IBM Tivoli Composite Application Manager for Internet Service Monitoring agent 7.4.0 Fix Pack 2 IF 04

Installation and Configuration Guide

0000-0000-00

Contents

Tables

Chapter 1. Introduction

The IBM Tivoli Composite Application Manager for Internet Service Monitoring agent (product code IS) consists of several components which measure internet services and response times, and track transactions, enabling you to identify and isolate problems in your information technology environment. ITCAM for Internet Service Monitoring agent integrates with the Tivoli Enterprise Portal in IBM Tivoli Monitoring enabling you to manage your entire enterprise with a single user interface.

ITCAM for Transactions includes the following components:

- Internet Service Monitoring
- Response Time
- Transaction Tracking

Chapter 2. Overview of the agent

ITCAM for Internet Service Monitoring agent delivers a comprehensive, unified transaction tracking management system that runs on a single, consolidated infrastructure with a tightly integrated user interface. Because problem isolation in today's complex IT environments can often take hours or days and can result in lost time, lost revenue, and low customer satisfaction, ITCAM for Internet Service Monitoring agent helps you rapidly isolate problem components which speeds up diagnosis and service restoration before poor customer experiences can directly affect revenue.

ITCAM for Transactions offers the following benefits:

- Integrates with the Tivoli Enterprise Portal in IBM Tivoli Monitoring so you can manage the entire enterprise with a single user-interface and quickly navigate views. This integration means that you do not need to learn multiple tools with different user interfaces so you can experience a faster return on investment.
- Provides several components for measuring internet services and response times, and tracking transactions, so that you can identify any problems when they occur or even before they occur, and isolate the problems to a specific part of your IT environment. ITCAM for Transactions also integrates with IBM Tivoli diagnostic tools such as Tivoli Business Service Manager, ITCAM for Application Diagnostics, and Tivoli OMEGAMON XE so that you can potentially diagnose and analyze any problems and then hand the details to the appropriate specialist to take corrective action.
- Provides the Application Management Console, so you can have an immediate view of your entire enterprise as a physical mapping of platforms, systems, monitoring agents, and monitored resources that shows operational status with links to the underlying component workspaces.
- Reduces the costs for IT lifecycle operations, support, and development through proactive, real-time, and automated problem resolution by providing an end-to-end view of services, transactions, and associated resources across platforms and subsystems.
- Reduces the time between problem identification and problem resolution by automatically identifying problem components in a transaction.
- Increases revenue and customer satisfaction by maintaining service level agreements.
- Increases the performance and availability of business-critical applications, including portal and service-oriented architecture (SOA) based technologies.
- Provides role-based user interfaces so you can provide the right level of information to the right user for help with quick problem identification, seamless hand off, and problem resolution.
- Integrates performance, availability, and problem identification information with several other IBM Tivoli products to help deliver even greater value. You can use response time information with the following products:
  - – IBM Tivoli Performance Analyzer to identify trends.
  - IBM Tivoli Business Service Manager to identify the impact to overall business services.
  - IBM Tivoli Provisioning Manager to take provisioning actions to help prevent SLA breaches.
  - IBM Tivoli Monitoring to determine if resource monitors (for CPU, memory, disk utilization, and so on) reveal the cause of problems.
  -

ITCAM for Transactions includes the following components:

- Internet Service Monitoring, which provides the tools to identify availability and response time problems and monitors to test the availability and performance of various internet services, including monitoring web sites, web-based e-commerce applications, and electronic mail (as well as the underlying services such as DNS, LDAP, and SMTP on which those services rely).

- v Response Time, which focuses on the end user experience, both real and simulated, by monitoring web transactions, playing back recorded scripts, and real user desktop experiences. Response Time includes the following components:
  - Application Management Console and Application Management Configuration Editor
  - Robotic Response Time
  - Web Response Time
- Transaction Tracking, which delivers an end-to-end view of response times across systems to quickly help isolate the cause of response time and availability problems. Transaction Tracking includes the following components:
  - Transaction Collector
  - Transaction Reporter
  - Transaction Tracking API
  - CICS TG Transaction Tracking
  - CICS TXSeries Data Collector
  - Data Collector for WebSphere Message Broker
  - MQ Tracking
  - Tuxedo Tracking
  - WASTT
  - Transaction Tracking for z/OS
    - Transaction Tracking for z/OS
    - CICS TG Transaction Tracking
    - CICS Tracking
    - IMS Tracking
    - MQ Tracking for z/OS
  - Transaction Tracking also integrates with:
    - Web Response Time
    - Robotic Response Time
    - ITCAM for Application Diagnostics
    - ITCAM for J2EE
    - ITCAM for SOA
    - Tivoli Business Service Manager
    - Optim Performance Manager
    - WebSphere Application Server
    - IBM HTTP Server
    - - IBM Tivoli OMEGAMON XE for CICS
    - IBM Tivoli OMEGAMON XE for IMS
    - IBM Tivoli OMEGAMON XE for Messaging
    - Monitoring Agent for Microsoft .NET Framework
    - Monitoring Agent for Microsoft Internet Information Services
    - Monitoring Agent for Active Directory

Integration with IBM Tivoli Monitoring

IBM Tivoli Monitoring is the base software for ITCAM for Internet Service Monitoring agent. IBM® Tivoli® Monitoring provides a way to monitor the availability and performance of enterprise systems from one or

several designated workstations. It also provides useful historical data for tracking trends and troubleshooting system problems.

You can use IBM Tivoli Monitoring to do the following tasks:

- Monitor for exception conditions on the systems that you are managing by using predefined situations or custom situations
- Establish performance thresholds
- Investigate the causes leading to an exception condition
- Gather comprehensive data about system conditions
- Perform actions, schedule work, and automate manual tasks
- Using the operating system agents:
  - Provide basic performance data about operating systems and hardware to Tivoli Enterprise Management Agents
  - Provide remote functions for the Tivoli Enterprise Management Agents
  - Provide Proxy Agent Services

The following table describes the main components of ITCAM for Internet Service Monitoring agent:

Table 1. Tivoli Monitoring and ITCAM for Transactions integration

Component	**Description**
Tivoli Enterprise Portal Tivoli Enterprise Portal Server	The Tivoli Enterprise Portal Server enables retrieval, manipulation, and analysis of data from the agents. The server is between the client and the Tivoli Enterprise Monitoring Server (monitoring server). The Tivoli Enterprise Portal client is a Java-based user interface for viewing and monitoring your enterprise. It provides two modes of operation: desktop and browser. The Tivoli Enterprise Portal provides a consolidated view of the monitored environment so you can monitor and resolve performance issues. You can view your enterprise by using default physical views or by using custom created logical views in the Navigator
Tivoli Enterprise Monitoring Server	Provides the collection and control point for alerts received from the monitoring agents and collects their performance and availability data. There are 2 types of monitoring servers: hub and remote.
Tivoli Data Warehouse	Stores historical data collected from monitoring agents. The data warehouse is located on a DB2®, Oracle, or Microsoft SQL database. To collect information to store in this database, you must install the Warehouse Proxy agent. To perform aggregation and pruning functions on the data, install the Warehouse Summarization and Pruning agent.

Table 1. Tivoli Monitoring and ITCAM for Transactions integration (continued)	
Component	**Description**
Internet Service Monitoring agents and monitors	Provides the tools to identify availability and response time problems and monitors to test the availability and performance of various internet services, including monitoring websites, web-based e-commerce applications, and electronic mail (as well as the underlying services such as DNS, LDAP, and SMTP on which those services rely).
Response Time	Focuses on the end user experience, both real and simulated, by monitoring web transactions, playing back recorded scripts, and real user desktop experiences. Response Time includes the following components: • Application Management Console agent and Application Management Configuration Editor - enable you to define and configure the applications and transactions that you want to monitor. By applying common profile configurations across the environment, you can deploy monitoring in large-scale environments more efficiently • Robotic Response Time - reports the results of simulated transactions (robotic scripts) so you can be proactive in managing availability and performance of your applications and identify bottlenecks before they impact customer satisfaction. • Web Response Time - reports real-user response time of web applications that can be broken down into browser (client) time, network time, server time, load time, and resolve time. Web Response Time monitors TCP traffic and detects components and protocols. It functions as an Aggregation agent for agentless tracking.

Table 1. Tivoli Monitoring and ITCAM for Transactions integration (continued)	
Component	**Description**
Transaction Tracking	Delivers an end-to-end view of your topology and response times across systems to quickly help isolate the cause of response time and availability problems. Transaction Tracking includes the following components: • Transaction Reporter - collects and stores the aggregated data from an Aggregation agent, such as the Transaction Collector and Web Response Time, and sends this data to the Tivoli Enterprise Portal workspaces. • Transaction Collectors - store the tracking data from multiple Data Collector plug-ins and compute aggregates • Transaction Tracking API - is installed on each data collector and sends events and tracking information to Transaction Tracking. • Data Collector plug-ins - monitor traffic for specific applications and by using the Transaction Tracking API send this information to the Transaction Collectors. • Custom ARM applications - your own custom application that you can program to send events and provide tracking information to Transaction Tracking by using the Transaction Tracking API.
Aggregation agents	Agents that store the tracking data from monitors or Data Collector plug-ins, and compute aggregates for use by the Transaction Reporter. Aggregation agents include the Transaction Collector and Web Response Time (T5) agents.

For more information about how to use IBM Tivoli Monitoring and the Tivoli Enterprise Portal, see the publications available from IBM Tivoli Monitoring Information Center

Integration with other products

IBM Tivoli Monitoring and the monitoring agents integrate with other products.

The following table shows how components integrate with IBM Tivoli Monitoring.

Table 2. How components integrate with IBM Tivoli Monitoring	
Product	**Description**
Change and Configuration Management Database	Provides an enterprise-ready platform for discovering and storing deep, standardized data on configurations and change histories to help integrate people, processes, information, and technology.

Table 2. How components integrate with IBM Tivoli Monitoring (continued)

Product	Description
IBM Tivoli Business Systems Manager (TBSM) (Later versions renamed to IBM Tivoli Business Service Manager)	Manages real-time problems in the context of the business priorities for an enterprise. Business systems typically span web, client-server, or host environments and are made of many interconnected application components; they rely on diverse middleware, databases, and supporting platforms. TBSM provides customers a single point of management and control for real-time operations of end-to-end business systems management. You can graphically monitor and control interconnected business components and operating system resources from one single console and give a business context to management decisions. The software helps users manage business systems by understanding and managing the dependencies between business systems components and their underlying infrastructure. ITCAM for Transactions can be integrated with TBSM by using Omnibus. Situation events from Transaction Tracking can be forwarded from IBM Tivoli Monitoring to IBM IBM Tivoli Netcool/OMNIbus for display in TBSM.View these in TBSM by navigating to **Availability** > **Service Availability**. In the Service Tree, select **Imported Business Services** > **Transactions Business Activities** to display Transaction Tracking information. When you install Integration support by using the installation media provided with this release, you can access a new view of the data from Response Time and Transaction Tracking monitoring agents.
Tivoli Enterprise Management Agent (monitoring agents)	An IBM Tivoli Monitoring agent that is built on the IBM Tivoli Monitoring infrastructure. Tivoli Enterprise Management Agents connect to the Tivoli Enterprise Monitoring Server by using IPv4 or IPv6. Some configuration is required for IPv6. See the latest IBM Tivoli Monitoring Information Center for further information.

Table 2. How components integrate with IBM Tivoli Monitoring (continued)	
Product	**Description**
IBM Tivoli Monitoring (Tivoli Monitoring)	Provides monitoring for system level resources, detects bottlenecks and potential problems, and automatically recovers from critical situations to free system administrators from manually scanning extensive performance data during problem resolution. Upon notification of a poorly performing transaction component, you can launch either of the following products: • The Tivoli Enterprise Portal integrates and consolidates system monitoring end-to-end. The Tivoli Enterprise Portal provides a console from which you can monitor host and distributed systems. You can customize the information that you see in the Tivoli Enterprise Portal for your enterprise. See the IBM Tivoli Monitoring documentation for information about how to use the Tivoli Enterprise Portal. • Tivoli Data Warehouse enables you to drill down to a lower level of a transactions and historical data, and enables you to identify issues such as poorly configured systems. With the addition of products such as IBM Tivoli Monitoring for Databases, IBM Tivoli Monitoring for Web Infrastructure, and IBM Tivoli Monitoring for Business Integration, you can further diagnose infrastructure problems and, in many cases, resolve them before they affect the performance of business transactions

About Internet Service Monitoring

The information gathered and processed by Internet Service Monitoring enables you to determine whether a particular service is performing adequately, identify problem areas, report service performance measured against Service Level Agreements (SLAs), and forward performance data to IBM Tivoli Monitoring, IBM Tivoli Composite Application Manager for Transactions, and other event management tools such as IBM Tivoli Netcool/OMNIbus.

Internet Service Monitoring works by emulating the actions of a real user. For example, the HTTP monitor tries to access particular web pages, then measures how well the HTTP service performed. The data recorded by the monitor provides an immediate indication of the status of the HTTP service to the service operators, and can also be used to provide reports on service performance.

Internet Service Monitoring architecture

The core components of the Internet Service Monitoring architecture are the Internet service monitors.

The Internet service monitors regularly poll or test Internet services to check their status. The test results generate data for SLA evaluation, reporting, and alert generation. Internet Service Monitoring can monitor the protocols.

DHCP	ICMP	RADIUS	SNMP
Dial - deprecated in ITCAM for Transactions V7.3	IMAP4	RPING	SOAP
DNS	LDAP	RTSP	TCPPort
FTP	NNTP	SAA	TFTP
HTTP	NTP	SIP	WMS - deprecated in ITCAM for Transactions V7.3
HTTPS	POP3	SMTP	Combinations of the other protocols by using TRANSX

The Internet Service Monitoring components are:

Monitors
Test the specific Internet services and forward the test results to the Databridge. They emulate the actions of a real user of the service. For example, the HTTP monitor periodically attempts to access a web page by emulating requests that a web browser would usually send when a user visits the page. It generates an event containing the results of the test (including status information) which is sent to the Databridge.

Monitors are distinguished from IBM Tivoli Netcool/OMNIbus probes by their polling functions. Probes connect to an event source to acquire the event data that it generates, while monitors actively poll or test services at regular intervals by injecting transactions or queries into the target service, and generating performance evaluation data.

Databridge
Acts as the communications bridge between the monitors, the IBM Tivoli Netcool/OMNIbus ObjectServer, and the Internet service monitoring agent. The Databridge receives the results of service tests performed by the monitors and converts this data into different formats for processing by the ObjectServer and the monitoring agent. The Databridge can also generate Host file system Internet service monitoring agent Event list Databridge Alerts Datalogs Results Polls Results Events IBM Tivoli Netcool/OMNIbus ObjectServer IBM Tivoli Monitoring Events Results ObjectServer module Datalog module IBM Tivoli Monitoring module Monitors Internet services HTTP, FTP, ... Internet Service Monitoring Figure 3. Internet Service Monitoring architecture Chapter 1. Introduction 9 XML datalogs that you can use for archiving or simple reporting purposes. Detailed reporting is available within IBM Tivoli Monitoring through workspace.

Internet service monitoring agent
Converts test results into the format required by IBM Tivoli Monitoring.

ObjectServer module
Converts events into alerts containing SLA and performance data and sends these alerts to the IBM Tivoli Netcool/OMNIbus ObjectServer. IBM Tivoli Netcool/OMNIbus users can then view service status information in the Event List. IBM Tivoli Netcool/OMNIbus ObjectServer and the Event List are part of IBM Tivoli Netcool/OMNIbus and are not installed with Internet Service Monitoring.

Datalog module
Converts test results to XML and then sends this information to a host file system for archiving or simple reporting purposes. The XML is useful for customers who have developed their own reporting tools and want to continue working with these tools.

IBM Tivoli Monitoring module
Sends results to the Internet service monitoring agent that uses a mapping file to convert the results into the format required by IBM Tivoli Monitoring for reporting in workspaces.

Chapter 3. Planning your ITCAM for Transactions installation

Before installing ITCAM for Transactions, you must plan what you want to monitor, which components to use, and where to install these components in your unique environment.

This section provides general information. For further information, see ITCAM for Transactions Planning and Deployment Best Practices.

Planning to install Internet Service Monitoring

Internet Service Monitoring can be installed on AIX®, Linux®, Solaris, UNIX, and Windows systems.

Hardware and software requirements

Internet Service Monitoring is available on a range of operating systems.

See the Supported operating systems for Internet Service Monitoring in the Prerequisites pages of the relevant ITCAM for Transactions Information Center for further information.

Installation prerequisites

Before installing Internet Service Monitoring, ensure that the target environment includes the list of required products, that they are configured, and that you have administrator access to their host computers.

Important: On Windows systems, install agents using a local Administrator account rather than a domain account, such as an account defined by Active Directory. If the default Administrator account is not available, create a new local user account and add that account to the local Administrators' group. You can then install agents using the new local user account.

Installation onto an IBM Tivoli Monitoring environment requires the following products. See the latest Prerequisite information in the ITCAM for Transactions Information Center for the required versions:

- Tivoli Enterprise Monitoring Server. Obtain the Tivoli Enterprise Monitoring Server IP address or Hostname before installation.
- Tivoli Enterprise Portal Server.

  If Tivoli Enterprise Portal Server uses Microsoft SQL Server 2000 as its database, you must manually create a user for that database with name `kis`, with roles `DB Creators` and `Bulk Insert Administrators`, and with access privileges `master = public, db_datareader, db_datawriter` and `teps = public, db_datareader, db_datawriter`.

  If Tivoli Enterprise Portal Server uses Microsoft SQL Server 2005 or Microsoft SQL Server 2008 as its database, add a **`kis`** schema to your Microsoft SQL Server Tivoli Enterprise Portal Server database before using the Internet Service Monitoring configuration tool in the Tivoli Enterprise Portal:

  1. Open Microsoft SQL Server Management Studio.
  2. Navigate to **Databases** > **teps** > **Security**.
  3. Right click **Schemas** and select **New Schema**.
  4. In the **General** tab, enter the following values:
     - **Schema name**: `kis`
     - **Schema owner**: `teps`
  5. In the **Permissions** tab, enter the following values:
     - **Database**: `teps`
     - **Schema name**: `kis`

- **Users or roles**: `[teps]`
- **Explicit permissions for teps**: Grant permissions for Alter, Control, Delete, Execute, Insert, References, Select, Update

6. Restart the Tivoli Enterprise Portal client.

- Tivoli Enterprise Portal.
- Tivoli Enterprise Management Agent Framework. If you are installing on 64-bit Windows, UNIX, or Linux systems with IBM Tivoli Monitoring V6.3.0.1 or later components installed, install the 32-bit Tivoli Enterprise Management Agent Framework from the IBM Tivoli Monitoring installation media *before* installing ITCAM for Transactions agents.
- Optional - Tivoli Data Warehouse and Summarization and Pruning Agent (equivalent version for IBM Tivoli Monitoring).

If you are installing Internet Service Monitoring purely as an event source for an IBM Tivoli Netcool/OMNIbus ObjectServer, only IBM Tivoli Netcool/OMNIbus version 7.3.0 is supported. Before performing the installation, obtain the name of the target ObjectServer, for example `NCOMS`, the IP address or host name of the computer hosting that ObjectServer, and the port on which the ObjectServer listens.

Installation considerations

Before installing Internet Service Monitoring consider how you want to deploy the product, the size of the resources needed, the scalability of the Internet service monitors, and whether you require historical reporting.

Planning deployment

If you want to use the graphical configuration, management, and reporting features of Internet Service Monitoring, you must install it into an IBM Tivoli Monitoring environment. This environment can be fully distributed. If you plan to use the product purely as an event source for IBM Tivoli Netcool/OMNIbus, IBM Tivoli Monitoring is not required.

Internet Service Monitoring can be installed onto a stand-alone system, onto the same system as the IBM Tivoli Monitoring environment (if installed on a single system), or onto the same system as any other IBM Tivoli Monitoring element in a distributed environment.

Internet Service Monitoring can be installed with any combination of the following:

- Tivoli Data Warehouse (for reporting of long term historical data)
- Summarization and Pruning Agent (for reporting of long term historical data with Tivoli Data Warehouse)
- Tivoli Enterprise Monitoring Server
- Tivoli Enterprise Portal Server
- Tivoli Enterprise Portal
- IBM Tivoli Netcool/OMNIbus (for use with IBM Tivoli Netcool/OMNIbus Event List)

Note: You can install Internet Service Monitoring at multiple sites for use with a single IBM Tivoli Monitoring environment.

Deployment scenarios

Internet Service Monitoring can be deployed in a range of different network infrastructures.

Three possible deployment scenarios for Internet Service Monitoring on service provider network infrastructures are described. Also provided are guidelines on the size and scale of the deployment. These factors are important because service monitoring activities use network, disk, and database resources.

Deployment within an ISP infrastructure

Deploying Internet Service Monitoring outside the Internet Service Provider (ISP) firewall on the De-Militarized Zone (DMZ) LAN, enables monitoring of Internet services inside and outside the firewall.

#unique_14/unique_14_Connect_42_deploy_isp on page 13 shows a sample Internet Service Monitoring deployment in a simple ISP infrastructure.

Internet Service Monitoring is installed outside the ISP firewall on the De-Militarized Zone (DMZ) LAN. This installation enables the monitors to emulate one of the customers for the ISP. Monitors installed on the DMZ LAN monitor Internet services inside or outside the firewall. For example, the HTTP monitor might monitor web pages served from the ISP Services LAN behind the firewall, and other web pages located elsewhere on the Internet through Router A which connects the DMZ LAN to the Internet.

