for the Agent Builder built agent, for example, K00. The agent must be restarted for the new settings to take effect.

Some of the environment variables are:

- CDP_DP_CACHE_TTL

  Any integer greater than or equal to 1. Data collected for an attribute group is cached for this number of seconds. Multiple requests for the same data in this time interval receive a cached copy of the data. This value applies to all attribute groups in the agent. (You cannot set different values for each attribute group.) The default is 30.

- CDP_NT_EVENT_LOG_GET_ALL_ENTRIES_FIRST_TIME

  If set to YES, the agent sends an event for every event in the Windows event log. If set to NO, only new events in the Windows event log are sent. The default is NO.

- CDP_NT_EVENT_LOG_CACHE_TIMEOUT

  The number of seconds Windows Event log events are cached by the agent. All cached events are returned when the event log attribute group is queried. The default is 3600 seconds

- CDP_PURE_EVENT_CACHE_SIZE

  The maximum number of events to cache when a log file data source is configured to process new records. Each new record in the log will cause an event to be sent. This environment variable defines how many events are remembered in a cache by the agent. The cached values are returned when the attribute group is queried. The default is 100.

- CDP_DP_ACTION_TIMEOUT

  The number of seconds to wait for a take action being handled by the agent to complete. The default is 20.

- CDP_DP_SCRIPT_TIMEOUT

  The number of seconds to wait for the program launched by a script based attribute group to complete. The default is 30.

- CDP_DP_PING_TIMEOUT

  The number of seconds to wait for the program launched by a functionality test to complete. The default is 30.

6.7 Agent Builder Demonstration Video

In this last section, we provide a link to a Demonstration Video of the Agent Builder. In this video, we provide an overview of how to use and create agents using the new IBM Tivoli Monitoring Agent Builder shipped with Version 6.2. The video shows you how to do the following actions:

- Create anew agent using the Agent Builder.
- Create runtime configuration information.
- Use the application availability wizard.
- Use Perfmon data.
- Use WMI data.
- Generate and install a local image of an agent.
- Configure an Agent Builder built agent from the Manage Tivoli Enterprise Monitoring Services (MTEMS).
- Start and stop the agent.
- Create situations against the installed Agent Builder built agent.
- Customize an already installed agent.
- Add additional attributes and create derived variables.
- Re-generate and re-install the agent.
- Review how to run scripts and SNMP based agents.
- Review the installation of a remote and solution installed image.

6.7.1 How to launch the video

Use the following link to launch the video:

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

Part 3

Planning for a client engagement

In this part, we focus on service engagement planning for IBM Tivoli Monitoring V6.2. The target audience of this part is IBM Business Partners and Solution Developers.

A

Planning for a client engagement

In this appendix, we discuss service engagement for IBM Tivoli Monitoring in general. The target audience of this appendix is IBM Business Partners and Solution Developers. The topics that we discuss include the following:

- “Services engagement preparation” on page 360
- “Solution scope and components” on page 361
- “Services engagement overview” on page 363
- “Estimating timings and activities of the engagement” on page 372

> **Important:** The time estimates in this chapter are not representative of all the possible implementation scenarios of a IBM Tivoli Monitoring based solution. Each environment is considered to be unique and the time estimates should be regarded as general guidelines, not absolute numbers.

Services engagement preparation

This section describes the resources that are available to help you successfully deliver a solution. The end goal of a services engagement may be comprised of all or some of the following items:

- Describe the IBM Tivoli Monitoring V6.2 architecture and components.
- Plan and design an IBM Tivoli Monitoring V6.2 solution based on client requirements/environment.
- Install and configure prerequisites for IBM Tivoli Monitoring V6.2.
- Install and configure IBM Tivoli Monitoring V6.2 infrastructure components and integrated products (IBM Tivoli Enterprise Console, IBM Tivoli Netcool®, IBM TADDM, and so on).
- Use and customize various interfaces to configure and administer the IBM Tivoli Monitoring V6.2 environment.
- Perform performance tuning and problem determination for IBM Tivoli Monitoring V6.2.

The discussion is divided into the following sections:

- "Implementation skills" on page 360
- "Available resources" on page 361

Implementation skills

To successfully develop and deploy a IBM Tivoli Monitoring based solution, you must acquire some specialized skills. The following lists the skills needed to implement and customize the solution:

- Working knowledge of OS Administration, networking, and firewall concepts.
- Working knowledge of the Extensible Markup Language (XML).
- Basic knowledge of security (SSL, data encryption, GS Kit, and system user accounts).
- Basic knowledge of databases and Open Database Connectivity (ODBC).
- Basic knowledge of the enterprise wide monitoring concepts.
- Basic knowledge of protocols, including HTTP and Simple Object Access Protocol (SOAP).

The exact skills balance that you will need depends on the environment that you intend to build with this technology, and also the server platform on which you intend to host the management solution.

Available resources

The prerequisite skills listed in “Implementation skills” on page 360 are needed to customize or develop the solution. For each of these skills, there are a variety of resources available to help acquire the necessary skill level. Some of the educational resources available are:

- Online help: Tivoli Monitoring provides seminars on the Web. Details of these materials can be found at:

  http://www-306.ibm.com/software/tivoli/education/edu_prd.html

- Further technical information, including trial codes, white papers, and support links, can be found at:

  http://www-306.ibm.com/software/tivoli/products/monitor/

- Classroom training: IBM PartnerWorld® provides current information about available classes, their dates, locations, and registration. Additionally, check the PartnerEducation Web site, which serves as a single point-of-contact for all IBM Business Partner education and training. Further details can be found at:

  http://www-306.ibm.com/software/tivoli/education/

- IBM Technical Education Services (ITES) offers a variety of classes at all knowledge levels to help you achieve any of the offering's prerequisite skills.
- IBM Redbooks publications: You can access various practical and architectural information regarding IBM hardware and software platforms from IBM Redbooks. PDFs are available for download from the Web site http://ibm.com/redbooks.

Solution scope and components

Define the scope of the solution. The solution can be one of the two types of basic offerings in “Basic solution definition” on page 362, or you can add additional components, as shown in “Advanced solution definition” on page 363.

IBM Tivoli Monitoring

IBM Tivoli Monitoring provides an integrated set of solutions for monitoring the status, availability, and performance of all systems and applications running in a heterogeneous, distributed environment. In addition, it notifies administrators and can take automated actions upon sensing events that may lead to problems that could affect business critical systems.

IBM Tivoli Monitoring is built on a robust architecture that provides a customizable portal, called the Tivoli Enterprise Portal (portal), which can be viewed using a standard browser or a thick client application. The Tivoli Enterprise Monitoring Server (monitoring server) gathers availability and performance data from dedicated agents running on the monitored machines or in an agent-less mode, and feeds data and events to the portal server.

Included with IBM Tivoli Monitoring is the Universal Agent that allows you to create or customize a monitor for applications where there are no existing Tivoli Monitoring agents.

> **Note:** IBM Tivoli Monitoring Express product might be more suited for small and medium-sized businesses. This product has a functions similarly to IBM Tivoli Monitoring V6.1 (IBM Tivoli Monitoring Express V6.2 does not yet exist), with some differences.
>
> For example, the IBM Tivoli Monitoring Express license is limited to a single server install and allows you to monitor up to 100 servers. You need a license for each server being monitored unless it is monitored using agent-less monitoring (for example, devices or computer sending SNMP alerts). In addition, the Express version is not licensed to integrate with certain non-Express versions of other Tivoli products (for example, IBM Tivoli Enterprise Console). So based on the monitoring requirements and the size of the implementation, you need to decide whether to use the Express or non-Express version of IBM Tivoli Monitoring. For a detailed discussion of IBM Tivoli Monitoring Express, refer to *Deployment Guide Series: IBM Tivoli Monitoring Express Version 6.1*, SG24-7217.

Basic solution definition

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

Advanced solution definition

The monitoring solution can be integrated with other systems management products or technologies to provide a more comprehensive solution, such as the following:

- Integration with IBM Tivoli Enterprise Console to quickly identify the root cause of business performance issues.
- Integration with IBM Tivoli Netcool/OMNIbus to provide real-time, end-to-end event management for complex infrastructures.
- Integration with IBM Tivoli Application Dependency Discovery Manager (TADDM), to provide complete and detailed application maps of business applications and their supporting infrastructure, including cross-tier dependencies, runtime configuration values, and complete change history.
  - The IBM Tivoli Monitoring integration with TADDM provides comprehensive monitoring of application resources, automatically identifies all resources that are unmonitored, and automatically provisions agents.
  - The benefits of using TADDM with IBM Tivoli Monitoring is faster closed loop troubleshooting, identification of infrastructure changes, and the reduction of Mean-Time-To-Resolution (MTTR) by the correlation of infrastructure health to changes.
- Integration with IBM Tivoli Provisioning Manager will provide the ability to install the IBM Tivoli Monitoring V6.2 Operating System Agent on to a machine that has been provisioned by IBM Tivoli Provisioning Manager.

Services engagement overview

Implementers of a solution routinely rely on their skills and previous experiences as a guide, but there are always some issues that may require some educated guesswork. The goal of this section is to help you minimize the guesswork involved in planning and implementing a solution by providing a framework and time estimates for the major tasks.

A typical services engagement consists of the following:

- Build an executive assessment (see “Executive Assessment” on page 364).
- Set up a demonstration system or proof of technology (see “Demonstration system setup” on page 365).
- Analyze the solution tasks (see “Analyze solution tasks” on page 369).