Internet Service Monitoring sends results through the firewall and Router B to IBM Tivoli Monitoring, which is connected to the Back Office LAN. From there, operators manage all Internet services and infrastructure in workspaces. Internet Service Monitoring also sends alerts through the firewall and Router B to IBM Tivoli Netcool/OMNIbus. IBM Tivoli Netcool/OMNIbus is connected to the Back Office LAN. From there, operators view the Event List and manage any problems.

Deployment within an MNS provider infrastructure
Deploying Internet Service Monitoring outside the Managed Network Service (MNS) firewall on the De-Militarized Zone (DMZ) LAN, enables monitoring of Internet services inside the firewall.

Internet Service Monitoring is installed outside the firewall for the MNS provider on the DMZ LAN. From outside the firewall, the monitors connect to customer networks to monitor their services.

Internet Service Monitoring sends results through the firewall to IBM Tivoli Monitoring. From there, operators view the results in workspaces.

Internet Service Monitoring also sends alerts through the firewall to IBM Tivoli Netcool/OMNIbus. From there, operators view the event list and manage any problems.

Deployment within a distributed ISP infrastructure
Many Internet Service Providers (ISPs) and large corporate intranet service providers use a distributed infrastructure to reduce WAN requirements and increase server performance. In this situation Internet Service Monitoring is installed within each Point Of Presence (POP).

Service providers can deploy Internet Service Monitoring to monitor the distributed services that they supply to their corporate customers.

Internet Service Monitoringis installed within each POP. Service monitor traffic, such as polls and responses, between the POPs are sent to IBM Tivoli Monitoring. From there, operators view the results in workspaces. Service monitor traffic is also sent to IBM Tivoli Netcool/OMNIbus. From there, operators view the event list and manage any problems.

Fault-tolerant deployment
The simplest configuration providing fault-tolerant operation is to create two separate Internet Service Monitoring installations, and distribute profiles to both installations.

Both installations then perform identical monitoring tasks, so the monitoring operations are duplicated. Performance data (events and test results) are also duplicated. This type of installation is suitable for disaster recovery requirements.

Note: The Internet service monitors and the ObjectServer module of the Databridge implement the store and forward features of the IBM Tivoli Netcool/OMNIbus Probe API. These features prevent the loss of performance data in the case of network connectivity loss or component failure.

Sizing guidelines
Service monitoring activities use network, disk, and database resources. For this reason, guidelines are provided to assist you with sizing and scaling of the Internet Service Monitoring deployment.

The formulas presented here are intended as a guide only. The exact requirements might vary according to operating environment and service monitoring application.

Network bandwidth use
Monitoring activities and forwarding of events to a IBM Tivoli Netcool/OMNIbus ObjectServer use network bandwidth. The bandwidth that is required depends on the size of the data, number of monitoring

requests, and frequency of the requests. Guidelines are provided to assist with estimating the required network bandwidth.

Monitor traffic

Note: The values described for bandwidth usage represent an upper limit, real values are likely to be lower.

HTTP monitor tests commonly comprise a large proportion of the incoming traffic to Internet Service Monitoring. A `GETALL` request to download a web page and its components, assuming a total size of 20 Kb size, requested every 10 minutes corresponds to network bandwidth use of 266.67 bps. 10,000 requests every 10 minutes, which is the limit of the HTTP monitor performance capability, corresponds to bandwidth use of 2.67 Mbps.

Tip: The more commonly used HTTP `GET` and `HEAD` requests use less bandwidth than `GETALL` requests.

ObjectServer events

The size of each HTTP event sent from the Databridge to a IBM Tivoli Netcool/OMNIbus ObjectServer, is approximately 2Kb. Running one HTTP monitor test every 10 minutes corresponds to network bandwidth use of 26.67 bps, outgoing from Internet Service Monitoring. 10,000 tests every 10 minutes corresponds to bandwidth use of 0.267 Mbps.

Monitor scalability and performance

The scalability and performance of Internet service monitors directly affects the volume of services that you can monitor.

Scalability and performance depend on a number of factors:

- Access speed of the disk system used by the monitors
- Response times of the monitored services
- Number of monitor threads running concurrently
- Time between tests
- Number of profiles
- Monitor poll interval

The monitoring environment determines the disk speeds and service response times. Monitor properties control concurrent threading and the time between tests. You control the number of profiles and the monitor polling intervals when you configure the monitors through the Internet Service Monitoring user interface in the Tivoli Enterprise Portal.

Monitor property settings

Internet service monitor properties include settings for the maximum number of threads, the interval at which the monitor spawns threads, and the maximum size of the event queue for the monitor. Ensure that these settings are optimized.

Table 3 on page 14 shows the optimal settings for the `MaxCCA`, `Pause`, and `QSize` properties.

Table 3. Optimal settings for Internet service monitor properties

Property	Description	Best setting
`MaxCCA` *n*	Sets the maximum number of threads running concurrently. The ICMP monitor does not provide this property because it is single-threaded.	`50` for high-volume polling (more than 500 profile elements) `10` for low-volume polling

Table 3. Optimal settings for Internet service monitor properties (continued)		
Property	**Description**	**Best setting**
`Pause n`	Sets the interval (in milliseconds) at which the monitor spawns threads. Setting it to a higher value, such as 100 or more, causes the monitor to spawn threads more slowly.	`50` for high-volume polling (more than 500 profile elements) `100` for low-volume polling
`QSize n`	Set the maximum size of the monitors event queue on disk.	`10` MB for most situations. In larger environments, increase this value for each monitor by 1 MB per 1000 elements.

Poll intervals

The number of poll intervals affects the response times. A guideline is provided to help with choosing the appropriate interval.

You define the poll interval when you create profile elements. Use the following formula as a guide:

```
minimum poll interval = number of profile elements × average response time / MaxCCA
```

The number of profile elements configured for a monitor determines the total number of tests performed by the monitor. The average response time varies according to the monitoring environment, so when selecting the poll interval, choose a value appropriate to the application environment. In the worst case, if the application fails to respond then the average response time is the timeout value set for the monitored element.

Note: If you use history collection, use the same poll intervals as the history collection intervals.

Response times in LAN monitoring environments

In LAN monitoring environments, server tests run over high-speed networks. Therefore the response times of services are low, typically less than one second.

The poll interval is also affected by data logging functions that involve a higher number of disk access operations. If you use monitors as data sources for only IBM Tivoli Netcool/OMNIbus and IBM Tivoli Monitoring, and you do not use the datalogs as storage for simple reporting or archiving results, then monitor data logging is not necessary and you can run the monitors without data logging. This condition permits shorter polling intervals of up to one half of the value indicated by the polling interval formula.

Response times in remote monitoring environments

In remote monitoring environments, where service tests run over a WAN or an Internet connection, the response times are less predictable, and it is the network response time, instead of monitor performance, that limits the poll interval. Use polling intervals that allow enough time for responses to be received before the next test starts.

Historical reporting

The Internet service monitoring workspaces in Tivoli Enterprise Portal show the most recent test results. By default, these results are the results of the last hour. You can configure IBM Tivoli Monitoring to store the test results thus providing access to historical data for short-term or long-term reporting in the history workspaces.

Short-term data refers to data that is available for up to 24 hours. Long-term data refers to data that is available for an indefinite time.

Short-term data reporting

You can save the most recent test results for up to 24 hours to enable short-term historical reporting. Short-term historical data is collected and stored in binary files.

Use the History data collection feature in Tivoli Enterprise Portal to configure the collection of historical data. See the Administrator's Guide for information about configuring history collection.

Long-term reporting

You can save test results produced by the Internet service monitors indefinitely to enable long-term historical reporting. Long-term historical data is stored in the Tivoli Data Warehouse. Use the History data collection feature in Tivoli Enterprise Portal to configure the collection of historical data and the pruning and summarization of the data.

When you configure the history data collection, specify Internet service monitors as the product from which to collect data, the type of data to be collected, the collection interval, and the location of the collected data. In addition, specify when data is to be send from the collection location to the Tivoli Data Warehouse and configure the pruning and summarization of the data. See the *IBM Tivoli Monitoring Administrator's Guide* for detailed information about history data collection.

Note: You must have Configure History permission to see and use the History data collection feature.

Installation of support files

In addition to installing Internet Service Monitoring, you must install support files for the IBM Tivoli Monitoring components that are used by Internet Service Monitoring.

Support files add support information for the predefined workspaces and situations to the Tivoli Enterprise Portal, Tivoli Enterprise Portal Server, and Tivoli Enterprise Monitoring Server components of IBM Tivoli Monitoring. There is a support file for each of these components.

Support files must be installed on the same computer as the components they are supporting. For example, for Tivoli Enterprise Monitoring Server, install the support file on the same computer as Tivoli Enterprise Monitoring Server.

The support files are included on the product CD or downloaded from the IBM Passport Advantage® website http://www.ibm.com/software/howtobuy/passportadvantage/ as part of the product. You install the files by using the Internet Service Monitoring InstallShield Wizard.

If you intend to use Internet Service Monitoring purely as an event source for IBM Tivoli Netcool/OMNIbus, installing support files is not necessary.

Simplifying installation

To simplify installation, you can use self describing agents.

Using self-describing agents (SDA)

ITCAM for Transactions V7.4 and later supports self-describing agents (SDA). This function enables you to install Tivoli Enterprise Monitoring Server and Tivoli Enterprise Portal Server support files automatically when installing ITCAM for Transactions agents. This function is only supported on ITM IBM Tivoli Monitoring V6.2.3 and later.

The support files are included with the agent installation files. When an SDA-enabled agent connects to the Tivoli Enterprise Monitoring Server or Tivoli Enterprise Portal Server, it automatically pulls the Transaction Tracking support files from the computer on which the agent is installed and updates the Tivoli Enterprise Monitoring Server or Tivoli Enterprise Portal Server.

Before you can use SDA, it must be enabled for each agent that you want to install.

For IBM Tivoli Monitoring V6.3, to enable SDA for all agents, run the following command:

```
tacmd editSdaInstallOptions -t default -i on
```

For IBM Tivoli Monitoring V6.3, to enable SDA for a particular agent and specified version, run the following command in the system where

```
tacmd addSdaInstallOptions -t product_code -v 07400000
```

where *product_code* is the product code of the agent, such as IS for Internet Service Monitoring. For more information about product codes, see http://www01.ibm.com/support/docview.wss?uid=swg21265222

For IBM Tivoli Monitoring V6.2.3, to enable SDA for **all** agents, set the variable **KMS_SDA=Y** in the following file:

```
install_dir/config/hostname_ms_temsname.config
```

If you attempt to install Tivoli Enterprise Monitoring Server and Tivoli Enterprise Portal Server support automatically with an agent installation without enabling SDA, you will see an error similar to the following error in the agent log:

```
(518B678E.0004-10:kraaulog.cpp,755,"IRA_OutputLogMsg") Self-Describing Agent
 Register/Install failed with STATUS (1024/0x400) for PRODUCT "IS", with TEMS
 "HUB_TIVVM340", VERSION_INFO "product_vrmf=07400000;tms_package_vrmf=07400000;
tps_package_vrmf=07400000;
tpw_package_vrmf=07400000;
```

Note: If you use SDA to install Tivoli Enterprise Portal Server support automatically for the Application Management Console (T3) or Transaction Collector (TU) agents, restart the Tivoli Enterprise Portal Server to complete the installation

Note: : If you are using SDA with Transaction Reporter, reconfigure the Tivoli Enterprise Portal Server using the Manage Tivoli Enterprise Monitoring Services. This corrects some inconsistencies in the installation

For more information on SDA, see the IBM Tivoli Monitoring documentation, search for 'Enabling self-describing agent capability at the hub monitoring server'

Product codes

If you want to install individual components, or to perform operations from the command-line, you might need the product code for the component you want to work with.

The following table lists the product codes of the individual components that make up ITCAM for Transactions.

Table 4. ITCAM for Transactions product codes

Component	Subcomponent	Product code
Internet Service Monitoring		`is`
Response Time	Application Management Console	`t3`
	Client Response Time - deprecated	`t4`
	Web Response Time	`t5`
	Robotic Response Time	`t6`

Table 4. ITCAM for Transactions product codes (continued)		
Component	**Subcomponent**	**Product code**
Transaction Tracking	CICS TXSeries Data Collector	t7
	Transaction Collector	tu
	Transaction Reporter	to
	MQ Tracking	th
	WASTT	tj
	Data Collector for WebSphere Message Broker	k3
	MQ Application Activity Trace data collector	m0

Chapter 4. Installing Internet Service Monitoring

Internet Service Monitoring can be installed on AIX, Linux, Solaris, UNIX, and Windows systems.

The installation uses an InstallShield Wizard to install and configure Internet Service Monitoring. Additional installation and configuration steps relate to the Tivoli Enterprise Portal, Tivoli Enterprise Portal Server, and the Tivoli Enterprise Monitoring Server components of the IBM Tivoli Monitoring environment.

Installing Internet Service Monitoring on Windows systems

You can install IBM Tivoli Composite Application Manager for Transactions to a system that also has other IBM Tivoli Monitoring components installed, or you can install IBM Tivoli Composite Application Manager for Transactions to a separate system.

Before you begin

Before beginning the installation, ensure that you have read "Planning to install Internet Service Monitoring" on page 11 for information about hardware and software prerequisites, planning and deployment considerations, and any special limitations.

Procedure

To install the IBM Tivoli Composite Application Manager for Transactions agent to a separate, Windows based, system:

1. Log on as a user with administrative privileges.

   Important: On Windows systems, install agents using a local Administrator account rather than a domain account, such as an account defined by Active Directory. If the default Administrator account is not available, create a new local user account and add that account to the local Administrators' group. You can then install agents using the new local user account.
2. Insert the product DVD or download the product from the IBM Passport Advantage® website: http://www.ibm.com/software/howtobuy/passportadvantage/.
3. Launch the installation wizard by double-clicking the `setup.exe` file. The InstallShield Wizard starts.

   Tip: On Windows Server 2008 systems, if instead of the installer you see the following message, right-click the `setup.exe` file in the file explorer and select **Run as Administrator**.

   ```
   Your logon ID must have Administrator rights to install IBM Tivoli Composite
    Application Manager for Transactions
   ```
4. On the **Welcome** window, click **Next**.
5. If no IBM Tivoli Monitoring components are installed on this computer the **Prerequisites** window is displayed. Read the information and click **Next**.
6. On the **Install Prerequisites** window, options to ensure that you have the correct version of IBM GSKit or IBM Java™ are selected. Click **Next**. The required software is installed automatically.
7. On the **Software License Agreement** window, read the agreement and click **Accept**.
8. If you install to a computer that does not have other IBM Tivoli Monitoring components installed, the **Choose Destination Location** window with the default installation location is displayed. Change the location if required and click **Next**.
9. On the **User Data Encryption Key** window, enter your own unique encryption key and click **Next** then click **OK** in the summary window.

   Note: You are only required to supply an encryption key if the IBM GSKit is not already installed on the computer. Use the same key across the enterprise.

10. On the **Select Features** window, select **Tivoli Enterprise Monitoring Agents** and click **Next**. This selects the **Tivoli Enterprise Monitoring Agent Framework** and the **IBM Tivoli Composite Application Manager for Transactions agent**.

    Note: Tivoli Enterprise Monitoring Agents may already be selected if the framework or any agents are already installed. You must expand this feature and also select **IBM Tivoli Composite Application Manager for Transactions agent**.
11. On the **Agent Deployment** window, select **Internet Service Monitoring** if you want to deploy to a remote location by using the Tivoli Enterprise Monitoring Server and click **Next**.

    If you are installing locally, do not select any agents.

    See Chapter 6, "Working remotely," on page 55 for further information.
12. On the **Start Copying Files** window, review the settings and if correct, click **Next**. The files are then copied. A **Setup Status** window informs you about progress.
13. On the **Setup Type** window, select all configuration options and click **Next**.

    You can delay some configuration until after installation if required. The following steps assume that all configuration options are selected.
14. On the **Configuration Defaults for Connecting to a TEMS** window, specify the Tivoli Enterprise Monitoring Server connection information and click **OK**:
    a) Select **Connection must pass through firewall** if the agent and the Tivoli Enterprise Monitoring Server are on different sides of a firewall.
    b) Select **Protocol 1** and select a protocol from the list. Several types of protocols are available: IP.UDP (uses unsecured UDP communications), IP.PIPE (uses unsecured TCP communications), IP.SPIPE (uses SSL secure TCP communications), and SNA (uses SNA for mainframe components).
    c) If additional protocols are required, select **Protocol 2** and select an second protocol from the list.
    d) Do not select **Optional Secondary TEMS Connection**. You can set up the failover support for the component later. See the *IBM Tivoli Monitoring User's Guide* for further information.
    e) Click **OK**.
15. In the summary Configuration Defaults for Connecting to a TEMS window, check the information and click **OK**.

    These settings define communications between the agent and the Tivoli Enterprise Monitoring Server. The host name or IP address of the local computer are displayed unless the Tivoli Enterprise Monitoring Server has already been specified. Ensure that you enter the host name or IP address of the Tivoli Enterprise Monitoring Server in the **Hostname or IP address** field if it is installed on another computer. The default port number for the previously selected protocol is also displayed (IP.PIPE is 1918, IS.SPIPE is 3660).
16. On the **Internet Service Monitoring Configuration** window, if using IBM Tivoli Netcool/OMNIbus select **YES** and enter the host name or IP address of the IBM Tivoli Netcool/OMNIbus ObjectServer and its port number.

    Tip: If you are using IBM Tivoli Netcool/OMNIbus but want to configure the connection later, select **NO**. Configure the ObjectServer connection later using the Manage Tivoli Enterprise Monitoring Services.
17. Click **OK**. The system configures and starts IBM Tivoli Composite Application Manager for Transactions.
18. Read the README file and click **Finish**. The **Manage Tivoli Enterprise Monitoring Services** window is displayed.
19. Verify the installation and configuration by checking the **Status** column for IBM Tivoli Composite Application Manager for Transactions. The **Status** column should show **Started**.

Results
Installation is complete.

What to do next

You can now install the support files and configure the product components.

Tip: Reconfigure connection to the Tivoli Enterprise Monitoring Server after installation using the Manage Tivoli Enterprise Monitoring Services.

Installing Tivoli Enterprise Monitoring Server support manually on Windows systems

Install Tivoli Enterprise Monitoring Server (TEMS) support to the system on which Tivoli Enterprise Monitoring Server is installed. Installation of Tivoli Enterprise Monitoring Server support on Windows also adds the application support.

Before you begin

Before beginning the installation, ensure that you have read "Planning to install Internet Service Monitoring" on page 11 for information about hardware and software prerequisites, planning and deployment considerations, and any special limitations.

Tip: You can install Tivoli Enterprise Monitoring Server and Tivoli Enterprise Portal Server support automatically when you install each agent. Ensure that SDA is enabled to use this feature. See Using self-describing agents (SDA) for more information.

Procedure

1. Log on as a user with administrative privileges to the system running Tivoli Enterprise Monitoring Server.
2. Insert the product CD or download the product from the IBM Passport Advantage® website: http://www.ibm.com/software/howtobuy/passportadvantage/.
3. Launch the installation wizard by double-clicking the `setup.exe` file. The InstallShield Wizard starts.
4. Click **Next** on the **Welcome** window.
5. On the **Install Prerequisites** window, the appropriate IBM GSKit or IBM Java check box will be selected if required. Click **Next**.
6. On the **Software License Agreement** window, read the agreement and click **Accept**.
7. On the **Select Features** window, select **Tivoli Enterprise Monitoring Server** and click **Next**. Only those components installed on the system are listed.
8. On the **Agent Deployment** window, click **Next**.

   The agent deployment refers to the Internet Service Monitoring application which is assumed to be installed on a separate system.
9. On the **Start Copying Files** window, review the settings and if correct, click **Next**. The files are then copied. A **Setup Status** window informs you about its progress.
10. On the **Setup Type** window, make sure that all setup types are selected and click **Next**.
11. The **Tivoli Enterprise Monitoring Server Configuration** window displays default values. The **TEMS Type**, **TEMS Name** and **Protocol 1** are automatically detected. If required, you can specify a second protocol to be used as a backup. Four types of protocols are available: IP.UDP (uses unsecured UDP communications), IP.PIPE (uses unsecured TCP communications), IP.SPIPE (uses SSL secure TCP communications), and SNA (uses SNA for mainframe components).
12. Click **OK**.
13. If you have a hub Tivoli Enterprise Monitoring Server, the **Hub TEMS Configuration** window is displayed. The hub settings are automatically detected and depend on the protocol selected in the previous step. The detected settings are:
    - For IP.UDP, the host name or IP address and the Port number (or Port Pools) of the hub server.
    - For IP.PIPE settings, the host name or IP address and the Port number of the hub server (the default port number is 1918).

- For IP.SPIPE settings, the host name or IP address and the Port number of the hub server (the default port number is 3660).
- For SNA settings, the SNA network identifier for your location, the LU name for the monitoring server (this LU name corresponds to the Local LU Alias in your SNA Communications software), the name of the LU6.2 LOGMODE (default is CANCTDCS) and the transaction program name.

14. If you have a remote Tivoli Enterprise Monitoring Server, the **Remote TEMS Configuration** window is displayed. Type the name of the remote TEMS in the **Hostname or IP Address** field.
15. In either window, click **OK**.

    The **Add application support to the TEMS** window is displayed.
16. Select **On this computer** as the location to which the support file should be added and click **OK**.

    The **Select application support to add to the TEMS** window is displayed.
17. Select **Internet Service Monitoring plugin** and click **OK**.
18. Review the installation summary on the **Application support addition complete** window and click **Next**.
19. Read the README file and click **Finish**.

Results
Installation of Tivoli Enterprise Monitoring Server support is complete.