- Create a contract, commonly known as a Statement of Work (see “Creating a contract” on page 370).

The representative tasks and the time involved for custom solution execution are included in the following section. Since each client has a unique set of needs, the actual set of tasks to accomplish and the time involved may vary. However, this list should help you understand the implementation details, size the solution more accurately for the client, and ensure a profitable engagement for yourself.

It is important to work with your clients to understand their expectations. After you gather this data, document the tasks, deliverables, and associated costs in a Statement of Work. The Statement of Work acts as your contractual agreement with the client for the duration of the project; therefore, a detailed and well-defined Statement of Work is advantageous both to you and to your client.

A good overall understanding of the solution scope is a crucial prerequisite to successfully developing and implementing it. As a Solution Provider, you must understand what is involved in developing such a solution before you can discuss it with your client and size it for a cost estimate.

Executive Assessment

The Executive Assessment is a service that can be offered to prospective clients as a billable service. It offers a process designed to help you evaluate the business needs of a company that is planning to deploy a solution for e-business.

This toolset helps you ask the right people the right questions, so that you get the information you need to propose the appropriate solution. The complete Executive Assessment process should take approximately 10 to 16 hours. The task breakdown is shown in Table A-1.

Table A-1   Solution task

Task	**Estimated time (hours)**
An initial fact-finding meeting, asking questions, and gathering data	3
A review and analysis of competing solutions	2
Preparation of a set of strategic recommendations	1
Creation of a demonstration prototype	3 - 9
A presentation of findings and close for a contract	1
Total	**10-16**

This is a business-case assessment, not a technical assessment, so the audience should be business owners, line-of-business executives, marketing and sales managers, and finally, the IT manager. The business owner or line-of-business executive is likely to be the decision maker.

For their initial investment, your clients get the following:

- A business assessment prepared by a professional (you)
- A competitive analysis
- A prototype solution for their review
- A strategic and tactical proposal for justifying and implementing their solution for e-business

Demonstration system setup

A demonstration system is typically set up in advance to show your clients the attributes of the solution. The demonstration system can typically be set up with a limited number of systems that are separate from the system that will be used by the production system. The demonstration can be virtualized with technologies such as Zen, VMWARE, or Microsoft Virtual Server.

A simple demonstration can be performed on one server that has all the IBM Tivoli Monitoring Server components installed and a selection of IBM Tivoli Monitoring agents.

If it is a key part of the engagement that you need to monitor some specific resources such as applications or log files, then it is important to get samples of these resources and show how IBM Tivoli Monitoring can be used to monitor them.

The demonstration system allows your clients to evaluate whether the solution suits their particular needs.

The tasks of demonstrating the solution and its time estimate are shown in Table A-2.

Table A-2 Solution demonstration tasks

Task	Estimated time (hours)
Set up hardware.	1 - 2
Install and configure Tivoli Monitoring Server Components.	2 - 3
Install and configure Tivoli Monitoring Server Agents.	1 - 2
Demonstrate Monitoring to client.	2
Total	**6- 9**

Hardware and software requirements

Check the product manuals and release notes for the exact revisions. Here are a few items to consider. The minimum configuration for the IBM Tivoli Monitoring server are discussed in the following sections.

Server hardware requirements

- For best performance, processor speeds are recommended to be at least:
  - 1 GHz for RISC architectures
  - 2 GHz for Intel architectures
- Except for the Tivoli Data Warehouse, single processor systems are suitable when an IBM Tivoli Monitoring infrastructure component is installed on a separate computer from the other components.
- The disk and memory requirements for each IBM Tivoli Monitoring component vary depending on the size of the environment, and the number of agents in the environment. More details can be found in the *IBM Tivoli Monitoring Version 6.2.0 Installation and Setup Guide,* GC32-9407.
- The disk requirements for the Tivoli Data Warehouse can be estimated using the Tivoli Data Warehouse 2.1 Warehouse Load Projections spreadsheet, which can be downloaded from the OPAL Web site at:

  `http://catalog.lotus.com/wps/portal/topal`

Server software requirements

Certain IBM Tivoli Monitoring components are only supported on certain platforms, as detailed in *IBM Tivoli Monitoring Version 6.2.0 Installation and Setup Guide,* GC32-9407. Some notable points are:

- For the Windows XP and Windows Vista operating systems, the Microsoft End User License Agreement (EULA) does not license these operating systems to function as a server. Tivoli products that function as a server on these operating systems are supported for demonstration purposes only.
- All IBM Tivoli Monitoring components are supported on Windows 2003 Server EE/SE (32 bit) with Service Pack 1.

Required software for integration with Netcool/OMNIbus

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

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

Required software for integration with Tivoli Enterprise Console

The following products must be installed and configured before you install event synchronization and configure event forwarding for Tivoli Enterprise Console:

- IBM Tivoli Enterprise Console 3.9 with Fix Pack 03

Database Server requirements

- The Tivoli Enterprise Portal Server (TEPS) requires either DB2 or MS SQL and the portal server database must be located on the computer where the portal server is installed.
  - On AIX, Linux, or Windows:
    - IBM DB2 UDB V8.1 with Fix Pack 10 or higher fix packs, V8.2 with Fix Pack 3 or higher fix packs, and V9.1 and fix packs.
  - On Windows:
    - IBM DB2 UDB V8.1 with Fix Pack 10 or higher fix packs, V8.2 with Fix Pack 3 or higher fix packs, and V9.1 and fix packs.

      or
    - MS SQL 2000 SP3

- The Tivoli Data Warehouse requires either DB2, MS SQL, or Oracle:
  - IBM DB2 UDB V8.1, Fix Pack 10 and higher fix packs, V8.2, Fix Pack 3 and higher fix packs, and V9.1 and fix packs on the following operating systems:
    - AIX 5L V5.3
    - HP-UX 11i V3
    - Solaris 10
    - Windows 2003 Server
    - SUSE Linux Enterprise Server 9 and 10 for Intel Red Hat Enterprise Linux 4 for Intel
  - MS SQL 2000 EE6 MS SQL 2005
  - Oracle V9.2, 10g Release 1, and 10g Release 2 on the following operating systems:
    - AIX 5L V5.3
    - HP-UX 11i V3
    - Solaris 10
    - Windows 2003 Server
    - SUSE Linux Enterprise Server 9 and 10 for Intel
    - Red Hat Enterprise Linux 4 for Intel

Client hardware requirements

The Tivoli Enterprise Portal (portal) Browser client and Desktop client require JRE 1.5. The portal browser client requires Microsoft Internet Explorer V6.0 or later with all critical updates.

Monitoring agents available for deployment

The agents available for deployment in the IBM Tivoli Monitoring suite are:

- IBM Tivoli Monitoring for Messaging and Collaboration monitors the status of Microsoft Exchange and Lotus® Domino® servers, identifies server and system problems in real time, notifies administrators, and takes automated actions to resolve server problems.
- IBM Tivoli Monitoring Active Directory® Option provides a central point of management for your Microsoft Active Directory service, allowing early problem detection and prevention. Multiple servers can be monitored from a single console, and information is standardized across the system.

- IBM Tivoli Monitoring for Databases for DB2, Oracle, Microsoft SQL Server, and Sybase helps simplify the management of your back-end database infrastructure by monitoring multiple types of database software.
- IBM Tivoli Monitoring for Applications monitors and manages SAP application performance and availability. It includes best practice situations and expert advice for quick problem identification, notification, and correction.
- IBM Tivoli Monitoring for Cluster Managers monitors cluster manager resource performance and availability and extends the monitoring and management capabilities of Tivoli Monitoring to include Microsoft Cluster Server.
- IBM Tivoli Monitoring for Virtual Servers centrally monitors server virtualization, consolidation, resource performance, and availability for Citrix Access Suite, VMware ESX, and Microsoft Virtual Server for efficient and cost-effective IT operations.

Analyze solution tasks

After the client agrees to use the solution in their environment, decide on what effort that you must perform to implement it. These estimates would then be collected and implemented into a contract or Statement of Work.

We discuss these tasks in detail in "Estimating timings and activities of the engagement" on page 372. The tasks are our suggested tasks and order; you may complete the tasks in a different order or may be omitting or adding tasks depending on the environment to which you implement the solution. The overall solution timing may be influenced by the amount of skill and experience that you or your team have on the solution, and also the access to resources facilitated by your client. The assumption of the estimated timings that we present is typically based on the following:

- Knowledge of the operating systems
- Knowledge of RDBMS and database configuration and management
- Knowledge of IBM Tivoli Monitoring

Depending on your skills and experience, the estimates presented may be too high or too low. Table A-3 illustrates one method of approximating more realistic time estimates for your efforts based on whether you or your team are new to each skill area or could be considered experts. A novice represents someone who completed training in the skill area but has no hands-on experience. An expert represents someone who completed training in the skill area and has also implemented IBM Tivoli Monitoring projects. You may use the percentages in Table A-3 to adjust your time estimate.

Table A-3 Skill adjustment

Skill	**Novice** **Increase by**	**Expert** **Reduce by**
Experience of the operating system	25%	10%
Experience of RDBMS and database management	10	10
Deep understanding of IBM Tivoli Monitoring	40%	20%
Deep understanding of resource monitoring techniques	30%	30%

For the detailed task breakdown, see “Estimating timings and activities of the engagement” on page 372.

Creating a contract

A contract or Statement of Work is a binding contractual agreement between you and your client that defines the service engagement that you must perform and the result that the client can expect from the engagement. The contract should leave nothing in doubt.