Installing Tivoli Enterprise Portal Server support manually on Windows systems

Install Tivoli Enterprise Portal Server (TEPS) support to the system on which Tivoli Enterprise Portal Server is installed.

Before you begin

Before beginning the installation, ensure that you have read "Planning to install Internet Service Monitoring" on page 11 for information about hardware and software prerequisites, planning and deployment considerations, and any special limitations.

Tip: You can install Tivoli Enterprise Monitoring Server and Tivoli Enterprise Portal Server support automatically when you install each agent. Ensure that SDA is enabled to use this feature. See Using self-describing agents (SDA) for more information.

Procedure

To install Tivoli Enterprise Portal Server support on Windows:

1. Log on as a user with administrative privileges.
2. Insert the product CD or download the product from the IBM Passport Advantage® website: http://www.ibm.com/software/howtobuy/passportadvantage/.
3. Launch the installation wizard by double-clicking the `setup.exe` file. The InstallShield Wizard starts.
4. Click **Next** on the **Welcome** window.
5. On the **Install Prerequisites** window, the appropriate IBM GSKit or IBM Java check box will be selected if required. Click **Next**.
6. On the **Software License Agreement** window, read the agreement and click **Accept**.
7. On the **Select Features** window, select **Tivoli Enterprise Portal Server** and click **Next**. Only those components installed on the computer are listed.
8. On the **Agent Deployment** window, click **Next**.

   The agent deployment refers to the Internet Service Monitoring application which is assumed to be installed on a separate system.
9. On the **Start Copying Files** window, review the settings and if correct, click **Next**. The files are then copied. A **Setup Status** window informs you about its progress.
10. On the **Setup Type** window, make sure that all setup types are selected and click **Next**.

11. On the **TEPS Hostname** window, enter the name of the Tivoli Enterprise Portal Server and click **Next**. The installation continues and a **Setup Status** window informs you of its progress.
12. If required, reconfigure the Tivoli Enterprise Monitoring Server connection information on the **Configuration Defaults for Connecting to a TEMS** window and click **OK**.

    Note: The **Configuration Defaults for Connecting to a TEMS** and the subsequent Configuration Defaults for Connecting to a TEMS summary window open only if the Tivoli Enterprise Monitoring Server is installed on the same system. See Chapter 5, "Configuring Internet Service Monitoring," on page 39 for details of the fields on these windows.
13. Read the README file and click **Finish**.

Results
Installation of Tivoli Enterprise Portal Server support is complete.

Installing Tivoli Enterprise Portal support on Windows systems

Install Tivoli Enterprise Portal (TEP) support to the system on which Tivoli Enterprise Portal is installed.

Before you begin

Before beginning the installation, ensure that you have read "Planning to install Internet Service Monitoring" on page 11 for information about hardware and software prerequisites, planning and deployment considerations, and any special limitations.

Procedure

To install Tivoli Enterprise Portal support on Windows:

1. Log on as a user with administrative privileges.
2. Insert the product CD or download the product from the IBM Passport Advantage® website: http://www.ibm.com/software/howtobuy/passportadvantage/.
3. Launch the installation wizard by double-clicking the `setup.exe` file. The InstallShield Wizard starts.
4. Click **Next** on the **Welcome** window.
5. On the **Install Prerequisites** window, the appropriate IBM GSKit or IBM Java check box will be selected if required. Click **Next**.
6. On the **Software License Agreement** window, read the agreement and click **Accept**.
7. On the **Select Features** window, select **Tivoli Enterprise Portal Desktop Client** and click **Next**. Only those components installed on the current system are listed.
8. On the **Agent Deployment** window, click **Next**.

   The agent deployment refers to the Internet Service Monitoring application which is assumed to be installed on a separate system.
9. On the **Start Copying Files** window, review the settings and if correct, click **Next**. The files are then copied. A **Setup Status** window informs you about its progress.
10. On the **Setup Type** window, make sure that all setup types are selected and click **Next**.
11. On the **TEPS Hostname** window, enter the name of the Tivoli Enterprise Portal Server and click **Next**. The installation continues and a **Setup Status** window informs you of the progress.

    Note: The Tivoli Enterprise Portal Server Hostname is automatically detected if the Tivoli Enterprise Portal Server is installed on the same system.
12. If required, reconfigure the Tivoli Enterprise Monitoring Server connection information on the **Configuration Defaults for Connecting to a TEMS** window and click **OK**.

    Note: The **Configuration Defaults for Connecting to a TEMS** and the subsequent summary window are only opened if the Tivoli Enterprise Monitoring Server is installed on the same system. See Chapter 5, "Configuring Internet Service Monitoring," on page 39 for details of the fields on these windows.
13. Read the README file and click **Finish**.

Results

Installation of Tivoli Enterprise Portal support is complete. If all other support files are installed, and the Internet service monitoring agent and Tivoli Enterprise Portal Server are reconfigured if required, you are ready to start Internet Service Monitoring.

Silent installation on Windows systems

Silent installation enables you to define the options for installing Internet Service Monitoring in an installation response file, then run the installation process from the command line without interactive input. This method is useful for performing repeated installations.

Before you begin

Before beginning the installation, ensure that you have read "Planning to install Internet Service Monitoring" on page 11 for information about hardware and software prerequisites, planning and deployment considerations, and any special limitations.

About this task

A sample installation response file, `silent.txt`, is available with the product installer. The file contains comprehensive instructions on how to modify and use it.

Procedure

To run a silent installation:

1. Open the installation response file in a text editor.
2. Uncomment and modify the installation options as required, and then save the file.
3. From a command prompt, change directory to the location of the installer, `setup.exe`, and execute the command:

   ```
   start /wait setup /z"/sfC:\temp\silent.txt" /s /f2"C:\temp\silent_setup.log"
   ```

   where:

   - `/z"/sf` specifies the name of the installation driver you have customized for your site. This file is required.
   - `/s` specifies a silent installation. No responses are displayed on the target installation computer during installation.
   - `/f2` specifies the name of the InstallShield log file. If you do not specify this parameter, a file called `Setup.log` is created in the same location as `setup.iss`.

     The installation log can be found in the installation target directory, such as `c:\IBM\Omegamon\Install`, or on the Windows boot drive root directory if the installation fails before the installation location is identified. In either case, the installation program must be able to create and write to this file.

Installing on Linux or UNIX systems

You can install Internet Service Monitoring to a system that also has other IBM Tivoli Monitoring components installed, or you can install Internet Service Monitoring to a separate system.

Before you begin

Before beginning the installation, ensure that you have read "Planning to install Internet Service Monitoring" on page 11 for information about hardware and software prerequisites, planning and deployment considerations, and any special limitations.

Procedure

To install the Internet Service Monitoring Tivoli Enterprise Management Agent on a Linux or UNIX system separate from IBM Tivoli Monitoring:

1. Log in as the same user used for the installation of IBM Tivoli Monitoring.
2. Insert the product CD or download the product from the IBM Passport Advantage® website: http://www.ibm.com/software/howtobuy/passportadvantage.
3. Mount the installation image.
4. In the mount directory, run the command `./install.sh` and press **Enter**.
5. 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.
6. 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**.
7. If any existing IBM Tivoli Monitoring components are currently running on the computer, the installer stops them during the installation process, then restarts them when the installation is complete. To confirm this action, type 1 when prompted and press **Enter**. If you choose not to stop the components, the installation process aborts.
8. Type 1 when prompted to `Install products to the local host` and press **Enter**.
9. The software license agreement is displayed. Type 1 to accept the agreement and press **Enter**.
10. If IBM GSKit is not already installed on the computer, you are prompted to provide an encryption key.

    Use the same key across the enterprise. Either type the key or accept the default and press **Enter**.
11. A list is displayed of available operating systems. Type the number for the operating system that you are installing on. The default value is your current operating system. Press **Enter**.
12. Type 1 to confirm the operating system and press **Enter**. A numbered list of products available for installation is displayed.
13. Type the number corresponding to Internet Service Monitoring and press **Enter**.
14. Type 1 to confirm your selection.
15. At the prompt `Do you want to install additional products or product support packages`, type 2 and press **Enter**.

Results

Installation of Internet Service Monitoring is complete. You can now install the support files, then configure the product components. See "Configuring the Internet service monitoring agent on Linux or UNIX systems" on page 40 for more information.

Installing Tivoli Enterprise Monitoring Server support on Linux or UNIX systems

Install Tivoli Enterprise Monitoring Server (TEMS) support to the system on which Tivoli Enterprise Monitoring Server is installed.

Before you begin

Before beginning the installation, ensure that you have read "Planning to install Internet Service Monitoring" on page 11 for information about hardware and software prerequisites, planning and deployment considerations, and any special limitations.

Procedure

To install Tivoli Enterprise Monitoring Server support on Linux or UNIX:

1. Log in as the same user as that used for the installation of IBM Tivoli Monitoring.
2. Insert the product CD or download the product from the IBM Passport Advantage® website: http://www.ibm.com/software/howtobuy/passportadvantage.
3. Mount the installation image.
4. In the mount directory, run the command `./install.sh` and press **Enter**.

5. 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.
6. 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**.
7. If any existing IBM Tivoli Monitoring components are currently running on the computer, the installer stops them during the installation process, then restarts them when the installation is complete. To confirm this action, type 1 when prompted and press **Enter**. If you choose not to stop the components, the installation process aborts.
8. Type 1 when prompted to `Install products to the local host` and press **Enter**.
9. The software license agreement is displayed. Type 1 to accept the agreement and press **Enter**. A list is then displayed of available operating systems and component support categories.
10. Type the number for Tivoli Enterprise Monitoring Server Support and press **Enter**.
11. Type 1 to confirm your selection and press **Enter**. A list is displayed of products for which support files are to be added.
12. Type the number for Internet Service Monitoring and press **Enter**.
13. Type 1 to confirm your selection and press **Enter**.
14. At the prompt `Do you want to install additional products or product support packages`, type 2 and press **Enter**.

Results

Installation of Tivoli Enterprise Monitoring Server support is complete. You can now add Tivoli Enterprise Monitoring Server application support. See "Adding Tivoli Enterprise Monitoring Server application support manually on Linux or UNIX systems" on page 26 for information about how to do this.

Note: If Tivoli Enterprise Portal and Tivoli Enterprise Portal Server are installed on the same system, you can type 1 at the prompt `Do you want to install additional products or product support packages` and press **Enter**. Then follow the prompts to install the Tivoli Enterprise Portal and Tivoli Enterprise Portal Server support files. In a distributed IBM Tivoli Monitoring environment, install the support files separately for each component.

Adding Tivoli Enterprise Monitoring Server application support manually on Linux or UNIX systems

After you have installed Tivoli Enterprise Monitoring Server support to Linux or UNIX systems, you must add application support.

Before you begin

Before beginning the installation, ensure that you have read "Planning to install Internet Service Monitoring" on page 11 for information about hardware and software prerequisites, planning and deployment considerations, and any special limitations.

Tip: You can install Tivoli Enterprise Monitoring Server and Tivoli Enterprise Portal Server support automatically when you install each agent. Ensure that SDA is enabled to use this feature. See Using self-describing agents (SDA) for more information.

About this task

You can add application support from the command line or from the **Manage Tivoli Enterprise Monitoring Services** window.

To add application from the command line, run the command: `./itmcmd support -t` *`temsname`* `is`.

Procedure

To add application support using the **Manage Tivoli Enterprise Monitoring Services** window:

1. Right click Tivoli Enterprise Monitoring Server in the **Manage Tivoli Enterprise Monitoring Services** window.

2. Select **Install Product Support** > **Advanced** and then select **Internet Service Monitoring**.

Installing Tivoli Enterprise Portal Server support on Linux or UNIX systems

Install Tivoli Enterprise Portal Server (TEPS) support to the system on which Tivoli Enterprise Portal Server is installed.

Before you begin

Before beginning the installation, ensure that you have read "Planning to install Internet Service Monitoring" on page 11 for information about hardware and software prerequisites, planning and deployment considerations, and any special limitations.

Procedure

To install Tivoli Enterprise Portal Server support on Linux or UNIX systems:

1. Login as the same user used for the installation of IBM Tivoli Monitoring.
2. Insert the product CD or download the product from the IBM Passport Advantage® website: http://www.ibm.com/software/howtobuy/passportadvantage.
3. Mount the installation image.
4. In the mount directory, run the command `./install.sh` and press **Enter**.
5. 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.
6. 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**.
7. If any existing IBM Tivoli Monitoring components are currently running on the computer, the installer stops them during the installation process, then restarts them when the installation is complete. To confirm this action, type 1 when prompted and press **Enter**. If you choose not to stop the components, the installation process aborts.
8. Type 1 when prompted to `Install products to the local host` and press **Enter**.
9. The software license agreement is displayed. Type 1 to accept the agreement and press **Enter**. A list is then displayed of available operating systems and component support categories.
10. Type the number for Tivoli Enterprise Portal Server support and press **Enter**.
11. Type 1 to confirm your selection and press **Enter**. A list is displayed of products for which support files are to be added.
12. Type the number for Internet Service Monitoring and press **Enter**.
13. Type 1 to confirm your selection and press **Enter**.
14. At the prompt `Do you want to install additional products or product support packages`, type 1 and press **Enter**.
15. If the system is running Tivoli Enterprise Portal Server, you can install Tivoli Enterprise Portal Browser Client support. From the list of component support categories, type the number for Tivoli Enterprise Portal Browser Client support and press **Enter**.
16. Repeat from step 10 through step 14, selecting Tivoli Enterprise Portal Browser Client Support.
17. At the prompt `Do you want to install additional products or product support packages`, type 2 and press **Enter**.

Results

Installation of Tivoli Enterprise Portal Server support is complete. You can now configure the Tivoli Enterprise Portal Server. See "Configuring Tivoli Enterprise Portal Server on Linux or UNIX systems" on page 41 for further information.

Installing Tivoli Enterprise Portal Desktop support manually on Linux systems

Install Tivoli Enterprise Portal (TEP) Desktop support to the system on which Tivoli Enterprise Portal is installed.

Before you begin

Before beginning the installation, ensure that you have read "Planning to install Internet Service Monitoring" on page 11 for information about hardware and software prerequisites, planning and deployment considerations, and any special limitations.

Tip: You can install Tivoli Enterprise Monitoring Server and Tivoli Enterprise Portal Server support automatically when you install each agent. Ensure that SDA is enabled to use this feature. See Using self-describing agents (SDA) for more information.

Procedure

To install Tivoli Enterprise Portal Desktop support on Linux:

1. Log in as the same user used for the installation of IBM Tivoli Monitoring.
2. Insert the product CD or download the product from the IBM Passport Advantage® website: http://www.ibm.com/software/howtobuy/passportadvantage.
3. Mount the installation image.
4. In the mount directory, run the command `./install.sh` and press **Enter**.
5. 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.
6. 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**.
7. If any existing IBM Tivoli Monitoring components are currently running on the computer, the installer stops them during the installation process, then restarts them when the installation is complete. To confirm this action, type 1 when prompted and press **Enter**. If you choose not to stop the components, the installation process aborts.
8. Type 1 when prompted to `Install products to the local host` and press **Enter**.
9. The software license agreement is displayed. Type 1 to accept the agreement and press **Enter**. A list is then displayed of available operating systems and component support categories.
10. Type the number for Tivoli Enterprise Portal Desktop Client support and press **Enter**.
11. Type 1 to confirm your selection and press **Enter**. A list is displayed of products for which support files are to be added.
12. Type the number for Internet Service Monitoring and press **Enter**.
13. Type 1 to confirm your selection and press **Enter**.
14. At the prompt `Do you want to install additional products or product support packages`, type n and press **Enter**.

Results

Installation of Tivoli Enterprise Portal Desktop support is complete. If all other support files are installed, and the Internet service monitoring agent and Tivoli Enterprise Portal Server are configured, you are ready to start Internet Service Monitoring.

Silent installation on UNIX systems

Silent installation enables you to define the options for installing Internet Service Monitoring in an installation response file, then run the installation process from the command line without interactive input. This method is useful for performing repeated installations.

Before you begin

Before beginning the installation, ensure that you have read "Planning to install Internet Service Monitoring" on page 11 for information about hardware and software prerequisites, planning and deployment considerations, and any special limitations.

About this task

A sample installation response file, `silent_install.txt`, is available with the product installer. The file contains comprehensive instructions on how to modify and use it.

Procedure

To run a silent installation:

1. Open the installation response file in a text editor.
2. Uncomment and modify the installation options as required, then save the file.
3. Execute the command:

   ```
   ./install.sh -q -h home -p response-file
   ```

   where *home* is the IBM Tivoli Monitoring home directory, typically `/opt/IBM/ITM`, and *response-file* is the absolute pathname of the installation response file.

Results

What to do next

After installation is complete, you can configure the product using the silent configuration process.

Silent configuration

After installing Internet Service Monitoring, you can configure it silently.

About this task

To perform silent configuration, you must create a configuration response file. Configuration response files are text files containing parameter-value pairs that specify the desired configuration settings.

The following syntax rules apply to configuration response files:

- Comment lines begin with a pound (#) character.
- Blank lines are ignored.
- Parameter-value pairs have the format: *PARAMETER=value*

  Do not use a space before the parameter name; you can use a space before or after an equal (=) character.

  Do not use dollar ($), equal (=), or pipe (|) characters in parameter values.

Procedure

To perform silent configuration:

1. Create a configuration response file containing the desired configuration settings.

   See "Sample silent configuration file" on page 30 for an example.
2. Execute the command:

```
./itmcdm config -A -p response-file is
```

where *response-file* is the absolute path to the configuration response file.

Sample silent configuration file

```
################### PRIMARY TEMS CONFIGURATION ###################

# Will this agent connect to a Tivoli Enterprise Monitoring Server (TEMS)?
# This parameter is required.
# Valid values are: YES and NO
##### TEP should not connect to TEMS, ignore all TEMS connection variables. #####
#CMSCONNECT=YES

# What is the hostname of the TEMS to connect to?
# This parameter is NOT required.  (default is the local system hostname)
#HOSTNAME=somehost.somewhere.com

# Will this agent connect to the TEMS through a firewall?
# This parameter is NOT required.  (default is NO)
# Valid values are: YES and NO
#   - If set to YES the NETWORKPROTOCOL must be ip.pipe
#FIREWALL=NO

# What network protocol is used when connecting to the TEMS?
# This parameter is required.
# Valid values are: ip, sna, ip.pipe, or ip.spipe
#NETWORKPROTOCOL=ip.pipe

# What is the first backup network protocol used for connecting to the TEMS?
# This parameter is NOT required. (default is none)
# Valid values are: ip, sna, ip.pipe, ip.spipe, or none
#BK1NETWORKPROTOCOL=none

# What is the second backup network protocol used for connecting to the TEMS?
# This parameter is NOT required. (default is none)
# Valid values are: ip, sna, ip.pipe, ip.spipe or none
#BK2NETWORKPROTOCOL=none

# If ip.pipe is one of the three protocols what is the IP pipe port number?
# This parameter is NOT required. (default is 1918)
#IPPIPEPORTNUMBER=1918

# If ip.pipe is one of the three protocol what is the IP pipe partition name?
# This parameter is NOT required. (default is null)
#KDC_PARTITIONNAME=null

# If ip.pipe is one of the three protocols what is the KDC partition file?
# This parameter is NOT required. (default is null)
#KDC_PARTITIONFILE=null

# If ip.spipe is one of the three protocols what is the IP pipe port number?
# This parameter is NOT required. (default is 3660)
#IPSPIPEPORTNUMBER=3660

# If ip is one of the three protocols what is the IP port number?
# This parameter is NOT required. (default is 1918)
# A port number and or one or more pools of port numbers can be given.
# The format for a pool is #-# with no embedded blanks.
#PORTNUMBER=1918

# If sna is one of the three protocols what is the SNA net name?
# This parameter is NOT required. (default is CANDLE)
#NETNAME=CANDLE

# If sna is one of the three protocols what is the SNA LU name?
# This parameter is NOT required. (default is LUNAME)
#LUNAME=LUNAME

# If sna is one of the three protocols what is the SNA log mode?
# This parameter is NOT required. (default is LOGMODE)
#LOGMODE=LOGMODE

################### SECONDARY TEMS CONFIGURATION ###################

# Would you like to configure a connection for a secondary TEMS?
# This parameter is NOT required. (default is NO)
# Valid values are: YES and NO
#FTO=NO
```

```
# If configuring a connection for a secondary TEMS, what is the hostname
# of the secondary TEMS?
# This parameter is required if FTO=YES
#MIRROR=somehost.somewhere.com

# Will the TEP connect to the secondary TEMS through a firewall?
# This parameter is NOT required. (default is NO)
# Valid values are: YES and NO
#FIREWALL2=NO

# What network protocol is used when connecting to the secondary TEMS?
# This parameter is required when FTO=YES and FIREWALL2 is NO
# Valid values are: ip, sna, or ip.pipe
#HSNETWORKPROTOCOL=ip.pipe

# What is the first backup network protocol used for connecting to the
# secondary TEMS?
# This parameter is NOT required. (default is none)
# Valid values are: ip, sna, ip.pipe, or none
#BK1HSNETWORKPROTOCOL=none

# What is the second backup network protocol used for connecting to the
# secondary TEMS?
# This parameter is NOT required. (default is none)
# Valid values are: ip, sna, ip.pipe, or none
#BK2HSNETWORKPROTOCOL=none

# If ip.pipe is one of the three secondary TEMS protocols what is the IP pipe
# port number?
# This parameter is NOT required. (default is 1918)
#HSIPPIPEPORTNUMBER=1918

# If ip is one of the three secondary TEMS protocols what is the IP port number?
# This parameter is NOT required. (default is 1918)
# A port number and or one or more pools of port numbers can be given.
# The format for a pool is #-# with no embedded blanks.
#HSPORTNUMBER=1918

# If sna is one of the three secondary TEMS protocols what is the SNA net name?
# This parameter is NOT required. (default is CANDLE)
#HSNETNAME=CANDLE

# If sna is one of the three secondary TEMS protocols what is the SNA LU name?
# This parameter is NOT required. (default is LUNAME)
#HSLUNAME=LUNAME

# If sna is one of the three secondary TEMS protocols what is the SNA log mode?
# This parameter is NOT required. (default is LOGMODE)
#HSLOGMODE=LOGMODE

#################### OPTIONAL PRIMARY NETWORK NAME CONFIGURATION ####################

# If the system is equipped with dual network host adapter cards you can designate
# another network name.  What is the network name?
# This parameter is NOT required. (default is none)
#PRIMARYIP=none

#################### ISM CONFIGURATION ####################

# Connect ISMs to an Object Server
# This parameter is required.(default is no)
#ISM_OMNIBUS_CONNECTION=no

# What is the Object server hostname?
# (default is localhost)
#ISM_OMNIBUS_HOSTNAME=localhost

# What is the Object Server port?
# (default is 4100)
#ISM_OMNIBUS_PORT=4100

# What is the name of the Object Server?
# (default is "NCOMS")
#ISM_OMNIBUS_NAME="NCOMS"
```

Starting Internet Service Monitoring

Starting Internet Service Monitoring requires you to start each of the product components individually.