A Statement of Work should contain the following:

- An executive summary of the solution, which is typically a short (less than a page) summary of the solution and its benefit. You must specify any major restriction of the implementation, such as the following:
  - The solution is only implemented for finance application servers.
  - The solution will be implemented in phases.
- A solution description, which contains the major components and solution building blocks that will be implemented. It should cover the conceptual architecture of the solution and solution scope in general. This description is aimed for technical personnel to understand the implementation scope.

- Assumptions, which lists all the assumptions that are used to prepare the contract and to provide task estimation. Any deviation from the assumptions that are used will definitely impact the scope of engagement and must be managed using the change management procedure. Typical changes include cost changes or scope changes.
- Business partner responsibilities, which lists all the responsibilities or major tasks to be performed by you or your team to implement the solution.
- Customer responsibilities, which lists all the responsibilities or items that the client must provide for you or your team to perform the engagement. If you cannot obtain any item in the client responsibilities, then a change management procedure may be invoked.
- Staffing estimates, which lists the estimated personnel that must implement the solution.
- Project schedule and milestones, which shows the major steps, schedule, and achievement calendar that can be used to check the project progress.
- Testing methodology, which lists the test cases to ensure that the project implementation is successful.
- Deliverables, which provides tangible items that the client will get at the end of the service engagement, including:
  - Machine installation
  - Documentation
  - Training
- Completion criteria, which lists the items that are provided to the client, which indicates that the engagement is successfully completed. For most service engagements, this is probably the most delicate item to define. It should have clear targets agreed by both parties, and should not be too general.

A sample Statement of Work is provided in Appendix B, “Sample Statement of Work for IBM Tivoli Monitoring” on page 379.

Estimating timings and activities of the engagement

The fundamentals of delivering a profitable and successful services engagement is to correctly identify the tasks that you must perform and to adequately allocate the necessary time to perform them. This section guides you on the tasks that you may need to perform to implement a Tivoli Monitoring solution and estimate the timing. The estimates rely on some basic assumptions, which invalidate the estimates if the items in the following list become a significant requirement for the client:

- Managed environment variance
  - The number and type of target servers' resources to monitor will determine which agents need to be deployed.
- Managed environment size and network topology
  - Do you need remote Tivoli Monitoring servers to cater for scalability, the size of the environment, and geographical and network layout?
- User characteristics and Tivoli Enterprise Portal Usage
  - The portal client is available as a browser client or a desktop client. You can install the desktop client from installation media or you can use IBM Java Web Start to download the desktop client from the Tivoli Enterprise Portal Server. Each of these alternatives has comparative advantages and disadvantages for you to consider when planning your installation.
    - The browser client does not require IBM JRE V1.5 as a prerequisite and it allows you to bookmark workspaces. In addition, the browser client is required for launching products in context, such as IBM Tivoli Application Dependency Discovery Manager.
    - When you use IBM Web Start for Java to obtain and run the desktop client, you benefit from the performance advantage of the desktop client as well as the convenience of centralized administration from the server. Upon each startup of the desktop client, any maintenance updates are downloaded from the server.
  - Do users have access to Internet Explorer?
    - Internet Explorer is required to use the browser client, which can run only from Windows; the desktop client can run on either Windows or Linux.
  - Is the required Java Runtime Environment installed on the users' desktops?
  - What type of users will be using the Tivoli Enterprise Portal?

- Technical users such as Network Administrators and Application specialists. DBAs may need to have access to Tivoli Enterprise Portal as well.

It is useful to characterize the monitoring type that is required by the client for either an operating system resource or application monitoring.

Perform environmental analysis and plan tasks

This section discusses the tasks for environment analysis engagement. Table A-4 shows the timing estimate for the major components of the tasks for the environment analysis service.

Table A-4 Estimated time in hours for identified tasks

Task	Operating system	Application
Identify business objectives and project sponsor.	2	2
Gather details of monitoring requirements (estimates are per resource to be monitored).	2	3
Complete design	5	5
Communicate plan to project sponsor.	2	2
TOTAL HOURS	11	12

To help gather these technical requirements, use the provided sample notes for the issues that they raise as in Table A-5 in order to guide the planning process.

Table A-5 Technical requirement gathering sample questions

Question	Notes
How many different types of platforms need to be monitored?	Each platform will have a specific monitoring agent.
What operating systems resource need to be monitored?	The out of the box monitoring provided by operating system agents has a fixed domain of monitoring. To monitor “non-out of-the-box”, resources may require a Universal Agent solution, or some other customization to be performed.

Question	Notes
How many types of resources need to be monitored, such as processes, log files, databases, application components, and Web transaction performance?	There may be an IBM Tivoli Monitoring agent available for monitoring the specific resource.
Who is responsible for environment configuration, and what is the lead time for making the operating system and application/resource configuration changes?	The configuration of agents (OS and non-OS) will have prerequisites that need to be in place for the correct operation of the agents.
Are there any firewalls in the environment to be monitored? If so, are they between the Monitoring Server (TEMS) and the Agents?	The firewalls will need to be configured to permit traffic on specific ports.
What are the reporting requirements in terms of: ▶ Attributes to be reported against ▶ Hourly, quarterly, weekly, monthly, or yearly reports ▶ Data retention period and pruning settings	The reporting requirements will determine the amount of data that will be captured and retained in the Tivoli Data Warehouse, which must be sized and optimized accordingly.
Are there any failover or disaster recovery requirements?	A hardware failover solution using RAID disks and clustering may be appropriate for mission-critical monitoring environments. In other cases, the IBM Tivoli Monitoring provided software failover solution may suffice.
What are the event correlation and event management requirements?	This will determine whether or not there is a need to have Tivoli Netcool OMNIbus as the repository of all events.
Is there a need to perform application dependency discovery?	A TADDM environment may need to be set up to show how IBM Tivoli Monitoring interfaces with it.
Does the client have any Web sites that need to be monitored for performance?	The IBM Tivoli Composite Application Management (ITCAM) family of products provide extensive Web site and J2EE™ transaction performance monitoring. This environment may need to be set up to show the tremendous value provided by such an integrated solution.

Plan the solution

Planning the deployment of a Tivoli Monitoring solution includes the sub-tasks described in the following list.

- Gather requirements.

  At the beginning of your engagement, you should meet with your clients to understand their proposed objectives and to gather their requirements. First, determine the functional requirements. Functional requirements define the business functions that the monitoring system is going to provide. You determine your requirements by developing a good understanding of the business needs and of what you hope to achieve. For example, look at issues such as business goals, purpose, and usage questions, such as who the users are, and how they expect to interact. It is important to gather these requirements early, and discover any challenges that may lie ahead while they can still be dealt with easily. After you determine the functional requirements, you can clarify the technical or system requirements.

  The technical requirement involves spending time at the client site to determine and understand the available data sources.

- Design the solution.

  Topics that should be addressed range from scalability, functionality, and performance of this solution.

  Design involves understanding the client's environment, including hardware, software, data volumes, special requirements, and operational procedures. It is necessary to identify and plan for any additional tuning of software that may be required because of the client's environment or special needs. In addition, an analysis of the modifications made to the scenarios and reports needs to be performed. After you design the proposed solution and review it with your client, you are ready to begin development of the offering.

- Perform gap analysis.

  This task may involve performing a gap analysis to give the client an estimate of the development effort required to set up the solution. At its core, the analysis seeks to determine what customizable components need to be extended, modified, or created. The number and complexity of customizable components drive the size of the project and the required resources.

After you design the proposed solution and review it with your client, you are ready to proceed.

Implement the solution

The implementation of the solution is performed using the tasks described in Table A-6. Note that here we are estimating times to perform the activity a single time. Remember that the numbers of each item may vary, which will reflect on the total time for the project. The number of agents that need to be deployed, and also the amount of workspaces that need to be configured for users, will also affect the total time for the project.

Table A-6 Timeline estimates for implementation activities

Task	**Estimated time (hours)**
Identify servers and configure any firewalls to allow appropriate IBM Tivoli Monitoring traffic.	1
Install and configure the OS and install the hub monitoring server.	3
Install RDBMS, IBM Tivoli Monitoring portal, and any remote monitoring servers.	2-6
Load depots with agent deployment images.	2
Deploy and Configure one agent.	1
Define user accounts, permissions, or LDAP integration.	2-6
Build managed systems lists and customize workspaces.	6-14
Integrate IBM Tivoli Monitoring with Tivoli Enterprise Console / OMNIbus.	2-3
Configure Historical Data Collection.	1
Test solution.	14
Deliver education: ▶ IBM Tivoli Monitoring for Operators (one day) ▶ IBM Tivoli Monitoring for Administrators (three days)	28
Document solution.	14
Total	**76-93**

Close the engagement

When the technical work is complete, and the education is delivered, formally close the engagement with the project sponsor or their deputy. We suggest that you cover the following agenda items during the meeting with the project sponsor:

1. Review of original business objectives.
2. Summarize how the solution meets the defined objectives.
3. Summarize the services delivered.
4. Summarize new capabilities.
5. Summarize other services or product identified during the engagement.
6. Thank the sponsor and close.

B

Sample Statement of Work for IBM Tivoli Monitoring

In this appendix, we provide a skeleton document that you can use for developing your own customized Statement of Work.

Building an operating system deployment solution

The content of the Statement of Work includes the following activities:

- Install the IBM Tivoli Monitoring component infrastructure.
- Install a selection of different IBM Tivoli Monitoring agents on different platforms.
- Configure Historical Data Collection.
- Configure users and assigning appropriate permissions.
- Configure user workspaces and views.