Before you begin

These guidelines assume that you have already started the Tivoli Enterprise Monitoring Server (TEMS) and the Tivoli Enterprise Portal Server (TEPS).

Procedure

To start Internet Service Monitoring:

1. *(Optional)* Start the Databridge and the Internet service monitors.
2. Start the Internet service monitoring agent.

   Note: As of ITCAM for Transactions V7.2, starting and stopping the Internet Service Monitoring agent also starts and stops all Internet service monitors and the Databridge automatically.
3. To create Internet service tests and view their results, start the Tivoli Enterprise Portal client.

Starting Internet Service Monitoring on Windows systems

To start Internet Service Monitoring on Windows, follow these steps.

About this task

To start the Databridge and the Internet service monitors:

1. Select **Start** > **Control Panel**, open the **Administrative Tools** group, then launch the **Services** console.
2. From the list of services, select the service named **NCO BRIDGE Internet Service Monitor**, and then select **Start** from the context menu.

   Tip: The installer configures the Databridge service to start automatically, so it is normally not necessary to start it manually.
3. From the list of services, select the service named **NCO *service-name* Internet Service Monitor** for each Internet service monitor that you want to run, then select **Start** from the context menu.

   Note: If you have deployed Internet service monitors on more than one host, you must start the monitor services on each host.

To start the Internet service monitoring agent:

1. Select **Start** > **Programs** > **IBM Tivoli Monitoring** > **Manage Tivoli Monitoring Services**.
2. From the list of components, select **Internet Service Monitoring**, and then select **Start** from the context menu.

To start the Tivoli Enterprise Portal desktop client:

1. Select **Start** > **Programs** > **IBM Tivoli Monitoring** > **Tivoli Enterprise Portal**. Alternatively, if you created a desktop icon, click the icon. The **Logon** window is displayed.
2. Enter your logon ID and password and click **OK**.

Alternatively, to start the Tivoli Enterprise Portal browser client:

1. In the **Address** field in Internet Explorer, enter `http://`*`ip of Tivoli Enterprise Portal Server`*`:1920`. For example, http://192.168.60.22:1920.
2. In the **IBM Tivoli Monitoring Service Index**, select **IBM Tivoli Enterprise Portal Web Client**.
3. In the **Warning - Security** dialog box, click **Yes** to indicate that you trust the applet distributed by IBM. If you do not trust the applet you will not be able to use the browser client.
4. Enter your user name and password and click **OK**.

The Internet Service Monitoring user configuration application is indicated in the toolbar of the Tivoli Enterprise Portal icon.

Note: When you start the user interface configuration, the **Internet Service Monitoring Configuration Loading** window is displayed. Closing this window while the interface configuration is still being loaded, does not stop the interface configuration from being launched. If you do want to stop using the configuration, wait until it is loaded.

Starting Internet Service Monitoring on Linux or UNIX systems

To start Internet Service Monitoring on Linux or UNIX systems, follow these steps.

About this task

To start the Databridge and the Internet service monitors, run the command:

```
$ISMHOME/bin/ism_startup.sh start
```

To start the Internet service monitoring agent, run the command:

```
/opt/IBM/ITM/bin/itmcmd agent start is
```

To start the Tivoli Enterprise Portal desktop client:

1. Run the command:

   ```
   /opt/IBM/ITM/bin/itmcmd agent start cj
   ```

2. Enter your login ID and password, and then click **OK**.

Alternatively, to start the Tivoli Enterprise Portal browser client:

1. In the **Address** field in Internet Explorer, enter `http://`*`ip of Tivoli Enterprise Portal Server`*`:1920`. For example, http://192.168.60.22:1920.
2. In the **IBM Tivoli Monitoring Service Index**, select **IBM Tivoli Enterprise Portal Web Client**.
3. In the **Warning - Security** dialog box, click **Yes** to indicate that you trust the applet distributed by IBM. If you do not trust the applet you will not be able to use the browser client.
4. Enter your user name and password and click **OK**.

The Internet Service Monitoring application is indicated in the toolbar of the Tivoli Enterprise Portal by the Internet Service Monitoring Configuration icon.

Note: When you start the user interface configuration, the **Internet Service Monitoring Configuration Loading** window is displayed. Closing this window while the interface configuration is still being loaded, does not stop the interface configuration from being launched. If you do want to stop using the configuration, wait until it is loaded.

Starting and stopping Internet Service Monitoring monitors using Tivoli Enterprise Portal

You can use Tivoli Enterprise Portal to start and stop monitors and the Databridge, including those deployed on remote computers.

Before you begin

To control monitors and the Databridge from the Tivoli Enterprise Portal, a Universal Agent must already be installed on the computer hosting those components.

Procedure

To start or stop the Internet Service Monitoring monitors using Tivoli Enterprise Portal:

1. Log into Tivoli Enterprise Portal.
2. In the Navigator pane, locate the computer hosting the monitors and expand its node.
3. Select **Internet Service Monitors**, and then right-click and select **Take Action** > **Select**.
4. In the **Take Action** dialog box, select the required action from the **Action** list. For example, to start the DHCP monitor, select **Start DHCP**.

- You can enter specific combinations of monitors in the **Command** field, for example `start DHCP FTP`.
- To start or stop all components, select the **Start all** or **Stop all** actions.

5. In the **Destinations** group, select all the host computers on which to perform the action.
6. Click **OK**.

What to do next

The **Action Status** dialog box displays the results of the selected actions. A `Return Code` of zero indicates that the actions were successful. The `Message` field provides additional information, where applicable.

Stopping Internet Service Monitoring

In ITCAM for Transactions V7.2 and later, when you stop the Internet Service Monitoring agent, you stop all monitors and the Databridge by default.

About this task

If you do not want the Internet Service Monitoring agent to automatically start and stop all monitors and the Databridge, you can disable the **`ManageServices`** property in the Internet Service Monitoring properties file (`kisagent.props`).

Note: Disabling the **`ManageServices`** property also stops Take Action commands and situations from starting the monitors and Databridge.

Procedure

In the `kisagents.props` file, set the **`ManageServices`** property to `0`.

What to do next

To enable the property again if required, set the value back to 1 in the `kisagents.props` file.

Uninstalling Internet Service Monitoring

Uninstalling Internet Service Monitoring is a two-step process if installed on the same system that is host to Tivoli Enterprise Monitoring Server, Tivoli Enterprise Portal Server, and Tivoli Enterprise Portal. You must first uninstall the product from the system and then remove the product from the Tivoli Enterprise Portal into which it is integrated.

About this task

If Internet Service Monitoring is installed in a distributed IBM Tivoli Monitoring environment, an additional step is required to remove the Tivoli Enterprise Monitoring Server, Tivoli Enterprise Portal Server, and Tivoli Enterprise Portal support files.

Removing Internet Service Monitoring does not affect your IBM Tivoli Monitoring

Uninstalling Internet Service Monitoring on Windows systems

Uninstalling Internet Service Monitoring from a Windows system that is also host to Tivoli Enterprise Portal, Tivoli Enterprise Portal Server, and Tivoli Enterprise Monitoring Server automatically removes the associated support files. If you have a distributed installation, ensure that you uninstall the Tivoli Enterprise Portal, Tivoli Enterprise Portal Server, and Tivoli Enterprise Monitoring Server support files separately from the remote systems.

Before you begin

Before uninstalling Internet Service Monitoring on Windows, run the pre-installation script `preuninstall.cmd` to clean up the services that were created during installation. The script is located in `%CANDLE_HOME%\TMAITM6\ism\platform\win32\bin\preuninstall.cmd`.

When you have run the script, you can uninstall Internet Service Monitoring.

Procedure

To uninstall Internet Service Monitoring on Windows:

1. Select **Start** > **Settings** > **Control Panel** > **Add and Remove Programs**.
2. Navigate to IBM Tivoli Monitoring and click **Remove**.
3. On the **Welcome** window of the IBM Tivoli Monitoring installation wizard, select **Modify** to remove only the selected features, or select **Remove** to remove all features and click **Next**.
4. Click **OK** in the information dialog box.
5. On the **Add or Remove Features** window, deselect those features you want to uninstall and click **Next**.
6. Click **OK** in the confirmation dialog box.

   Internet Service Monitoring is removed.
7. On the **Product Remove Complete** window, click **Finish**.

Results

Internet Service Monitoring is removed. If you want to clear the corresponding Internet Service Monitoring agents from display in the Tivoli Enterprise Portal, you must do this manually. See "Removing agents from Tivoli Enterprise Portal" on page 36.

Uninstalling Internet Service Monitoring on UNIX systems

Uninstalling Internet Service Monitoring from a UNIX system that is also host to Tivoli Enterprise Portal, Tivoli Enterprise Portal Server, and Tivoli Enterprise Monitoring Server, automatically removes the associated support files. If you have a distributed installation, ensure that you uninstall the Tivoli Enterprise Portal, Tivoli Enterprise Portal Server, and Tivoli Enterprise Monitoring Server support files separately from the remote systems.

Procedure

To uninstall Internet Service Monitoring on UNIX systems:

1. From a command shell, type `cd /opt/IBM/ITM/bin`.
2. Type the command `./uninstall.sh`. The name of the system on which the product is installed, is displayed.
3. Type the number corresponding to Internet Service Monitoring (this is the entry indicated by the product code `is`).
4. Enter 1 to confirm your selection and press **Enter**.
5. To exit the uninstaller, enter 99 and press **Enter**.

Results

Internet Service Monitoring is removed. If you want to clear the corresponding Internet Service Monitoring agents from display in the Tivoli Enterprise Portal, you must do this manually. See "Removing agents from Tivoli Enterprise Portal" on page 36.

What to do next

On AIX systems, run the following command to remove the Internet Service Monitoring libraries:

```
slibclean
```

Removing agents from Tivoli Enterprise Portal

After you have uninstalled Internet Service Monitoring, you may want to clear unused Internet Service Monitoring agents from display in the Tivoli Enterprise Portal (TEP).

Procedure

To clear an unused Internet Service Monitoring agent from Tivoli Enterprise Portal:

1. In the Tivoli Enterprise Portal, select **Enterprise** in the navigator.
2. Right click on **Enterprise** and select **Workspace** > **Managed System Status**.
3. In the **Managed System Status** view, right click Internet Service Monitoring that has a status of **Offline** and select **Clear offline entry**.

   The application is removed from the Tivoli Enterprise Portal.
4. Click **Refresh** to update the Tivoli Enterprise Portal display.

Uninstalling support files

In an IBM Tivoli Monitoring environment where both Internet Service Monitoring and the IBM Tivoli Monitoring components are installed on the same system, the support files are automatically removed when uninstalling Internet Service Monitoring. In a distributed environment, you must manually remove the support files from the remote systems.

Uninstalling Tivoli Enterprise Monitoring Server support on Windows systems

Uninstall both Tivoli Enterprise Monitoring Server (TEMS) application support and the support file from Tivoli Enterprise Monitoring Server.

About this task

Remove Tivoli Enterprise Monitoring Server application support first and then remove the Tivoli Enterprise Monitoring Server support component.

To remove Tivoli Enterprise Monitoring Server application support on Windows:

1. Open the **Manage Tivoli Enterprise Monitoring Services** window on the system where Tivoli Enterprise Monitoring Server is installed.
2. Right click **Tivoli Enterprise Monitoring Server**.
3. Select **Advanced** > **Remove TEMS application support**.
4. In the **Remove application support from the TEMS** dialog box, select **On this computer** and click **OK**.
5. In the **Select the application support to remove from the TEMS** dialog box, select **Internet Service Monitoring** and click **OK**.

Procedure

To uninstall Tivoli Enterprise Monitoring Server support on Windows:

1. Select **Start** > **Settings** > **Control Panel** > **Add and Remove Programs**.
2. Navigate to **IBM** and click **Change/Remove**.
3. On the **Welcome** window of the Internet Service Monitoring installation wizard, select **Modify** and click **Next**.
4. On the **Add or Remove Features** window, expand **Tivoli Enterprise Monitoring Server**, deselect **Internet Service Monitoring** and click **Next**.
5. Follow the prompts to complete the uninstall process and click **Finish**.

Uninstalling Tivoli Enterprise Portal Server support on Windows systems

Uninstall Tivoli Enterprise Portal Server (TEPS) support from Tivoli Enterprise Portal Server.

Procedure

To uninstall Tivoli Enterprise Portal Server support on Windows:

1. Select **Start** > **Settings** > **Control Panel** > **Add and Remove Programs**.
2. Navigate to IBM Internet Service Monitoring and click **Change/Remove**.
3. On the **Welcome** window of the Internet Service Monitoring installation wizard, select **Modify** and click **Next**.
4. On the **Add or Remove Features** window, expand **Tivoli Enterprise Portal Server**, deselect **Internet Service Monitoring** and click **Next**.
5. Follow the prompts to complete the uninstall process and click **Finish**.

Uninstalling Tivoli Enterprise Portal support on Windows systems

Uninstall Tivoli Enterprise Portal (TEP) support by uninstalling both Tivoli Enterprise Portal Browser Client support and Tivoli Enterprise Portal Desktop Client support from Tivoli Enterprise Portal.

About this task

On Windows, Tivoli Enterprise Portal Browser Client support is bundled with Tivoli Enterprise Portal Server support. The browser client is uninstalled when Tivoli Enterprise Portal Server support is uninstalled.

Procedure

To uninstall Tivoli Enterprise Portal Desktop Client support on Windows:

1. Select **Start** > **Settings** > **Control Panel** > **Add and Remove Programs**.
2. Navigate to Internet Service Monitoring and click **Change/Remove**.
3. On the **Welcome** window of the Internet Service Monitoring installation wizard, select **Modify** and click **Next**.
4. On the **Add or Remove Features** window, expand **Tivoli Enterprise Portal Desktop Client**, deselect **Internet Service Monitoring** and click **Next**.
5. Follow the prompts to complete the uninstallation process and click **Finish**.

Reinstalling Internet Service Monitoring

Before reinstalling Internet Service Monitoring check here.

To reinstall Internet Service Monitoring follow the procedures described in Chapter 4, “Installing Internet Service Monitoring,” on page 19.

Chapter 5. Configuring Internet Service Monitoring

Before you can use Internet Service Monitoring, it must be configured to work with IBM Tivoli Monitoring or IBM Tivoli Netcool/OMNIbus.

Configuring the Internet service monitoring agent on Windows systems

To configure the Internet service monitoring agent to work with IBM Tivoli Monitoring, you must set connection parameters that enable it to contact the Tivoli Enterprise Monitoring Server (TEMS), or the ObjectServer if using ObjectServer IBM Tivoli Netcool/OMNIbus. On Windows, these parameters are typically configured during installation of the Tivoli Enterprise Monitoring Server support file but you can reconfigure them at any time by starting the configuration procedure manually.

About this task

Each configuration generates a log file that you can use to diagnose problems. The location of the log file is

`C:\IBM\ITM\InstallITM\plugin\executionEvents\logs\install_plugin_comp-is_`*n*

where *n* is a number increasing by one for each configuration.

Note: Ensure that Tivoli Enterprise Portal Server is running before you configure Internet Service Monitoring.

Procedure

To manually configure the Internet Service Monitoring agent on Windows systems:

1. Select **Start** > **Programs** > **IBM Tivoli Monitoring** > **Manage Tivoli Monitoring Services**.
2. Right-click **Internet Service Monitoring** and select **Reconfigure**. The **Agent Advanced Configuration** window opens. This window is called **Configuration Defaults for Connecting to a TEMS** if accessed during the installation process.
3. On the **Configuration Defaults for Connecting to a TEMS** window, specify the Tivoli Enterprise Monitoring Server connection information and click **OK**:
   a) Select **Connection must pass through firewall** if the agent and the Tivoli Enterprise Monitoring Server are on different sides of a firewall.
   b) Select **Protocol 1** and select a protocol from the list. Several types of protocols are available: IP.UDP (uses unsecured UDP communications), IP.PIPE (uses unsecured TCP communications), IP.SPIPE (uses SSL secure TCP communications), and SNA (uses SNA for mainframe components).
   c) If additional protocols are required, select **Protocol 2** and select an second protocol from the list.
   d) Do not select **Optional Secondary TEMS Connection**. You can set up the failover support for the component later. See the *IBM Tivoli Monitoring User's Guide* for further information.
   e) Click **OK**.
4. In the summary Configuration Defaults for Connecting to a TEMS window, check the information and click **OK**.

   These settings define communications between the agent and the Tivoli Enterprise Monitoring Server. The host name or IP address of the local computer are displayed unless the Tivoli Enterprise Monitoring Server has already been specified. Ensure that you enter the host name or IP address of the Tivoli Enterprise Monitoring Server in the **Hostname or IP address** field if it is installed on another computer. The default port number for the previously selected protocol is also displayed (IP.PIPE is 1918, IS.SPIPE is 3660).
5. On the **Internet Service Monitoring Configuration** window, if using IBM Tivoli Netcool/OMNIbus select **YES** and enter the host name or IP address of the IBM Tivoli Netcool/OMNIbus ObjectServer and its port number.

Tip: If you are using IBM Tivoli Netcool/OMNIbus but want to configure the connection later, select **NO**. Configure the ObjectServer connection later using the Manage Tivoli Enterprise Monitoring Services.

6. Click **OK**. The system continues the agent configuration. Upon completion you are returned to the **Manage Tivoli Monitoring Services** window.

Configuring the Internet service monitoring agent on Linux or UNIX systems

To configure the Internet service monitoring agent to work with IBM Tivoli Monitoring, you must set the connection parameters that enable it to contact the Tivoli Enterprise Monitoring Server (TEMS) or to the ObjectServer if using ObjectServer IBM Tivoli Netcool/OMNIbus. This configuration must be done manually on Linux or UNIX systems after installing Internet Service Monitoring.

About this task

Perform the configuration as the same user that was used when IBM Tivoli Monitoring was installed. You can update your configuration at any time. A log file is generated for each configuration. Use this file to diagnose any problems.

The file is located at:

`/opt/IBM/ITM/InstallITM/plugin/executionEvents/logs/install_plugin_comp_is_`*n*

where *n* is a number increasing by one for each generation.

Note: Ensure that Tivoli Enterprise Portal Server is running before you configure the Internet service monitoring agent.

To configure the Internet service monitoring agent from the command line, run the following command from the computer where the agent is installed:

```
/opt/IBM/ITM/bin/itmcmd config -A is
```

Procedure

To configure the agent using **Manage Tivoli Enterprise Monitoring Services**:

1. Change directory to `/opt/IBM/ITM/bin`.
2. Run the command: `./itmcmd manage`. The **Manage Tivoli Enterprise Monitoring Services** window is displayed.
3. Select **Internet Service Monitoring**.
4. Right click and select **Configure**. The **Internet Service Monitoring Configuration** window is displayed, and the **Object Server Connection** tab is presented.
5. If using IBM Tivoli Netcool/OMNIbus, set **Configure Object Server Connection** to **YES** and enter the name of the ObjectServer, the host name or IP address of the IBM Tivoli Netcool/OMNIbus ObjectServer computer and its port number. Click **OK**.
6. Ensure that the check box for **No TEMS** is cleared and type the **TEMS Hostname**.
7. On the **Protocol 1** tab select the protocol required to communicate with the monitoring server. You can specify two protocols, one as the standard protocol and one to be used as a backup. Four types of protocol are available: IP.TCP, IP.PIPE (uses unsecured TCP communications), IS.PIPE (uses SSL secure TCP communications), and SNA (uses SNA for mainframe components).
8. Enter the settings or accept the defaults for the selected protocol and click **Save**.

   Note: The default port number for IP.PIPE is 1918, for IP.SPIPE the port number is 3660.

Configuring Tivoli Enterprise Portal Server on Linux or UNIX systems

After you have installed Tivoli Enterprise Portal Server (TEPS) Support on Linux or UNIX systems you must reconfigure the Tivoli Enterprise Portal Server.

Before you begin

You can reconfigure Tivoli Enterprise Portal Server after you have completed the installation of Tivoli Enterprise Portal Server Support using the command line or **Manage Tivoli Enterprise Monitoring Services**.