The IBM Tivoli Monitoring solution Statement of Work consists of the following activities:

- "Executive summary" on page 380
- "Solution description" on page 381
- "Assumptions" on page 381
- "Business Partner responsibilities" on page 381
- "Customer responsibilities" on page 382
- "Staffing estimates" on page 382
- "Testing" on page 382
- "Deliverables" on page 383
- "Completion criteria" on page 383

Executive summary

This service will provide an IT management solution that enables a mid-market business to visualize and monitor its IT resources, and anticipate and resolve issues before they impact the business.

This service will build the infrastructure required to support the monitoring of resources in your environment. It will also supply working samples of the key items that you will need to continue monitoring new machines that enter the environment.

After this work is completed, you will have the infrastructure necessary to successfully monitor operating systems and application resources on your machines, with the following key benefits:

- Increase IT resource availability and reduce cost through quickly identifying and solving problems; less disruption to business.

- Save time and money managing the IT infrastructure through self-managing capabilities.
- Have better visibility and control of an increasing complex IT infrastructure and applications.

Solution description

This solution will build and deploy a monitoring solution that will allow you to visualize the computing resources in your IT Infrastructure in order to monitor for and react to any events that may affect the delivery of critical business services.

We will install and configure the monitoring agents to gather data from one or more systems that you need to monitor in a heterogeneous operating system environment.

Assumptions

These are the assumptions that are made in this Statement of Work:

- We will have local administrator access on the servers on which the ITM components will be installed.
- We will have administrative access to the servers on which monitoring agents need to be installed.
- We will have access to Network Administrators who will be able to configure firewall ports.
- We will have details of which users need access to the Tivoli Monitoring environment, which should be supplied by the customer.

Business Partner responsibilities

This service will be provided according to the high standards of *<name of Business Partner>*, an IBM Certified Business Partner.

We will provide the following:

- Skilled staff to undertake the defined activities
- Documentation of the completed solution
- Project management of these activities

Note: Insert any additional responsibilities here that you will be taking on as part of this project.

Customer responsibilities

This section describes the responsibilities the customer has to the Business Partner, for example:

- Designating a representative who will be the focal point for all communication with the Business Partner relative to this project and who will have the authority to act on the customer’s behalf in matters regarding this project.
- Designating operations personnel to work with the Business Partner as appropriate.
- Providing all product data in the requested format.
- Providing all data and information required for implementation.
- Providing a suitable workspace with Internet and telephone access for the services specialists while working on the customer premises.
- Providing user IDs, passwords, and IP addresses as required, enabling the Business Partner to perform the service.

> **Note:** Add any client responsibilities that you need to assign in order to complete a successful delivery of your service.

Staffing estimates

The project will be performed with one Tivoli Monitoring specialist who will be on site as required by the project schedule. We will also provide project management services, and will be on site at the end of the project for its formal closure. The project is estimated to be performed within <x> working days. This is <x> man days of effort in total.

We expect that we will need a single member of your staff working with us throughout this time who will also perform any mediation role required between us and any other required technical resources within your computer operation. This would be five man days in total.

> **Note:** You may want to revise these estimates if you want to provide extra services, such as education.

Testing

The testing of the solution will be done through the use of the infrastructure, to ensure that the resources are successfully being monitored.

Testing will be complete when we have successfully performed the following:

- Deployed agents of each appropriate type on each platform type.
- Ensured that each agent has successfully connected to the Tivoli Monitoring Server, and is available in the Tivoli Enterprise Portal.
- Ensured that situations on each agent type are being evaluated correctly, and appropriate actions are taken place.
- Ensured that events are successfully forwarded to Tivoli Enterprise Console or OMNIbus, and 2-way synchronization is also working.

Deliverables

At the end of this engagement, you will have the following:

- One Tivoli Monitoring environment with all required server side software installed
- One Tivoli Monitoring Agent of each type deployed and configured
- Documentation for the deployed environment

Completion criteria

The completion criteria for this project are as follows:

- The successful completion of all the tests
- The delivery of the solution documentation