To reconfigure Tivoli Enterprise Portal Server from the command line:

1. Run the following command on the computer where the Tivoli Enterprise Portal Server is installed:

```
/opt/IBM/ITM/bin/itmcmd config -A cq
```

2. (Linux only) Run the following command on the computer where the Tivoli Enterprise Portal Desktop Client is installed:

```
/opt/IBM/ITM/bin/itmcmd config -A cj
```

Procedure

To reconfigure the Tivoli Enterprise Portal Server using **Manage Tivoli Enterprise Monitoring Services**:

1. Open the **Manage Tivoli Enterprise Monitoring Services** window on the computer where the Tivoli Enterprise Portal Server is installed.
2. Right click **Tivoli Enterprise Portal Server** and select **Configure**.
3. In the **Configure** dialog box, select **Save** (no changes are required).
4. (Linux only) Open the **Manage Tivoli Enterprise Monitoring Services** window on the computer where the Tivoli Enterprise Portal Desktop Client is installed.
5. Right click **Tivoli Enterprise Portal Desktop Client** and select **Configure**.
6. In the **Configure** dialog box, select **Save** (no changes are required).

Configuring Tivoli Enterprise Portal on Linux systems

After you have installed Tivoli Enterprise Portal Desktop Support on a Linux system you must reconfigure the Tivoli Enterprise Portal. You can reconfigure the Tivoli Enterprise Portal Desktop Client after you have completed the installation of Tivoli Enterprise Portal Desktop Support using the command line or **Manage Tivoli Enterprise Monitoring Services**.

Before you begin

To reconfigure Tivoli Enterprise Portal Desktop Client from the command line, run the following command on the computer where the Tivoli Enterprise Portal Desktop Client is installed:

```
/opt/IBM/ITM/bin/itmcmd config -A cj
```

Procedure

To reconfigure the Tivoli Enterprise Portal Desktop Client Tivoli Enterprise Portal Server using **Manage Tivoli Enterprise Monitoring Services**:

1. Open the **Manage Tivoli Enterprise Monitoring Services** window on the computer where the Tivoli Enterprise Portal Desktop Client is installed.
2. Right-click **Tivoli Enterprise Portal Desktop Client** and select **Configure**.
3. In the **Configure** dialog box, select **Save** (no changes are required).

Databridge configuration

Configuring the Databridge involves setting properties for the Databridge that control its operation such as the connection of the component modules and the Internet service monitors.

Operation and configuration

The Databridge and its component modules are configured through properties files. The properties determine the operation of the Databridge and its component modules.

The component modules are:

- IBM Tivoli Monitoring module, which sends test results to IBM Tivoli Monitoring for reporting in workspaces.
- The ObjectServer module, which sends events to a ObjectServer IBM Tivoli Netcool/OMNIbus ObjectServer.
- Datalog module, which generates XML datalog files for archiving or simple, external reporting purposes. Use this module only with ObjectServer IBM Tivoli Netcool/OMNIbus.

The Databridge, including its component modules, properties files, and the systems to which the modules connect. The ObjectServer module has a properties file named objectserver.props, the IBM Tivoli Monitoring module has a properties file named pipe_module.props, and the Databridge has a properties file named databridge.props. The Datalog module does not have a properties file.

Configuring the Databridge

The Databridge must be configured to receive data from the Internet service monitors and to forward that data to its component modules for further processing.

Table 5 on page 42 lists the files associated with the Databridge. The **Properties file**, **Store And Forward file**, and **Log file** are described in more detail in the appropriate sections.

Table 5. Databridge files and their location

Databridge file	Location and/or name
Executable file	`$ISMHOME/platform/arch/bin/nco_m_bridge`
Properties file	`$ISMHOME/etc/props/bridge.props`
Store and Forward file	Name and location are specified by properties in the `bridge.props` file. The default name and location is `$ISMHOME/var/sm_bridge.saf`
Log file	`$ISMHOME/log/bridge.log`
Error log file	`$ISMHOME/log/bridge.err`

Databridge properties and command line options

The properties file controls the operation of the Databridge. The properties specify the modules to which information is forwarded for further processing, the time at which log files should be generated, and any other Databridge properties.

You can modify the property values in the Databridge properties file or specify the values on the command line. If you make any changes to the properties file, you must restart the Databridge before the changes take affect.

By default, the Databridge uses the properties file `$ISMHOME/etc/props/bridge.props`, however you can instruct it to use an alternative file by starting it using the command:

```
$ISMHOME/platform/arch/bin/nco_m_bridge -propsfile file
```

where *arch* is the specific platform name and *file* is the path and filename of the required properties file.

Table 6 on page 43 lists the properties and command-line options available for the Databridge. You can also obtain a list of the available command-line options using the command:

```
$ISMHOME/platform/arch/bin/nco_m_bridge -help
```

Table 6. Databridge properties and command-line options

Property name	Parameter	Command line option	Description
MaxCCA	integer	-maxcca	Sets the maximum number of concurrent connections supported by the Databridge at any one time. **Note:** Setting MaxCCA to a high value may severely affect the performance of the Databridge. Default: 30
MessageLog	string	-messagelog	Specifies the location of the Databridge log file. Default: $ISMHOME/log/bridge.log
Module*n*PropFile	string	Not applicable	The name of the modules properties file.
Module*n*SharedLib	string	Not applicable	The name of the modules shared library file.
MsgDailyLog	0|1	-msgdailylog	Enables generation of a daily log file: • 0 - Enabled • 1 - Disabled
MsgTimeLog	string	-msgtimelog	Specifies the time (in 24-hour format HHMM) after which the Databridge generates a daily log if MsgDailyLog has the value True. Default: 0000 - 12:00am
NoRecover	0|1	-norecover	Suppresses automatic recovery of the store and forward file. • 0 - Disabled • 1 - Enabled
Not applicable	string	-propsfile	Specifies the path and filename of the Databridge properties file. Default: $ISMHOME/etc/props/bridge.props
QFile	string	-qfile	Sets the name of the store and forward file. Default: $ISMHOME/var/sm_bridge.saf
QSize	integer	-qsize	Sets the reserved size of the store and forward file (in bytes). Default: 51200000

Table 6. Databridge properties and command-line options (continued)

Property name	Parameter	Command line option	Description
SocketBacklog	integer	-socketbacklog	Sets the maximum number of pending connections in the Databridge socket's listen queue. If the length of the queue exceeds this value, the Databridge refuses further connection requests. Default is 10.
SocketBufferSize	integer	-socketbuffersize	Sets the buffer size of the Databridge socket connection (in kilobytes). Specify a minimum of 8. Default: 256
SocketPort	integer	-socketport	Specifies the port number on which the Databridge listens for connections. Default: 9510
SocketTimeout	integer	-sockettimeout	Sets the timeout of Databridge socket connections (in seconds). Default: 10
BridgeSSL AuthenticatePeer	0|1	-bridgessl authenticatepeer	Specifies whether the Databridge needs to authenticate monitor encryption certificates. • 0 - Disabled • 1 - Enabled
BridgeSSL CertificateFile	string	-bridgessl certificatefile	Specifies the path and filename of the digital Bridge SSL certificate. Default: $ISMHOME/certificates/bridgeCert.pem
BridgeSSLCipherSet	string	-bridgesslcipherset	Specifies a CipherSet. If you update this value, use the Cipher syntax defined in the OpenSSL documentation. **Restriction:** Set the same value on the Internet service monitoring agent, all monitors, and the Databridge. Default: RC4:3DES:DES:+EXP 1

Table 6. Databridge properties and command-line options (continued)

Property name	Parameter	Command line option	Description
BridgeSSLDisableSSLv2	0|1	-bridgessldisablesslv2	Determines which types of sockets are accepted. • If set to 0, both SSLv2 and SSLv3 are accepted • If set to 1, sockets are opened in SSLv3 only **Restriction:** Set the same value on the Internet service monitoring agent, all monitors, and the Databridge. Default: 0
BridgeSSL Encryption	0|1	-bridgessl encryption	Specifies whether Bridge SSL encryption applies. • 0 - Enabled • 1 - Disabled **Note:** Set to the same value as for the monitors.
BridgeSSL KeyFile	string	-bridgessl keyfile	The path and the filename of the Bridge SSL private key file. Default: $ISMHOME/certificates/bridgeKey.pem
BridgeSSL KeyPassword	string	-bridgessl keypassword	The password used to encrypt the Bridge SSL private key. Default: tivoli
BridgeSSL Truststore	string	-bridgessl truststore	The path and file name of the Trusted certificate file for authentication. This is only required when using the AuthenticatePeer setting. Default: $ISMHOME/certificates/trust.pem

On Windows platforms, specify path separators using \ in place of /.

Store And Forward file

If the Databridge is unable to forward data to ObjectServer IBM Tivoli Netcool/OMNIbus, it stores all of the data it would normally send in a Store And Forward (SAF) file. When ObjectServer IBM Tivoli Netcool/OMNIbus becomes available again, it processes all of the events stored in the SAF file.

The QFile and QSize properties in the Databridge properties file determine the name, location and operation of the store and forward processing.

Log file
The Databridge sends daily messages about its operations to a message log file.

By default, the name of this file is `$ISMHOME/log/bridge.log`. It is updated at midnight (12:00am). The Databridge properties `MsgDailyLog` and `MsgTimeLog` control the operation of message logging.

Starting the Databridge
To start the Databridge, use either the Windows Services console, or the command-line or shell prompt.

About this task

Note: If the ObjectServer module is connected to the Databridge, ensure that its target system is running before starting the Databridge. If any of the Databridge modules fails to initialize correctly, the Databridge will not start.

To start the Databridge from the command prompt on Windows, use the command:

```
%ISMHOME%\platform\win32\bin
```

To start the Databridge from the command-line or shell prompt on UNIX, use the command:

```
$ISMHOME/bin/nco_m_bridge
```

Procedure

To start the Databridge from the Services console:

1. From the Windows desktop, select **Start** > **Administrative Tools** > **Services**.
2. From the list of services, select the service named `NCO BRIDGE Internet Service Monitor`, then select **Start** from the context menu.

Connecting modules
The Databridge properties file defines the modules to connect to the Databridge.

About this task
Each `Module`*n*`SharedLib` and `Module`*n*`PropFile` property pair defines the connection for one module. Modules are loaded in order of definition, starting from `Module0`.

To connect individual modules to the Databridge:

1. In the Databridge properties file, identify the next available `Module`*n*`SharedLib` and `Module`*n*`PropFile` property pair.
2. Set `Module`*n*`SharedLib` to the name of the module's shared library (its binary implementation).
3. Set `Module`*n*`PropFile` to the full path of the module's properties file.

To connect all modules to the Databridge on UNIX, add the following entries to the Databridge properties file `$ISMHOME/etc/props/bridge.props`:

```
[1]Module0PropFile        : "$ISMHOME/etc/props/objectserver.props"
[2]Module0SharedLib       : "libSMModuleObjectServer"
[3]Module1PropFile        : ""
[4]Module1SharedLib       : "libSMModuleDatalog"
[5]Module2PropFile        : "$ISMHOME/etc/props/pipe_module.props"
[6]Module2SharedLib       : "libSMModulePipe"
```

In this example, lines 1 and 2 connect the ObjectServer module, lines 3 and 4 connect the Datalog module, lines 5 and 6 connect the IBM Tivoli Monitoring (`pipe`) module. The Datalog module does not have a properties file, so the entry for the properties file has the value `""`.

Disabling modules
To disable a module, set the corresponding `Module`*n*`SharedLib` property to `"NONE"` and the `Module`*n*`PropFile` property to `""`. All other modules that have a value higher than *n* are also ignored.

Connecting monitors

Internet service monitors connect to the Databridge over TCP. Each monitor has a set of properties that configure the connection to the Databridge.

About this task

To connect a monitor to the Databridge, set the value of the `BridgePort` property defined in the monitor's properties file to the value of the `SocketPort` property defined in the Databridge properties file. The default value of each monitor's `BridgePort` property and the Databridge's `SocketPort` property is `9510`.

The Databridge supports SSL encryption of the test results that it receives from the monitors. To encrypt a monitor's test results, set the values of the `BridgeSSL` properties defined in the monitor's properties file to the values of the `BridgeSSL` properties defined in the Databridge properties file. To encrypt all monitors' test results, all monitors must have the same `BridgeSSL` properties.

Configuring the IBM Tivoli Monitoring module

The IBM Tivoli Monitoring module directs test results to the Internet service monitoring agent. The monitoring agent converts this data to the required format and distributes it to the Tivoli Enterprise Monitoring Server.

You configure both the IBM Tivoli Monitoring module and the Internet service monitoring agent through their respective properties files.

IBM Tivoli Monitoring properties

You configure the operation of the IBM Tivoli Monitoring module by modifying the property values defined in the module properties file.

The module properties file is named `pipe_module.props`. This file is located in the `$ISMHOME/etc/props/` directory.

Table 7 on page 47 lists the properties available for the module. If you make changes to the properties, you must restart the Databridge for those changes to take effect.

Table 7. IBM Tivoli Monitoring module properties

Property name	Type	Description
TEMAHOST	string	The name of the host running the monitoring agent. Default: `localhost`
TEMAPORT	integer	The port number used by the host. Default: `9520`

Internet Service Monitoring agent properties

You configure the operation of the Internet service monitoring agent by modifying the property values defined in the monitoring agent properties file.

The monitoring agent properties file is named `kisagent.props`. This file is located in the `$ISMHOME/etc/props/` directory.

Table 8 on page 48 lists the properties available for the monitoring agent.

Table 8. Monitoring agent properties		
Property name	**Type**	**Description**
TEMAPORT	integer	The port number used by the host. This must be the same as the port number for the TEMAPORT property listed in the module properties file. Default: 9520
ObsoleteDuration	integer	The time, in seconds, after which any data that has not been updated is deleted from the monitoring agent's memory. Data might not be updated when, for example, a profile element has been stopped or a network failure has occurred. **Note:** Do not set the ObsoleteDuration time to a value less than the poll interval because this results in loss of data between poll intervals. Default: 900
AggDuration	integer	The time, in seconds, after which the monitoring agent stops data from being aggregated and reported in statistical workspaces. Any data that is older than the specified time is deleted from the monitoring agent's memory. Older data is calculated by comparing the interval between the start and the current time to the aggregate duration time. If the interval is greater than the aggregate duration time, 10% of the older data is removed and the start time is increased by 1/10th of the interval. The monitoring agent performs this calculation every five minutes. Default: 3600
ManageServices	0|1	Starts and stops all monitors and the Databridge when the Internet Service Monitoring agent is started or stopped. 1 is enabled, and 0 is disabled. Default: 1

Connecting the Internet Service Monitoring agent
The connection between the Internet service monitoring agent and the IBM Tivoli Monitoring module is created when you install Internet Service Monitoring.

Connection information for UNIX is located in $CANDLE_HOME/config/. For Windows, connection information is stored in the kisenv configuration file located in %CANDLE_HOME%/TMAITM6/.

Configuring the ObjectServer module

The ObjectServer module converts events into alerts which it then forwards to the ObjectServer IBM Tivoli Netcool/OMNIbus ObjectServer.

The operation of the ObjectServer module is very similar to ObjectServer IBM Tivoli Netcool/OMNIbus probes except that its data source is the event stream received from monitors rather than a network device. Using a rules file, the ObjectServer module converts elements contained in monitor events into fields in ObjectServerIBM Tivoli Netcool/OMNIbus alerts, which it sends to an ObjectServer. The ObjectServer module uses *all* rules in the rules file. Table 9 on page 49 lists the files associated with the ObjectServer module.

Table 9. ObjectServer module files and their location	
Module file	**Location and/or name**
Library	`libSMModuleObjectServer`
Log file	`$ISMHOME/log/objectserver.log`
Properties file	`$ISMHOME/etc/props/objectserver.props`
Rules file	`$ISMHOME/etc/rules/objectserver.rules`

Releases before Internet Service Monitoring 6.0.0 included multiple ObjectServer modules, however version 6.0.0 and higher provides one common module, `libSMModuleObjectServer`, for connecting to all ObjectServers.

ObjectServer properties

You can configure the operation of the ObjectServer module by modifying the property values defined in the ObjectServer module properties file.

Table 10 on page 49 lists the properties available for the ObjectServer module. If you make changes to the properties, you must restart the Databridge for those changes to take effect.

Table 10. ObjectServer module properties		
Property name	**Type**	**Description**
`AuthPassword`	string	Specifies the password associated with the username that the ObjectServer module uses to authenticate itself when the target ObjectServer is running in secure mode. This password must be encrypted with the `nco_crypt` utility. Default: `""`
`AuthUserName`	string	Specifies the username that the ObjectServer module uses to authenticate itself when the target ObjectServer is running in secure mode. Default: `""`
`AutoSAF`	`0`|`1`	Enables automatic store and forward mode: • `0` - Disabled • `1` - Enabled
`Buffering`	`0`|`1`	Enables buffering of alerts: • `0` - Disabled • `1` - Enabled
`BufferSize`	integer	Sets the number of status messages that the ObjectServer module stores in its buffer. Default: `10`

Table 10. ObjectServer module properties (continued)		
Property name	**Type**	**Description**
LookupTableMode	0|1|3	Specifies how table lookups are performed: • 1 - All external lookup tables are assumed to have a single value column. Tabs are not used as column delimiters. • 2 - All external lookup tables are assumed to have multiple columns. If the number of columns on each line is not the same, an error is generated that includes the file name and the line on which the error occurred. • 3 - The rules engine attempts to determine the number of columns in the external lookup table. An error is generated for each line that has a different column count from the previous line. The error includes the file name and the line on which the error occurred. For detailed information about lookup table operations, see the *ObjectServer IBM Tivoli Netcool/OMNIbus Probe and Gateway Guide*.
MaxLogFileSize	integer	Specifies the maximum size of the log file (in bytes) before it rolls over to the objectserver_old.log file. Default: 1
MaxRawFileSize	integer	Specifies the maximum size of the raw capture file in kilobytes. If RawCaptureFileBackup is disabled, this property is ignored. If RawCaptureFileBackup is enabled, this property specifies the approximate file size at which a new file is started. Default: -1 (unlimited size)
MaxSAFFileSize	integer	Specifies the maximum size of the store and forward file (in bytes). Default: 1MB
MessageLog	string	Specifies the location of the ObjectServer module log file. Default: $ISMHOME/log/objectserver.log
NetworkTimeout	integer	Specifies the period (in seconds) after which the connection to an ObjectServer will time out if a network failure occurs. Default: 0 (no timeout)
RawCapture	0|1	Controls the raw capture mode: • 0 - Disabled • 1 - Enabled

Table 10. ObjectServer module properties (continued)

Property name	Type	Description
RawCaptureFileAppend	0|1	If specified, new data is appended to the existing raw capture file, instead of overwriting it: • 0 - Overwrite • 1 - Append
RawCaptureFileBackup	0|1	Enables backup of the raw capture file when it exceeds the maximum file size specified by the MaxRawFileSize property: • 0 - Disabled • 1 - Enabled
RawCaptureFile	string	The name of the raw capture file. Default: $ISMHOME/var/objectserver.cap
RetryConnectionCount	integer	The number of events the probe must process in store and forward mode before trying to connect to the ObjectServer. Default: 15
RetryConnectionTimeOut	integer	The number of seconds the probe must process events in store and forward mode before trying to connect to the ObjectServer. Default: 30
RulesFile	string	Specifies the location and filename of the ObjectServer module rules file. Default: $ISMHOME/etc/rules/objectserver.rules
SAFFileName	string	The name of the ObjectServer module store and forward file. Default: $ISMHOME/var/objectserver.saf.*name*, where *name* is the name of the target ObjectServer.
Server	string	Specifies the name of the ObjectServer to which the ObjectServer module sends the events generated from the Internet service monitors. Default: NCOMS
ServerBackup	string	Defines a secondary ObjectServer if the primary ObjectServer connection fails. If NetworkTimeout is set and a virtual ObjectServer is in use, use ServerBackup to refer to your secondary ObjectServer. Default: ""
StoreAndForward	0|1	Controls the store and forward operations: • 0 - Disabled • 1 - Enabled

On Windows, specify path separators using \ in place of /.

Raw capture mode

Like probes, the ObjectServer module provides a raw capture mode in which it saves the complete stream of events into a file without any processing by the rules file. This mode is useful for auditing, recording, or debugging the ObjectServer module.

The `RawCapture`, `RawCaptureFile`, `RawCaptureFileAppend`, `RawCaptureFileBackup`, and `MaxRawFileSize` ObjectServer properties control the operation of raw capture mode.

Store And Forward mode

The ObjectServer module provides a Store And Forward (SAF) mode for fault-tolerant operation.

The module enters SAF mode if it is unable to send alerts to the target ObjectServer, for example if the network connection between the two systems fails. In SAF mode, the module stores alert information in a file instead of sending it to the ObjectServer. When the ObjectServer becomes available again, the module forwards all alerts stored in the SAF file and returns to normal operation.

The `AutoSAF` and `StoreAndForward` properties control the operation of SAF mode. When AutoSAF has the value 1, the module enters SAF mode if the target ObjectServer is either unavailable when the Databridge starts, or if it becomes unavailable while the Databridge is running. When `StoreAndForward` has the value 1, the module only enters SAF mode if the target ObjectServer becomes unavailable while the Databridge is running; the Databridge will not start if the ObjectServer is unavailable.

If both `AutoSAF` and `StoreAndForward` have the value 1, `AutoSAF` takes precedence. The `SAFFileName` and `MaxSAFFileSize` ObjectServer properties define the name and size of the SAF file.

Rules files

The ObjectServer module and each Internet service monitor provide a rules file for converting monitor events into alert information which is used by ObjectServer IBM Tivoli Netcool/OMNIbus.

The ObjectServer module's rules file acts as a wrapper for individual Internet service monitor rules files, each of which contains rules specific to the elements generated by that monitor.