Abbreviations and acronyms

BASH	Bourne Again SHell
CCMDB	Change and Configuration Management Database
CEC	Common Event Console
COBIT	Control Objectives for Information and related Technology
DNS	Domain Name System
EIB	Enterprise Information Base
EIF	Event Integration Facility
ERP	Enterprise Resource Monitoring
eTOM	Telecom Operations Map
EULA	End User License Agreement
FQDN	Fully Qualified Domain Name
GSKIT	Global Security ToolKit
GUI	Graphical User Interface
HIPPA	Health Insurance Portability and Accountability Act
IBM	International Business Machines Corporation
ISM	IBM Service Management
ITCAM	IBM Tivoli Composite Application Management
ITES	IBM Technical Education Services
ITIL	IT Infrastructure Library
ITM	IBM Tivoli Monitoring
ITSO	International Technical Support Organization
JMX	Java Management Extensions
Monitoring agent	Tivoli Enterprise Monitoring Agent
Monitoring server	Tivoli Enterprise Monitoring Server
MTEMS	Manage Tivoli Enterprise Monitoring Services
MTTR	Mean-Time-To-Resolution
NFS	Network File System
NIC	Network Interface Card
NIS	Network Information Service
LDAP	Lightweight Directory Access Protocol
OPAL	Open Process Automation Library
PAC	Proactive Analysis Component
Perfmon	Performance Monitor
Portal	Tivoli Enterprise Portal
Portal server	Tivoli Enterprise Portal Server
REXEC	Remote Execution
RM	Resource Model
RSH	Remote Shell
SMB	Server Message Block
SNMP	Simple Network Management Protocol
S&P	Summarization and Pruning agent
SSH	Secure Shell
SSL	Secure Sockets Layer
SOAP	Simple Object Access Protocol
TCSH	TC-Shell
TEC	Tivoli Enterprise Console
TMR	Tivoli Management Region
UA	Universal Agent
WMI	Windows Management Instrumentation
WPA	Warehouse Proxy agent

Related publications

The publications listed in this section are considered particularly suitable for a more detailed discussion of the topics covered in this book.

IBM Redbooks

For information about ordering these publications, see “How to get Redbooks” on page 388. Note that some of the documents referenced here may be available in softcopy only.

- *Deployment Guide Series: IBM Tivoli Monitoring Express Version 6.1,* SG24-7217
- *IBM Tivoli Monitoring: Implementation and Performance Optimization for Large Scale Environments,* SG24-7443

Other publications

These publications are also relevant as further information sources:

- *IBM Tivoli Monitoring Version 6.2.0 Administrator’s Guide,* SC32-9408
- *IBM Tivoli Monitoring Version 6.2.0 Agent Builder User's Guide*, SC32-1921
- *IBM Tivoli Monitoring Version 6.2.0 Command Reference,* SC23-6045
- *IBM Tivoli Monitoring Version 6.2.0 Installation and Setup Guide,* GC32-9407
- *IBM Tivoli Monitoring Version 6.2.0: Upgrading from V5.1.2*, GC32-1976

Online resources

These Web sites are also relevant as further information sources:

- Agent Builder Demonstration Video

  `ftp://www.redbooks.ibm.com/redbooks/SG247444/itm62.html`
- IBM education and training Web site

  `http://www-306.ibm.com/software/tivoli/education/`

- IBM Tivoli Monitoring product Web site

  http://www-306.ibm.com/software/tivoli/products/monitor/
- Java for AIX Web site

  http://www-128.ibm.com/developerworks/java/jdk/aix/service.html
- Microsoft downloads Web site

  http://www.microsoft.com/downloads
- OPAL Web site

  http://www.ibm.com/software/tivoli/opal
- Oracle Web site

  http://www.oracle.com
- Platform support matrix for Tivoli Products

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

How to get Redbooks

You can search for, view, or download Redbooks, Redpapers, Technotes, draft publications and Additional materials, as well as order hardcopy Redbooks, at this Web site:

ibm.com/redbooks

Help from IBM

IBM Support and downloads

ibm.com/support

IBM Global Services

ibm.com/services

Index

Redbooks

Deployment Guide Series: IBM Tivoli Monitoring V6.2

(0.5" spine)
0.475"<->0.875"
250 <-> 459 pages

Deployment Guide Series: IBM Tivoli Monitoring V6.2

Deployment best practices, Agent Builder, and ITM 5.x migration

Case studies and proof of concept scenarios

Sales engagement planning

IBM Tivoli Monitoring Version 6.2 is a powerful monitoring product from IBM, that is easily customizable and provides real-time and historical data that enables you to quickly diagnose and solve issues through the IBM Tivoli Enterprise Portal component. This common, flexible, and easy-to-use browser interface helps users to quickly isolate and resolve potential performance problems.

This IBM Redbooks publication presents a deployment guide for IBM Tivoli Monitoring V6.2. We cover planning, installing, and configuration of IBM Tivoli Monitoring V6.2 for small, medium, and large environments. In addition, we provide some case studies, such as IBM Tivoli Monitoring V5.x migration, event management integration, and Agent Builder.

Agent Builder is a very powerful tool that you can use to develop your own monitoring agents. In order to show you how this tool can be used in a real life scenario, we have created a 30 minute video that you can launch from the ITSO Web site.

We have also added an appendix that discusses IBM Tivoli Monitoring sales engagement planning for Business Partners and Solution Developers.

The target audience for this documentation is IT Specialists and Business Partners who will be working on IBM Tivoli Monitoring V6.2 implementations and proof of concepts.

Redbooks

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

SG24-7444-00 ISBN 0738485527