Note: To define lookup tables for processing events generated by a specific monitor, define them at the start of the ObjectServer rules file rather than in the monitor rules file. Rules file parsing requires that lookup tables appear before any processing statement, so any lookup tables that are defined in a monitor rules file result in parser errors in the ObjectServer rules file.

If you modify the rules files, you must restart the Databridge for the changes to take effect. On UNIX, you can force the ObjectServer module to re-read the rules files by issuing the command `kill -HUP pid`, where `pid` is the process ID of the ObjectServer module process. For information about rules files and their syntax, see the *IBM Tivoli Netcool/OMNIbus Probe and Gateway Guide*. By default, rules files are located in the `$ISMHOME/etc/rules` directory.

Log file

The ObjectServer module reports information about its operations to a log file.

The `MessageLog` property specifies the location of the log file. The `MaxLogFileSize` property specifies the size of the log file before it rolls over to the `objectserver_old.log` file.

Connecting to the ObjectServer

The ObjectServer module properties file defines the ObjectServer IBM Tivoli Netcool/OMNIbus ObjectServer to which the ObjectServer module sends alert information.

To configure the module to connect to the ObjectServer, set the `Server` property to the name of the ObjectServer.

Note: When connecting the ObjectServer module, ensure that the target ObjectServer IBM Tivoli Netcool/OMNIbus is running before starting the Databridge.

If the target ObjectServer is running in secure mode, the ObjectServer module must authenticate itself when connecting to it. The `AuthUserName` and `AuthPassword` properties define the credentials that the ObjectServer module uses during authentication. Encrypt passwords using the `nco_g_crypt` utility. For more information about this utility, see the *ObjectServer IBM Tivoli Netcool/OMNIbus ObjectServer Administration Guide*.

Connecting to the ObjectServer on UNIX

To configure the connection of the ObjectServer module to an ObjectServer on UNIX:

- Ensure that the connections data file $ISMHOME/objectserver/etc/omni.dat contains an entry for the target ObjectServer. If it does not, add one to the file using the format:

  ```
  [OBJSERVERNAME] {Primary: hostname port}
  ```

  where OBJSERVERNAME is the name of the target ObjectServer, and hostname and port represent the DNS name, or IP address, and port of the system on which the ObjectServer is running.
- Generate an interfaces file using the command:

  ```
  $ISMHOME/objectserver/bin/nco_igen
  ```

Connecting to the ObjectServer on Windows

To configure the connection to the ObjectServer on Windows, add the following entry for the target ObjectServer in the connections data file $ISMHOME\objectserver\ini\sql.ini:

```
[OBJSERVERNAME]
master=NLWNSCK,hostname,port
query=NLWNSCK,host,port
```

where OBJSERVERNAME is the name of the target ObjectServer, and hostname and port represent the DNS name, or IP address, and port of the system on which the ObjectServer is running.

Configuring the Datalog module

The Datalog module generates XML datalog files from the test results received from the Internet service monitors. You can store the datalog files on a local host for archiving purposes or for generating simple reports.

The Datalog module does not have a properties file. The file associated with the Datalog module is the libSMModuleDatalog library file.

Note: Datalogs can occupy a large amount of disk space. See “Disk space requirements” on page 54 for a guideline on calculating the amount of disk space required.

Datalog files

Datalog files store the monitor data generated for a profile element over a 24-hour period. Datalog files can be used for testing or basic reporting purposes and are mainly used by customers who have developed their own reporting tools.

Datalogs are located in subdirectories in $ISMHOME/datalogs on the local host. The datalogs are grouped by profile and profile element name. Datalog filenames have the format *YYYYMMDD*.xml, where *YYYYMMDD* represents the monitoring period.

The format of the monitor data in the datalog files is defined by a set of default datalogs.

Default datalog file

The default datalog file determines the format of the monitor data in datalog files.

Each time the Datalog module generates a new datalog file, it uses the default datalog file for the corresponding monitor as a template. The default datalog files are stored in $ISMHOME/datalogs/default.

Note: Before modifying a default datalog file, create a backup copy of the original.

Enabling data logging

Datalog files store the test results data received from the Internet services monitors. When you enable data logging, you can store the datalog files for archiving purposes or for generating simple reports.

Procedure

To enable data logging:

1. Make sure that the Datalog module is connected to the Databridge.
2. Set the `Datalog` property in each monitor's properties file to 1.

Disk space requirements

Datalogs are created by the Databridge Datalog module. These datalogs can occupy a large amount of disk space.

Note: Typically the Datalog module is not required; it is disabled by default.

To calculate the amount of disk space required by datalog files, use the following formula:

```
(600 / poll_interval) × 15 KB per profile element per day
```

For example, a single HTTP profile element polling a web page every 5 minutes for one year would require 10.95 MB of disk space:

```
(600 / (5 × 60)) × 15 × 365 = 10.95 MB
```

Chapter 6. Working remotely

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

Note: For complete information about remote deployment, see chapter *Deploying monitoring agents across your environment* in the *IBM Tivoli Monitoring Installation and Setup Guide*.

Table 11 on page 55 describes the steps required to set up and manage remote agent deployment:

Table 11. Remote agent deployment tasks

Goal	Where to find information
Create and populate the agent deploy depot with installable agent images	"Populating the agent depot" on page 55
Manage the agent depot	"Managing your agent depot" on page 59
Use one agent depot for all the monitoring servers in your monitoring environment.	"Sharing an agent depot across your environment" on page 59
Deploy OS agents	"Deploying OS agents" on page 60
Deploy non-OS agents	"Deploying non-OS agents" on page 61
Upgrade non-OS agents remotely	"Upgrading non-OS agents remotely" on page 63
Remove non-OS agents remotely	"Removing non-OS agents remotely" on page 63

Note: After you have deployed an agent, you can reconfigure it. Right-click on the agent in the Tivoli Enterprise Portal and select **Configure**. For more information about post-configuration tasks, see the section *Post-installation configuration and customization* in the *IBM Tivoli Monitoring Installation and Setup Guide*.

You can also use the remote agent deployment function to configure deployed agents and install maintenance on your agents. For information, see the *IBM Tivoli Monitoring Administrator's Guide*. See the *IBM Tivoli Monitoring Command Reference* for commands that you can use to perform these tasks.

Important:

> Run the **`tacmd login`** command before executing commands from the `tacmd` library. This requirement does not apply to the `addBundles` command. Run the **`tacmd logoff`** command after you finish using the `tacmd` command library.

Note: If you install an agent manually and then perform a remote uninstall, the remote uninstall does not remove the entry from Windows Add/Remove program. You must remove the entry manually.

Populating the agent depot

The *agent depot* is an installation directory on the monitoring server from which you deploy agents and maintenance packages across your environment. Before you can deploy any agents from a monitoring server, you must first populate the agent depot with bundles. A bundle is the agent installation image and any prerequisites.

When you add a bundle to the agent depot, you need to add the bundle that supports the operating system to which you want to deploy the bundle. For example, if you have a Windows Tivoli Enterprise Monitoring Server and Web Response Time agent on Linux and you want to remote configure the Linux agent, the Tivoli Enterprise Monitoring Server must have the Web Response Time Linux package in the

depot. (If you are installing from different media for each platform type, for example, Windows, AIX and Solaris, HP-UX, Linux, you need to add the bundle from the specific platform media for the component.)

You can have an agent depot on each monitoring server in your environment or share an agent depot, as described in "Sharing an agent depot across your environment" on page 59. If you choose to have an agent depot for each monitoring server, you can customize the agent depot based on the types of bundles that you want to deploy and manage from that monitoring server. For example, if you have a monitoring server dedicated to monitoring with Web Response Time agents, populate the depot with Web Response Time-related agent bundles. If you deploy an agent from a remote monitoring server, you must have a agent bundle in the depot available to the monitoring server.

Note: Agent depots cannot be located on a z/OS® monitoring server.

There are two methods to populate an agent depot:

- Populating the agent depot from the installation image
  - "Populating the agent depot during installation: Windows" on page 56
  - "Populating the agent depot during installation: Linux and UNIX" on page 57
- "Populating an agent depot with the tacmd addBundles command" on page 58

You can use the installation image to populate the agent depot only when you are populating the depot with bundles for the same operating system as your monitoring server. For example, you can use the installation image to add a bundle for a Windows agent to a Windows monitoring server, but you cannot use the Linux installation image to add a Linux bundle to a Windows monitoring server. If you need to add bundles for operating systems other than that used by your monitoring server, use the `tacmd addBundles` command, as described in "Populating an agent depot with the tacmd addBundles command" on page 58.

Note:

Only Tivoli-provided product agent bundles should be loaded into the IBM Tivoli Monitoring deployment depot. User-provided or customized bundles are not supported. Use only Tivoli provided tacmd commands to process bundles and to execute agent deployments. Manual manipulation of the depot directory structure or the bundles and files within it is not supported and may void your warranty.

Populating the agent depot during installation: 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 in this section that applies to the image you are using:

- Base IBM Tivoli Monitoring installation image
- Application agent installation image

Base IBM Tivoli Monitoring installation image:

Use the following steps to populate the agent depot from the IBM Tivoli Monitoring installation image:

1. Launch the installation wizard by double-clicking the `setup.exe` file in the `\Windows` subdirectory of the installation image.
2. Click **Modify** on the Welcome window and select **Next**.
3. Click **OK** the warning message regarding existing components on this computer.
4. Click **Next** on the Add or Remove Features window without making any changes. (Do not clear any selected items because this removes them from the computer.)
5. On the Agent Deployment window, select the agents that you want to add to the depot and click **Next**.
6. Review the installation summary and click Next to begin the installation. After the agents are added to the agent depot, a configuration window (called the Setup Type window) is displayed.
7. Clear all selected components. You have already configured all components on this computer and do not need to reconfigure any now. Click **Next.**

8. Click **Finish** to complete the installation.
9. Click **Finish** on the Maintenance Complete window.

Application agent installation image:

Use the following steps to populate the agent depot from an application agent installation image:

1. Launch the installation wizard by double-clicking the `setup.exe` file in the `\Windows` subdirectory of the installation image.
2. Click **Next** on the Welcome window.
3. Click **Next** on the Select Features window without making any changes.
4. On the Agent Deployment window, select the agents that you want to add to the depot and click **Next**.
5. Review the installation summary and click **Next** to begin the installation. After the agents are added to the agent depot, a configuration window (called the Setup Type window) is displayed.
6. Clear all selected components. You have already configured all components on this computer and do not need to reconfigure any now. Click **Next.**
7. Click **Finish** to complete the installation.
8. Click **Finish** on the Maintenance Complete window.

Populating the agent depot during installation: Linux and UNIX

Populating the agent depot during a Linux and UNIX installation.

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

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

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

Type 2 to start the installation and press Enter.
```

   The end user license agreement is displayed. Press Enter to read through the agreement.
5. Type 1 to accept the agreement and press Enter.
6. Type the number that corresponds to the agent or agents that you want to add to the agent depot and press Enter. If you are going to add more than one agent, use a comma (,) to separate the numbers. To select all available agents, type `all`. You can select multiple agents with consecutive corresponding numbers by typing the first and last numbers for the agents, separated by a hyphen (-). For example, to add all of the agents between 8 and 12, type 8-12. To clear an agent that you previously selected, type the number for the agent again.

   Note: Use the following keys to navigate the list of agents:

   U Moves up a line in the list.

   D Moves down a line in the list.

   F Moves forward one page in the list.

   B Moves back one page in the list.
7. When you have specified all the agents that you want to add to the agent depot, type E and press Enter to exit.

Populating an agent depot with the tacmd addBundles command

Populating an agent depot with the **tacmd addBundles** command.

To add bundles for operating systems other than that used by your monitoring server, use the tacmd addBundles command.

Restriction: Only Tivoli-provided product agent bundles should be loaded into the IBM Tivoli Monitoring deployment depot. User-provided or customized bundles are not supported. Use only Tivoli provided tacmd commands to process bundles and to execute agent deployments. Manual manipulation of the depot directory structure or the bundles and files in it is not supported and may void your warranty.

Important: Run the tacmd login command before executing commands from the tacmd library. Run the tacmd logoff command after you finish using the tacmd command library.

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

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

For the full syntax, including parameter descriptions, see *IBM Tivoli Monitoring Command Reference*.

Examples:

- The following example copies every agent bundle, including its prerequisites into the agent depot on a UNIX from the installation media (cd image) located at /mnt/cdrom/:

  ```
  tacmd addBundles -i /mnt/cdrom/unix
  ```

- The following example copies all agent bundles for the Oracle agent into the agent depot on a UNIX computer from the installation media (cd image) located at /mnt/cdrom/:

  ```
  tacmd addBundles -i /mnt/cdrom/unix -t or
  ```

- The following example copies all agent bundles for the Oracle agent into the agent depot on a Windows computer from the installation media (cd image) located at D:\WINDOWS\Deploy:

  ```
  tacmd addBundles -i D:\WINDOWS\Deploy -t or
  ```

- The following example copies the agent bundle for the Oracle agent that runs on the AIX version 5.1.3 operating system into the agent depot on a UNIX computer from the installation media (cd image) located at/mnt/cdrom/:

  ```
  tacmd addbundles -i /mnt/cdrom/unix -t or -p aix513
  ```

By default, the agent depot is located in the %CANDLE_HOME%\CMS*depot_directory* on Windows and $CANDLE_HOME/tables/*tems_name*/depot directory on UNIX. The **tacmd addBundles** command puts the agent bundle in that location unless another location is defined in the monitoring server configuration file for DEPOTHOME.

If you want to change this location, do the following before you run the tacmd addBundles command:

1. Open the KBBENV monitoring server configuration file located in the %CANDLE_HOME%/CMS/ directory on Windows and the $CANDLE_HOME/tables/*tems_name* directory on Linux and UNIX.
2. Locate the DEPOTHOME variable. If it does not exist, add it to the file.
3. Type the path to the directory that you want to use for the agent depot.
4. Save and close the file.
5. On UNIX or Linux only, add the same variable and location to the kbbenv.ini file located in $CANDLE_HOME/config/kbbenv.ini.

Note: If you do not add the variable to the kbbenv.ini file, it is deleted from the KBBENV file the next time the monitoring server is configured.

Managing your agent depot

Use the following commands to manage your agent depot:

Table 12. Agent depot management commands

Command	Description
`tacmd listbundles`	Lists the details for one or more bundles available to be added to the local agent depot.
`tacmd removebundles`	Deletes one or more bundles from the local agent depot.
`tacmd viewdepot`	Lists the types of bundles available in either the local or remote agent depot.

See the IBM Tivoli Monitoring Command Reference for the full syntax of these commands.

Important: Only Tivoli-provided product agent bundles should be loaded into the IBM Tivoli Monitoring deployment depot. User-provided or customized bundles are not supported. Use only Tivoli provided tacmd commands to process bundles and to execute agent deployments. Manual manipulation of the depot directory structure or the bundles and files within it is not supported and may void your warranty.

Sharing an agent depot across your environment

If your monitoring environment includes multiple monitoring servers (a hub monitoring server and remote monitoring servers), you can put your agent depot in a central location, such as a shared file system, and access the depot from all of the monitoring servers.

After populating your agent depot with either of the methods described in "Populating the agent depot" on page 55, use the following steps to share the agent depot:

1. Open the KBBENV monitoring server configuration file located in the %CANDLE_HOME%\CMS directory on Windows systems, and the $CANDLE_HOME/tables/*tems_name* directory on Linux and UNIX systems.
2. Locate the *DEPOTHOME* variable. By default, the agent depot is located in the %CANDLE_HOME%\CMS *depot_directory* on Windows systems, and the $CANDLE_HOME/tables/*tems_name*/*depot_directory* on UNIX or Linux systems.
3. Type the path to the shared agent depot for the *DEPOTHOME* variable.
4. Save and close the file.
5. On UNIX or Linux systems only, add the same variable and location to the kbbenv.ini file located in $CANDLE_HOME/config/kbbenv.ini.

   Note: If you do not add the variable to the kbbenv.ini file, it will be deleted from the KBBENV file the next time the monitoring server is reconfigured.

If you are using a Windows monitoring server connecting to a depot on another Windows computer, you must set the service ID for the Windows monitoring server to **Administrator**. Also, instead of specifying a mapped drive letter for the path to the depot directory, use the UNC path (such as \\server\share).

Use the following steps to change the service ID:

1. From the Control Panel, double-click **Administrative Tools** then **Services**.
2. Select **Tivoli Enterprise Monitoring Svcs** > **Properties**.
3. On the **Log On** tab, select **This Account**.
4. Type Administrator in the **This Account** field.

5. Type the password for the administrator in the **Password** field. Confirm the password by typing it again in the **Confirm password** field.
6. Click **Enable**.

   If the Administrator user does not have Logon as a service right, you are prompted to add it.

Deploying OS agents

Before you can deploy any non-OS agent, you must first install an OS agent on the computer where you want the non-OS agent to be deployed.

In addition to monitoring base OS performance, the OS agent also installs the required infrastructure for remote deployment and maintenance.

Note: Ensure that you have populated your agent depot, as described in "Populating the agent depot" on page 55, before attempting to deploy any agents.

You can install the OS agent locally, as described in Integrating 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.

Requirements for the tacmd createNode command

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

- On Windows, the user ID that you specify using the -u parameter must have administrator privileges on the target computer. On UNIX and Linux, you must specify the *root* user ID using the **-u** parameter and the root password using the **-p** parameter for the **tacmd createNode** command to execute correctly. No other user ID may be specified.
- Any computer to which you want to deploy the OS agent must have a supported protocol installed.
- Security in your environment must be configured to permit **createNode** to pass through the firewall, using the protocol that you specify in the command parameters.
- On Windows computers:
  - SMB requires that the default, hidden, and administrative share are available on the drive being accessed and on the drive that hosts the System temporary directory.
  - SMB signing is not supported when connecting using SMB. The computer to which you are deploying an OS agent cannot require SMB signing.
  - For Windows XP, disable Simple File Sharing. Simple File Sharing requires that all users authenticate with guest privileges. This is not supported for createNode. To disable Simple File Sharing, do the following:
    1. Open the Windows Explorer.
    2. Select **Tools** > **Folder Options**.
    3. On the **View** tab, scroll through the list of settings to **Use Simple File Sharing**.
    4. Clear the check box for **Use Simple File Sharing** and click **OK**.
  - For Windows XP computers with Service Pack 2, disable the **Internet Connection Firewall**.

  - For Windows XP computers, set **Network Access Sharing and Security** to `Classic - local users authenticate as themselves`. Use the following steps:
    1. From the Control Panel, double-click **Administrative Tools**.
    2. Double-click **Local Security Policy**.
    3. Select **Local Policies** > **Security Options**.
    4. Right-click **Network access**: **Sharing and security for local accounts** and click **Properties**.
    5. Select **Classic - local users authenticate as themselves** from the list and click **OK**.
  - For all Windows computers, enable remote registry administration. (This is enabled by default.)
- On UNIX systems, if you are using the RSH protocol, run the **`tacmd createNode`** command as root on the monitoring server.
- If you are deploying the OS agent to a UNIX or Linux computer, that computer must have the ksh shell. Only the Korn shell is supported for the execution of the installation and runtime scripts.
- If you are using SSH V2 (for either Windows or UNIX), configure SSH on the target computers to permit the use of password authentication. To permit this, do the following:
  1. Edit the `/etc/ssh/sshd_config` file on the target computer.
  2. Locate the following line: `PasswordAuthentication`.
  3. Change `no` to `yes` and save the file.
  4. Restart the daemon.

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

Using the tacmd createNode command

To deploy an OS agent from the command line interface, use **`tacmd createNode`** command. For the full syntax, including parameter descriptions, see *IBM Tivoli Monitoring Command Reference.*

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

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

Important:

Unless you specifically indicate otherwise, the agent that you deploy using this command assumes that the monitoring server to which it connects is the monitoring server from which you run the command. The agent also uses the default settings for the communications protocol (IP.PIPE for protocol type and 1918 for the port). To change these defaults (especially if you are not using the IP.PIPE protocol), use the following property (specified with the **`-p`** parameter) when running the command: **`SERVER=[PROTOCOL://][HOST|IP][:PORT]`**. For example, **`SERVER=IP.PIPE://server1.ibm.com:1918`**.

Deploying non-OS agents

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

- 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 Integrating.
- Ensure that you have populated your agent depot, as described in “Populating the agent depot” on page 55, before attempting to deploy any agents.
- You must have already installed an OS agent on the computer where you are now deploying the non-OS agent and the agent must be running.

Deploying agents using the Tivoli Enterprise Portal

Before you deploy an agent using the Tivoli Enterprise Portal, application support for that agent must be installed on the portal server (see Install application support for Linux and UNIX or Install application support for Windows systems).

Use the following steps to deploy an agent through the Tivoli Enterprise Portal:

1. Open the Tivoli Enterprise Portal.
2. In the Navigation tree, navigate to the computer to which you want to deploy the agent.
3. Right-click the computer and click **Add Managed System**.
4. In the **Select a Monitoring Agent** window, select the agent that you want to deploy and click **OK**.
5. In the **New Managed System Configuration** window, 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**.

   If the computer where you are deploying the agent already has a version of that agent installed, you can stop the deployment, add a new instance of the agent, if possible, or reconfigure the existing agent.

   A message will tell you when the deployment finishes successfully.

Deploying agents through the command line

To deploy non-OS agents from the command line, use the **tacmd addSystem** command. See the *IBM Tivoli Monitoring Command Reference* for the full syntax of this command, including parameter descriptions. You can run the **cinfo** command on UNIX systems, or the **kincinfo -i** command on Windows systems to list the product codes for agents installed on the current computer.

For example, the following command deploys the Application Management Console using the CLI syntax **tacmd addSystem** {-t|--type} *pc* {-n|--node} *MANAGED-OS* {-p|--property},

where

-t|--type
Specifies the type of agent to add to the monitoring system.

-n|--node
Identifies the node or the directory on the monitoring system where the OS agent is installed, to which you want to add the agent. The name of a node includes the computer where the OS agent is installed and the product code for the OS agent. For example, `stone.ibm.com:LZ` is the name of the node on computer `stone.ibm.com`, which has a Linux OS agent installed.

-p|--property
Specifies `SECTION.NAME=VALUE` pairs that identify agent configuration properties and their values, where `SECTION` specifies the name of the section containing the key-value pair. `KEY` specifies the name of the configuration property, and `VALUE` specifies the property value. Refer to the agent configuration chapters for the agent that you want to deploy in Integrating to obtain the`KEY/VALUE` pairs. See *IBM Tivoli Monitoring: Installation and Setup Guide* for complete details on using the `property SECTION.NAME=VALUE` pairs.

Each agent bundle has its own unique configuration parameters that you need to provide in this command. If you have an installed agent of the same type that you want to deploy, you can view the configuration parameters by running the following command from a monitoring server:

```
tacmd describeSystemType -t pc -p platform
```

An agent of the same type and platform must be deployed into the depot available to the monitoring server from which the command is run. For more information about agent-specific parameters, see the configuration chapters for the agent that you want to deploy in Integrating.

Note: If you deploy a Web Response Time agent to a Windows system remotely, ensure that you restart the target system after you have deployed the agent.

Upgrading non-OS agents remotely

You can upgrade non-OS agents from the command line.

- 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 Integrating.
- Ensure that you have populated your agent depot, as described in "Populating the agent depot" on page 55, before attempting to deploy any agents.
- You must have already installed an OS agent on the computer where you are now deploying the non-OS agent and the agent must be running.

Upgrading through the command line

To upgrade non-OS agents from the command line, use the **tacmd updateagent** command.

See the *IBM Tivoli Monitoring Command Reference* for the full syntax of this command, including parameter descriptions.

You can run the **cinfo** command on UNIX systems, or the **kincinfo -i** command on Windows systems to list the product codes for agents installed on the current computer.

Note: If you deploy a Web Response Time agent to a Windows system remotely, ensure that you restart the target system after you have deployed the agent.

Removing non-OS agents remotely

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

You can also uninstall non-OS agents from the Tivoli Enterprise Portal by stopping the agent and removing its configuration settings. After you have removed the agent from the Tivoli Enterprise Portal, you can completely uninstall the agent from the managed system. When you remove an agent, it is removed from any managed system lists to which it is assigned, any situation or policy distribution lists it was on, and any custom Navigator view items to which it was assigned.

Removing using the Tivoli Enterprise Portal

To remove a non-OS agent using the GUI:

1. Open the Tivoli Enterprise Portal.
2. In the Navigation tree, navigate to the computer from which you want to remove the agent.
3. Right-click the agent that you want to remove and select **Remove**.
4. Click **Yes** when you are asked to confirm the removal of the agent.
5. Click **Yes** when you are asked to confirm that you want to permanently uninstall the agent.

Removing through the command line

To remove non-OS agents from the command line, use the **tacmd removeSystem** command:

```
tacmd removeSystem -t product code -n Managed-OS
```

For example, to remove the Transaction Collector from `ibm001` which uses a Linux OS agent:

```
./tacmd removeSystem -t TU -n ibm001:LZ
```

See the *IBM Tivoli Monitoring Command Reference* for the full syntax of this command, including parameter descriptions.

You can run the **cinfo** command (UNIX) or the **kincinfo -i** command (Windows) to list the product codes for agents installed on the current computer.

Chapter 7. Configuring the Eclipse help server

You must configure the Tivoli Enterprise Portal client's Eclipse help server after installation is complete.

Before you begin

- Find out the port number for the Tivoli Enterprise Portal from the person who installed IBM Tivoli Monitoring.
- If you are using an IBM Tivoli Monitoring version 6.1 with Fix Pack 3 on UNIX or Linux systems, the Eclipse server cannot start when it is installed. To resolve this problem, upgrade to ITM V6.2 FP1 iFix 1.

Procedure

1. Start Manage Tivoli Monitoring Services:

Windows	UNIX and Linux
Click **Start** > **All Programs** > **IBM Tivoli Monitoring** > **Manage Tivoli Monitoring Services**	Run the following command: **./itmcmd manage**

   Note: The user interface might vary slightly, depending on the operating system.
2. Locate the Eclipse Help Server entry.
   a. If `Configured` displays `Yes`, go to step "4" on page 65.
   b. If `Configured` displays `No`, go to step "3" on page 65.
3. To configure the Eclipse Help Server:
   a. Right-click the Eclipse Help Server entry.
   b. Select **Configure Using Defaults** from the pop-up menu.
   c. Enter the port number specified when installing IBM Tivoli Monitoring.
   d. Click **OK**.
4. To set up the Eclipse help to automatically start the whenever this node is restarted,
   a. Right-click the **Eclipse Help Server** entry.
   b. Select **Change Startup** from the pop-up menu to display the Service Startup for Eclipse Help Server window.
   c. Select **Automatic** at **Startup Type**.
   d. Click **OK**.

Chapter 8. Starting and stopping servers and agents

Start and stop IBM Tivoli Monitoring components and Tivoli Enterprise Management Agents using the Manage Tivoli Enterprise Monitoring Services, or the command line.

Starting and stopping the Tivoli Enterprise Monitoring Server

Follow these directions to start or stop the Tivoli Enterprise Monitoring Server.

Start the server

On Windows platforms, perform the following steps:

1. Click **Start** > **Programs** > **IBM Tivoli Monitoring** > **Manage Tivoli Monitoring Services**.
2. Right-click Tivoli Enterprise Monitoring Server.
3. Select **Start**.

On UNIX platforms, run the following command:

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

Stop the server

On Windows platforms, perform the following steps:

1. Click **Start** > **Programs** > **IBM Tivoli Monitoring** > **Manage Tivoli Monitoring Services**.
2. Right-click Tivoli Enterprise Monitoring Server.
3. Select **Stop**.

On UNIX platforms, run the following command:

```
./itmcmd server stop tems_name
```

tems_name is the name of the monitoring server

Starting and stopping the Tivoli Enterprise Portal server

Follow these directions to start or stop the Tivoli Enterprise Portal server:

Start the portal server

On Windows platforms, perform the following steps:

1. Click **Start** > **Programs** > **IBM Tivoli Monitoring** > **Manage Tivoli Monitoring Services**.
2. Right-click Tivoli Enterprise Portal Server.
3. Select **Start**.

On UNIX platforms, run the following command:

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

Stop the portal server

On Windows platforms, perform the following steps:

1. Click **Start** > **Programs** > **IBM Tivoli Monitoring** > **Manage Tivoli Monitoring Services**.
2. Right-click Tivoli Enterprise Portal Server.
3. Select **Stop**.

On UNIX platforms, run the following command:

```
./itmcmd agent stop cq
```

Starting and stopping the Tivoli Enterprise Portal desktop client

Follow these directions to start or stop the Tivoli Enterprise Portal desktop client

Start the desktop client

On Windows platforms, perform the following steps:

1. Click **Start** > **Programs** > **IBM Tivoli Monitoring** > **Tivoli Enterprise Portal desktop**.
2. Enter your user ID and password on the logon window. The default user ID is `sysadmin`.
3. Click **OK**.

On UNIX platforms, run the following command:`./itmcmd agent start cj`

Stop the desktop client

On Windows platforms, perform the following steps:

1. Click **Start** > **Programs** > **IBM Tivoli Monitoring** > **Manage Tivoli Monitoring Services**.
2. Right-click Tivoli Enterprise Portal desktop.
3. Select **Stop**.

On UNIX platforms, run the following command:`./itmcmd agent start cj`

Starting and stopping monitoring agents

Start and stop monitoring agents using the Manage Tivoli Enterprise Monitoring Services or the from the user interface in both Windows and UNIX environments. You can also use the command line in UNIX.

You can also run the `ITMAgents1` script from the `/etc/init.d` directory. The location varies for different environments. Only run the `ITMAgents1` script if the system restarts other Response Time agents.

Alternatively, you can restart the Transaction Tracking agents from the Tivoli Enterprise Portal if required by using the Proxy Agent Services. See the IBM Tivoli Monitoring Information Center for further information.

If an OS agent is installed on the same computer as an agent and shares the same `CANDLE_HOME` directory, you can remotely stop and start the agent from the Tivoli Enterprise Portal. Right click on the agent in the Tivoli Enterprise Portal and select **Stop** or **Restart**.

Note: Your user ID must have the proper permission to start and stop agents. See the IBM Tivoli Monitoring documentation for more information about permissions.

Note: If you install Response Time on SUSE SLES 10 platform, the agent might not restart automatically when the environment reboots. You can start the agent manually with instructions in this section.

Follow these directions to start or stop the monitoring agents:

Start a monitoring agent

On Windows platforms, perform the following steps:

1. Access the Navigator.
2. Right-click the monitoring agent that you want to start
3. Select the green Start icon.

On UNIX platforms, run the following command:

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

Stop a monitoring agent

On Windows platforms, perform the following steps:

1. Access the Navigator.
2. Right-click the monitoring agent that you want to stop.
3. Select the red Stop icon .

On UNIX platforms, run the following command:

```
./itmcmd agent stop pc
```

Where *pc* is the product code for the monitoring agent that you want to start or stop. See Product codes for a list of codes.

For example to start Tivoli Enterprise Portal desktop client, run the following command: `./itmcmd agent start t5`

Note: On UNIX systems, the Web Response Time monitoring agent occasionally gives the following error: `[root@rh5ma bin]# ./CandleAgent -h /opt/IBM/ITM -c stop t5 Stopping ITCAM for Web Response Time ... Product t5 was not stopped`. If this happens, use `-f` to force Web Response Time to stop. If you are uninstalling remotely for Web Response Time, you should also use this option to stop the monitoring agent *before* doing the remote uninstall.

Chapter 9. Monitoring Internet services

When monitoring Internet services, you define what is to be monitored, for whom, and when. You configure Internet service monitoring through the Internet Service Monitoring Configuration user interface, within the Tivoli Enterprise Portal, or through the Internet Service Monitoring command-line interface.

Internet service monitors test specific Internet services and forward the results of the tests to the Databridge. The monitors emulate the actions of a real user of the service.

For example, the HTTP monitor periodically attempts to access a web page by emulating requests that a web browser would usually send when a user visits the page. The monitor records the result of the test, which is sent to the Databridge.

You can use either the Internet Service Monitoring Configuration command-line interface or the **ismbatch** command on the command-line. The Internet Service Monitoring Configuration command-line interface mirrors the operations that you can complete with the Internet Service Monitoring Configuration user interface. Both of these interfaces update the Tivoli Enterprise Portal Server database.

Tip: In ITCAM for Transactions V7.4 iFix 3 and later, multiple users can configure Internet Service Monitoring simultaneously. Both the Internet Service Monitoring Configuration user interface and the Internet Service Monitoring Configuration command-line interface can be run at the same time. See “Editing profiles with multiple administrators” on page 76 for more information.

The **ismbatch** command offers similar functionality to Internet Service Monitoring Configuration command-line interface. However, **ismbatch** commands are run only locally and do not update the Tivoli Enterprise Portal Server database.

Internet service monitoring

Each monitor is designed to test one type of protocol or service. For example, the HTTP monitor tests the availability of resources such as web pages over the Hypertext Transfer Protocol, and the FTP monitor tests the transfer of files between hosts running the File Transfer Protocol.

A monitor can test many different instances of the same service, such as a series of web pages served by a range of hosts.

Web service monitoring

Using the Internet Service Monitoring range of monitors, you can tailor the type of web service monitoring you provide— from basic Internet service monitoring testing the availability of a web page, to combining sequences of tests.

Internet service monitoring uses high volume, low complexity polling to test the availability of web services. For example, if you want to monitor the general availability of a website, you might use the HTTP monitor to poll a large number of URLs at regular intervals.

Using a combination of monitors, you can build a level of service monitoring appropriate to your requirements:

- HTTP and HTTPS monitors

  Monitor the availability of resources over HTTP or HTTPS by running basic, single-request tests at high volume.

- Transaction monitor (TRANSX)

  Combine sequences of tests performed by a group of monitors, simulating the actions of a real user. For example, dialing up a service, accessing a number of pages on several websites and then accessing e-mail services.

Monitors and probes

Monitors are distinguished from ObjectServer IBM Tivoli Netcool/OMNIbus probes by their polling functions.

Probes connect to an event source to acquire the event data that it generates, while monitors actively poll or test services at regular intervals by injecting transactions or queries into the target service and generating performance evaluation data.

Available Internet Service Monitoring monitors

The Internet Service Monitoring suite of monitors provides coverage for a broad range of Internet services.

Table 13 on page 72 lists the monitors available with Internet Service Monitoring and the types of service that they monitor.

Table 13. Available Internet service monitors

Monitor name	**Type of service monitored**
DHCP	Dynamic Host Configuration Protocol
Dial - deprecated in ITCAM for Transactions V7.3	Dial-up Service
DNS	Domain Name Service
FTP	File Transport Protocol
HTTP	HyperText Transport Protocol
HTTPS	HyperText Transport Protocol (Secure)
ICMP	Internet Control Message Protocol
IMAP4	Internet Message Access Protocol
LDAP	Lightweight Directory Access Protocol
NNTP	Network News Transport Protocol
NTP	Network Time Protocol
POP3	Post Office Protocol
RADIUS	Remote Authentication Dial-In User Service
RPING	Remote Ping (Cisco, Juniper, and RFC2925)
RTSP	Real-Time Streaming Protocol
SAA	Cisco Service Assurance Agent
SIP	Session Initiation Protocol
SMTP	Simple Mail Transport Protocol
SNMP	Simple Network Management Protocol
SOAP	XML-based messaging protocol
TCPPort	Transmission Control Protocol
TFTP	Trivial File Transfer Protocol
TRANSX	Transactions

Table 13. Available Internet service monitors (continued)	
Monitor name	**Type of service monitored**
WMS - deprecated in ITCAM for Transactions V7.3	Windows Multimedia Streaming

Monitor files

Each Internet service monitor consists of an executable file, properties file, rules file, and a log file.

Executable file
Executable files implement the monitor functionality.

Monitor executable files are located in the `$ISMHOME/platform/`*`arch`*`/bin` directory.

The value for *arch* is the architecture code for the operating system:

- Windows - `win 32`
- Linux - `linux2x86`
- Solaris - `solaris2`
- AIX - `aix5`

Properties file
Properties files define the operating parameters of the monitors. There are generic parameters that apply to all monitors and monitor specific parameters. Each monitor has a property file.

The properties file is a text file and includes default settings that are preceded by the hash symbol.

To change a setting, either change the default setting and remove the hash symbol or copy and paste the line containing the setting to below the default settings, then make the change and remove the hash symbol. This enables you to restore the defaults later.

Note: You can also specify properties using the command-line.

Monitor properties files are located in the `$ISMHOME/etc/props` directory.

Rules file
Rules files define the mapping from monitor data elements to ObjectServer alert fields. The ObjectServer module running on the Databridge uses each monitor's rules file to convert events into IBM Tivoli Netcool/OMNIbus alerts, which it sends to an ObjectServer.

Rules files are similar to ObjectServer IBM Tivoli Netcool/OMNIbus probe rules files. For information about their syntax, see the *ObjectServer IBM Tivoli Netcool/OMNIbus Probe and Gateway Guide*.

Monitor rules files are located in the `$ISMHOME/etc/rules` directory.

Log file
Log files store messages about the monitor's operation.

Monitor log files are located in the `$ISMHOME/log` directory. The `MessageLog` property in the monitor properties file specifies the file to which the monitor writes the messages.

The `MessageLevel` property selects the level of information written to the log file, for example, detailed debugging messages or fatal error messages. The `MaxLogFileSize` property determines the size of the log file before rolling over.

The default name of the log file is *name*`.log` where *name* is the name of the monitor.

Internet Service Monitoring concepts

To monitor Internet services, you create *user profiles*, *profile elements*, and *monitoring schedules*.

A user profile is a customer, department, or a group of services for which you monitor Internet or web services. For each user profile you define one or more profile elements. For example, you might define a profile element to monitor a web page delivered over an HTTP service, or a profile element to monitor the availability of an FTP service. User profiles typically contain multiple profile elements, each testing one of the services you provide to that user.

Each user profile also has an associated monitoring schedule that determines on which day and at what time the tests defined in the profile are to run.

Internet Service Monitoring configuration interface

Configure user profiles, profile elements, and monitoring schedules using the Internet Service Monitoring user interface or the command-line interface.

Tip: In ITCAM for Transactions V7.4 iFix 3 and later, multiple users can configure Internet Service Monitoring simultaneously. Both the Internet Service Monitoring Configuration user interface and the Internet Service Monitoring Configuration command-line interface can be run at the same time. See "Editing profiles with multiple administrators" on page 76 for more information.

To access the Internet Service Monitoring Configuration window, click the ISM Configuration icon in the toolbar of Tivoli Enterprise Portal. The interface consists of two panes. Use the left pane to create and remove user profiles. Use the right pane to create the profile elements, the monitoring schedules, and to distribute user profiles to other systems.

When you select a monitor type and click **Add**, the right pane changes to display the available profile element parameters for the selected monitor. The parameters shown in the top section are mandatory. The mandatory parameters define the resources to be monitored and identify the element. The parameters in the bottom section are optional.

Note: You must supply at least one mandatory parameter before you can access the optional parameters.

The **OK**, **Cancel**, and **Apply** buttons perform the following functions:

Table 14. User interface buttons

Button	Description
OK	Saves the configuration details to the Tivoli Enterprise Portal Server database, distributes the updates to the Internet Service Monitoring agent if required, and exits the user interface.
Cancel	Cancels all configuration details that you defined since the last Save operation and exits the user interface.
Apply	Saves the configuration details to the Tivoli Enterprise Portal Server database and distributes the updates to the Internet Service Monitoring agent if required. The user interface remains open.
Resync Agent	Clears out the profiles and resends all the deployed profiles to the Internet Service Monitoring agent. When working with profiles, use **Resync Agent** only when there are problems and the Internet Service Monitoring agent is not synchronized. **Note:** If there are a large number of profile elements, resynchronizing these elements may take more than 10 minutes. In normal operation, use the **Apply** button to save profile updates to the Tivoli Enterprise Portal Server and distribute to the Internet Service Monitoring agent.
Help	Displays the online documentation.

Important notes on profile management

You can use either the Internet Service Monitoring Configuration user interface or the Internet Service Monitoring Configuration command-line interface interchangeably to manage user profiles.

However, using both these tools and the **ismbatch** command line utility to manage user profiles is not supported, and may lead to inconsistencies in user profile configuration, or loss of user profiles. User profiles created using **ismbatch** are not visible in the Internet Service Monitoring Configuration window or the Internet Service Monitoring Configuration command-line interface. Deploying a user profile to a managed system on which **ismbatch** was used to create user profiles, or using the **Resync Agent** facility removes any existing profiles from that system.

Managed systems do not send user profiles back to IBM Tivoli Monitoring; they only report status information indicating the success or failure of profile deployment operations. That is, the Internet Service Monitoring Configuration user interface and Internet Service Monitoring Configuration command-line interface do not register changes made using **ismbatch**. Internet Service Monitoring Configuration is the central repository of user profiles; a managed system receives a snapshot of a user profile when it is deployed.

Use either of the Internet Service Monitoring Configuration interfaces or **ismbatch** to manage user profiles, but not both. Do not attempt to use the Internet Service Monitoring Configuration interface or Internet Service Monitoring Configuration command-line interface to modify or deploy profiles to managed systems on which **ismbatch** has been used to manage profiles.

Whether using either the Internet Service Monitoring command line interface or the Internet Service Monitoring Configuration user interface, note that national language strings are not supported. You cannot specify profile names or descriptions, for example, in a language other than English.

Accessing the Internet Service Monitoring Configuration interface

If you are not a system administrator, you do not have access to the Internet Service Monitoring Configuration interface, unless permission has been granted to you.

The system administrator can grant permissions to users other than **sysadmin** so that they can view and modify profiles and monitors. To grant access to another user, complete the following steps:

1. Log into the Tivoli Enterprise Portal.
2. Select **Edit** > **Administer Users**.
3. In the Administer Users dialog box, on the **Users** tab, select the user you want to grant permissions to. For example, *itmuser*.
4. On the **Permissions** tab:
   a. In the **Authorities** list, select **Situation**.
   b. In the **Permissions** list, select **Modify**. The other options are selected automatically.
   c. Click **Apply**.
5. On the **Navigator Views** tab, assign at least one view, usually **Physical**, to the user, and click **Apply**.
6. On the **Applications** tab, move at least **Internet Service Monitors** to the **Allowed Applications** list and click **Apply**.

   To make all applications available to this user, move **All Applications** to the **Allowed Applications** list.
7. Click **OK**.

To test that the permissions have been granted, log out of the Tivoli Enterprise Portal, and log back in with the user account that you have just configured. The Internet Service Monitoring Configuration interface should be visible and the user should be able to view and modify ISM profiles and monitors.

Editing profiles with multiple administrators

ITCAM for Transactions V7.4 iFix 3 and later includes multiple administrator support, for editing profiles from multiple Internet Service Monitoring Configuration windows and Internet Service Monitoring Configuration command-line interfaces simultaneously.

Each Internet Service Monitoring Configuration opened conceptually takes a snapshot of the Tivoli Enterprise Portal Server database. Locks applied to profiles by other users after you opened your Internet Service Monitoring Configuration instance will not be visible until you refresh the Internet Service Monitoring Configuration.

Locks are applied when you open a profile to edit it. Locks are removed when you apply the changes, or close the Internet Service Monitoring Configuration by clicking **OK** or **Cancel**.

In the , locks are represented in the following way:

- **Edit** icon shows that the profile is locked by you and is available to edit.
- **Lock** icon shows that the profile is locked and is being edited by another user.

The status bar provides information about the lock status of the profiles.

- `Lock granted` - displayed when you successfully lock a profile for editing.
- `Locked by` *`user`* `on` *`hostname`* `at` *`date`* - displayed when a profile is locked by another user.
- `Configuration out of date reloading:` *`profile`* - displayed when there is a conflict because a user attempted to edit a profile without first refreshing the Internet Service Monitoring Configuration to load the latest updates. If this occurs, local changes are discarded. However, changes lost are minimal.

Best practices

- Ensure that all users have unique accounts with system administrator privileges. If the users are not unique, the locks are indistinguishable.
- Refresh Internet Service Monitoring Configuration to see the latest updates from other users before attempting to edit a new profile if the window has been open for some time.
- If you want to edit multiple profiles using the Internet Service Monitoring Configuration command-line interface, ensure that none of the profiles that you want to edit are already locked by another user. If a lock cannot be acquired for all profiles concerned, the operation will fail.

Internet Service Monitoring user profiles

You can create, modify, copy, and delete user profiles as well as distribute profiles to other locations.

User profiles represent departments within an organization, clients for whom you are performing monitoring services, or a group of web and internet services.

Creating user profiles

User profiles are identified by a name. The name may be a department within an organization, the name of the client for whom services are being monitored, or a group of services. For example, web services or internet services.

About this task

The maximum size of the user name is 64 alphanumeric characters. You can use the underscore (_) and hyphen (-) symbols but any other symbols, including spaces, are not allowed.

Procedure

To create a user profile:

1. In the Internet Service Monitoring Configuration window, click **Create Profile**.

2. Type a name for the profile.
3. Click **OK**.

Copying user profiles

You can copy user profiles, which is useful if you need a similar profile for another user. You can then modify the copied profile to suit user specific requirements.

Procedure

To copy a user profile:

1. In the Internet Service Monitoring Configuration window, select the user profile that you want to copy.
2. Click the Copy Profile icon.
3. Type a new name for the profile (spaces and symbols other than _ (underscore) are not allowed).
4. Click **OK**.
5. Assuming the profile contains elements, select the element to be modified and change its parameters as required.
6. Repeat step 5 for each element that needs to be changed.
7. Click **Apply** to save.

Profile distribution

You can distribute user profiles to other systems so that you can monitor the service from different locations.

You can distribute user profiles to any managed system that has an Internet service monitor installed and running. There are two methods of distributing user profiles: by profile and by system. Distributing by profile allows you to distribute one profile at a time to multiple systems. Distributing by system allows you distribute multiple profiles to a single system.

By profile

Distributing user profiles by profile enables you to distribute one profile at a time to multiple managed systems.

About this task

If a managed system is not running, an error message is displayed and no distribution is possible until you start the managed system.

Procedure

To distribute a user profile by profile:

1. In the Internet Service Monitoring Configuration window, select the profile.
2. Ensure that the **Distribution** tab at the top of the right pane is selected.
3. From the **Available Systems** list, select the systems to which you want to distribute the profile (use the Shift and Ctrl keys to select multiple systems).
4. Click the right arrow to move the selected systems to the **Deployed Systems** list.
5. Click **Apply** to save.

Results

Note: To stop all profile elements in a profile from running on a particular system, select the system from the **Deployed Systems** list and click the left arrow.

By system
Distributing user profiles by system enables you to distribute multiple profiles at the same time to a single system. You can also immediately see whether a system is running or is not synchronized.

About this task
A system that is not synchronized indicates that there are inconsistencies between the profiles on the system and the profiles in the Tivoli Enterprise Portal Server database. This may occur when, for example, a profile is configured and distributed to several systems but the distribution to one system fails due to a network problem. Use the **Resync Agent** button to reset the profiles on the managed system to those in the Tivoli Enterprise Portal Server database.

Note: If there are a large number of profile elements, resynchronizing these elements may take more than 10 minutes. In normal operation, use the **Apply** button to save profile updates to the Tivoli Enterprise Portal Server and distribute to the Internet Service Monitoring agent.

Procedure

To distribute user profiles by system:

1. In the Internet Service Monitoring Configuration window, select **Profiles**.
2. Ensure that the **Distribution** tab at the top of the right pane is selected.
3. Select the system to which you want to distribute the profiles.
   a) If availability is **No**, check that the managed system is running.
   b) If a status of `Out of Sync` is displayed, click **Resync Agent** to synchronize the agents.

      Note: If there are a large number of profile elements, resynchronizing these elements may take more than 10 minutes.
4. In the **Available Profiles** section, select the profiles to be distributed (use the Shift and Ctrl keys to select multiple profiles).
5. Click the right arrow to move the selected profiles to the **Deployed Profiles** list.
6. Repeat steps 3-5 for any additional systems to which you want to distribute profiles.
7. Click **Apply** to save the changes to the Tivoli Enterprise Portal Server and distribute to the Internet Service Monitoring agents.

Results

Note: To stop all profile elements in a profile from running, select the profile from the **Deployed Profiles** list and click the left arrow.

Deleting user profiles

You can delete user profiles that are no longer required. When you delete a user profile, all profile elements belonging to that profile and its associated monitoring schedule are also deleted.

About this task
If you want to temporarily stop a profile's elements from running on a particular system, consider removing the system from the distribution list.

Procedure

To delete a user profile:

1. In the Internet Service Monitoring Configuration window, select the profile to be deleted.
2. Click the Delete Profile icon.
3. Click **Yes** to confirm the deletion.
4. Click **Apply** to save.

Internet Service Monitoring profile elements

Profile elements define the tests performed on an Internet service. Every profile element is associated with a particular monitor, such as HTTP, and contains a set of parameters that define how the service is tested.

Profile elements contain mandatory parameters and optional parameters. Mandatory parameters are the parameters that define what is to be monitored and a description. For example, for the HTTP monitor these parameters are `server` and page where `server` defines the name of the web server and page defines the URL of the web page that you want to monitor. The description parameter identifies the element. The default description is *`monitor server element`*. For example, HTTP `www.ibm.com element`. If you have more than one profile element for the same monitor and that uses the same server, you can use the `element` part of the description to further identify the element.

Optional parameters define how you want to monitor the service. For example, how often to retest a service before a failed service is recorded, how to monitor service levels, and how to search for information in test results. You can use up to 50 regular expressions to assist with searching. For example, the expression `r.t` matches strings `rat`, `r t` but not `root`.

Mandatory element parameters

Mandatory element parameters consist of generic parameters that apply to all monitors and parameters that are monitor specific.

Generic parameters are the **Description** and **Active** parameters. Use the **Description** parameter to identify the element. Use the **Active** parameter check box to indicate that an element is available for performing tests immediately after you have defined the element.

The monitor specific parameters consist of parameters that define what is to be monitored. Table 15 on page 79 lists both the generic and monitor specific parameters. For detailed information about monitor-specific parameters, see the information for each monitor in Internet Service Monitoring monitors in detail.

Table 15. Mandatory element parameters

Monitor type	Required parameters
DHCP	server, description, active
DNS	server, host, description, active
FTP	server, description, active
HTTP	server, page, description, active
HTTPS	server, page, description, active
ICMP	server, description, active
IMAP4	server, description, active
LDAP	server, search database, filter, description, active
NNTP	server, newsgroup, description, active
NTP	server, description, active
POP3	server, description, active
RADIUS	server, shared secret, username, password, description, active
RPING	server, router type, host, community string, description, active
RTSP	server, remote file, description, active
SAA	server, community string, probe type, description, active

Table 15. Mandatory element parameters (continued)	
Monitor type	**Required parameters**
SIP	server, description, active
SMTP	server, description, active
SNMP	server, object group name, description, active, OID group
SOAP	Wsdl, operation, operation names, location, description, active
TCP Port	server, port, description, active
TFTP	server, local file, remote file, description, active
TRANSX	name, description, active

Optional element parameters

Optional element parameters are grouped under tabs. Some optional parameters are available to all monitors whereas others are monitor specific.

The optional parameters that can be applied to all monitors are located on the **Advanced** and **SLC** tabs.

- Use the **Advanced** tab to define general parameters such as poll interval and number of required retries.
- Use the **SLC** tab to specify service level classifications (in previous releases, service level classifications were referred to as *DVCs* (Discrete Value Classifications).

The tabs for optional parameters that are monitor specific are only visible when defining elements for a particular monitor. These tabs can be **RegExp**, **Parameters**, **Body**, **Proxy Details**, **SAA Probe**, **Soap Parameters**, and **Steps**.

- Use the **RegExp** tab to specify regular expressions for use when searching for information in test results.
- Use the **Parameters** tab if you want the monitor to send extra data in the header fields and message body of HTTP requests.
- Use the **Body** tab if you want the HTTP and HTTPS monitors to send extra data in the body part of POST requests.
- Use the **Proxy Details** tab if you want to test the availability of web pages through a proxy server.
- Use the **SAA Probe** tab to configure a router's SAA to test the availability of another network device or service using timed echo request/responses defined in the Cisco Response Time Monitor MIB (Management Information Base).
- Use the **Soap Parameters** tab to configure Soap inputs and outputs.
- Use the **Steps** tab to define a series of activities, which the TRANSX monitor performs using several different Internet service monitors. For example, you could configure TRANSX to access pages of a website using the HTTP monitor, download some files, send or retrieve e-mails using the POP3 and SMTP monitors, and then access a Network News Server using the NNTP monitor.

For details on monitor configuration parameters, see the required monitor.

Service level classifications

Service level classifications are optional monitor parameters that can be applied to all monitors. They define the rules used by monitors to evaluate how well a monitored service is performing. The results form the basis for service level agreements (SLAs) evaluation.

Specify service level classifications on the **SLC** tab.

Service level classifications consist of a set of conditions that monitors apply to the collated results data to determine whether the service level is `GOOD`, `MARGINAL`, or `FAILED`.

Service level classifications are entered as a set of `If-then-Else` statements. You can have multiple statements. With multiple statements you can specify a range of performance data for classifying the service level. Monitors process these statements sequentially. The **final** statement defines the service level classifications that are applied if none of the test expressions in the preceding statements are true.

Each statement may also contain multiple logical `AND` conditions. For example, in the `If` statement you can specify that the status is FAILED if the status does not equal 200, 301 or 302

The *metrics* in the statement specify the collated results data to which you want to apply service levels. This data depends on the monitor type. For example, available metrics for the DHCP monitor are `TotalTime`, `LookupTime`, `ResponseTime`, and `Message`. The most common result data is displayed in the **Metric** list. To use less common result data, manually enter the name of the required result data.

Tip: Use the default condition of `GOOD` and specify service level classifications for failing conditions to test if monitored services have failed. Using this approach, if you do not assign a condition to a metric, it defaults to `0` in the workspace, but may actually be empty. Any service level classification using the empty metric gives a result of `true` (failed).

Select the *operators* that you can use in a statement from the **Operator** list. A description of the available operators is provided in Table 16 on page 81.

The *operand* is a string or positive number.

Table 16. Available operators

Symbol	Description
=	Equal to.
!=	Not equal to.
>	Greater than.
<	Less than.
<=	Less than or equal to.
>=	Greater than or equal to.
`between`	Enter a comma separated list. For example, to specify a value between 5 and 12, enter `5,12`.
`outside`	Enter a comma separated list. For example, to specify a value outside 5 to 12, enter `5,12.`
`contains`	Must contain the specified value.
`!contains`	Must not contain the specified value.
`IGNORE`	Do not apply this condition.

Note: If a service level classification contains more `Else-if` statements than you require, set the operator for the unused conditions to `IGNORE`.

Notes on service level classifications
When defining service level classifications, the types of test expressions that you may use depend on the type of information contained in a monitor element.

- Expressions that test `Message` and `Regexp` (regular expression) monitor elements require a string rather than a number.
  - The `Regexp` string may be any text string, for example, `FAILED`.
  - The `Message` string must be one of the messages of the `$message` element. Use this type of test to determine whether a service has failed. For example:

```
If Message != OK then status FAILED
```

Note: Not all monitors use 0K to indicate success. For information about alternate positive response messages provided by a monitor, see the detailed information about each monitor in the appendixes of this guide.

- Where applicable, a test expression may contain a `Status` element instead of, or as well as, a `Message` element to classify the service level. For example, for the FTP monitor the test for successful file transfer is:

```
If Status != 226 then status FAILED
```

  Status codes are determined by the protocol associated with the monitor. See the relevant protocol specification, usually an RFC, for further information about status codes.
- Some monitors provide elements named `checksum` and `previousChecksum`. Although these monitor elements are available when defining service level classifications, evaluating their values in a test expression does not normally provide meaningful results because checksum values are not known when the profile element is created (monitors calculate `checksum` values while tests are in progress).

  The `checksum` and `previousChecksum` monitor elements can be used for alert enrichment using monitor rules files. Monitor rules files are located in `$ISMHOME/etc/rules`.

Service level agreements
Returned service levels are measured against service level agreements (SLAs).

In Internet Service Monitoring, SLAs are specified through situations in the Internet service monitor workspaces. If you are using ObjectServer IBM Tivoli Netcool/OMNIbus, the SLAs are specified in rules files.

Retest period
The service retest parameters are generic optional monitor parameters. The parameters define the period after which a failed service level is generated. Failed service levels affect your service agreement with the client.

Internet services are sometimes momentarily interrupted due to transient failures. If a service fails but then recovers during the retest period the monitor does not record a service level failure. This allows you to ignore transient errors.

For example, you might have an HTTP monitor that is configured to perform a test on a web page every ten minutes. In addition, you can configure the monitor so that if the web page fails, the monitor tests the web page five more times with five second intervals between the tests. If the web page fails all retests, the monitor records a failure for the service.

Monitors indicate the number of interim failures during the retest period in the `$consecutiveFailures` field of the test results data.

Situations
Internet Service Monitoring provides predefined situations for service level agreements.

- **KIS_Host_SLA_Failed**

  The **KIS_Host_SLA_Failed** situation indicates that a monitored host has failed its service level agreement. By default, this situation is triggered when the percentage of service level classifications returning the result Good falls below 95% of all tests performed on that host.
- **KIS_Host_SLA_Marginal**

  The **KIS_Host_SLA_Marginal** situation indicates that a monitored host is close to failing its service level agreement. By default, this situation is triggered when the percentage of service level classifications returning the result Good is below 100% but greater than or equal to 95% of all tests performed on that host.
- **KIS_*monitor*_Inactive**

  When a monitor is not running or has not submitted any results recently, a situation is triggered to indicate the inactive status of the monitor. If the monitor has stopped, this situation will automatically

attempt to restart the monitor using Take Action commands. If the monitor is idle, no action is taken. To stop the monitor for maintenance or similar purposes, stop the agent or the associated situation so that the monitor will not continue to attempt to restart. If you do not wish to be notified of the inactivity of the monitor, stop the situation. This process is applicable to the following situations:

  - **KIS_Bridge_Inactive**
  - **KIS_DHCP_Inactive**
  - **KIS_DNS_Inactive**
  - **KIS_FTP_Inactive**
  - **KIS_HTTP_Inactive**
  - **KIS_HTTPS_Inactive**
  - **KIS_ICMP_Inactive**
  - **KIS_IMAP4_Inactive**
  - **KIS_LDAP_Inactive**
  - **KIS_NNTP_Inactive**
  - **KIS_NTP_Inactive**
  - **KIS_POP3_Inactive**
  - **KIS_RADIUS_Inactive**
  - **KIS_RPING_Inactive**
  - **KIS_RTSP_Inactive**
  - **KIS_SAA_Inactive**
  - **KIS_SIP_Inactive**
  - **KIS_SMTP_Inactive**
  - **KIS_SNMP_Inactive**
  - **KIS_SOAP_Inactive**
  - **KIS_TCPPORT_Inactive**
  - **KIS_TFTP_Inactive**
  - **KIS_TRANSX_Inactive**
- **KIS_Element_SLA_Failed**

  The **KIS_Element_SLA_Failed** situation indicates that the service monitored by a profile element has failed its service level agreement. By default, this situation is triggered when the percentage of service level classifications returning the result Good falls below 95% of all tests performed by the profile element.
- **KIS_Element_SLA_Marginal**

  The **KIS_Element_SLA_Marginal** situation indicates that the service monitored by a profile element is close to failing its service level agreement. By default, this situation is triggered when the percentage of service level classifications returning the result Good is below 100% but greater than or equal to 95% of all tests performed by the profile element.

Tip: Before modifying a predefined situation, always make a copy of it using **Create Another**.

Scenario

You are monitoring Java Virtual Machine using the TCPPORT monitor and would like Internet Service Monitoring to report the Java Virtual Machine host name instead of the agent host name if the monitored Java Virtual Machine stops responding.

Update the situation to report the Java Virtual Machine host name:

1. In the Tivoli Enterprise Portal, in the Navigator right-click **Internet Service Monitoring** and select **Situations**.

2. In the **Situation Editor**, select the following values:
   - In the **Attribute Group** list, **KIS TCPPort**
   - In the **Attribute Item** list, **ServiceLevel**
3. In the **Formula** field, set the situation trigger for **ServiceLevel** to `!=1`.
4. Click **Advanced**.
5. In the **Advanced Situation Options** dialog box, on the **Display Item** tab, select `Host` in the **Item** list and click **OK**.
6. Click **Apply** to save the situation.
7. Distribute the situation to one or more managed systems and click **Apply**.
8. In the left column, right-click the new situation and select **Start** to start the situation.

Regular expressions
Regular expressions are optional monitor specific parameter elements. You can perform a regular expression search on the test results by entering up to 50 regular expressions to match. The monitor attempts to match the contents retrieved to each of the regular expressions.

If a match for a specified regular expression is found, the matched lines (or as much as can fit in the monitor's internal buffer) are returned in the corresponding `$regexpMatch`*n* test result element. If the regular expression matches more than once in the test results, only the first match is returned. The status of each regular expression test is indicated by the `$regexpStatus`*n* test result element. The `$regexpStatus`*n* element may have the following values:

- `NONE` (no regular expression checking is configured)
- `MATCHED` (a match was found for the regular expression)
- `FAILED` (a match was not found for the regular expression)

Regular expressions are entered as `[operator] expression [operator]`. For example, to search for web pages that return a login and password instead of pages that return messages such as `'page not found'` or `'cannot access the server'` you enter the expressions:

```
1 .*login.*
2 .*password.*
```

The operators `.*` indicate that the expression matches any number of any characters before and after the expression. For a list and description of regular expression operators supported by Internet Service Monitoring, see Appendix F, “Regular expression syntax in Internet Service Monitoring,” on page 123.

Note: You can use the regular expression matches and their status information as criteria for service level classifications.

Body
Body text is an optional parameter element for the HTTP and HTTPS monitors. Specify the body part of a POST request.

For example, you could specify the following body text for the POST request:

```
<?xml version='1.0' encoding='utf-8' ?>
<SOAP-ENV:Envelope xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns:xsi="http://www.w3.org/2001/
XMLSchema-instance">
<SOAP-ENV:Body>
<ns1:echoString xmlns:ns1="http://soapinterop.org/">
<ns2:input xsi:type="xsd:string" xmlns:ns2="http://soapinterop.org/xsd">
</ns2:input>
</ns1:echoString>
</SOAP-ENV:Body>
</SOAP-ENV:Envelope>
```

To add body text to the POST request:

1. In the Internet Service Monitoring Configuration, select an HTTP or HTTPS profile.

2. On the **Advanced** tab, change the command to **POST**.
3. On the **Body** tab, which is now enabled, enter the body text for the POST request.

The Content-Type parameter is automatically added to the **Parameters** tab. The parameter defaults to `application/x-www-form-urlencoded`. Modify the parameter to the type of request inserted into the body tab. In the above example, change the Content-Type to `text/xml`.

Alternatively, you can configure the body for the POST request using the Internet Service Monitoring Configuration command-line interface or ismbatch and the `@Body` group. For example:

```
ismconfig -config -add monitor=http profile=httpbodytest command=POST page="/"
server="10.1.1.1" @Body "body text"
```

Creating profile elements

Profile elements define Internet service tests. When creating a profile element, you select the type of monitor that matches the service you wish to test, then define parameters to determine how that service is tested.

About this task

Note: Make sure that the OID group exists before you define elements for the SNMP monitor.

Procedure

To create a profile element:

1. In the left pane of the Internet Service Monitoring Configuration window, select the user profile for which you want to add profile elements.
2. Make sure that the **Distribution** tab in the right pane is selected.
3. Select the required monitor from the **Monitor type** list.
4. Click **Add**.
5. In the mandatory parameter section, click in the blank row and enter the compulsory parameters (press Tab to move to each field or click in the required field).
6. Select the **Active** check box to enable the element to start collecting performance data upon completion of the element definition.
7. Specify optional element parameters as required.

   Note: To add multiple `Else if` statements on the **SLC** tab, click **Add Group**. To specify metrics in statements, select from the **Metric** list or manually enter them. The **Metric** list contains the most common metrics for the monitor.
8. Click **Apply** to save.

Deactivating profile elements

You can temporarily stop a profile element from polling by deactivating it. Deactivating a profile element rather than deleting it enables you to make the element available again at a later stage.

Procedure

To temporarily deactivate a profile element:

1. In the left pane of the Internet Service Monitoring Configuration window, select the user profile containing the element to be stopped.
2. In the right pane, select the element by clicking in any of the element's mandatory parameters fields.
3. Clear the **Active** check box next to the selected element.
4. Click **Apply** to save.

Deleting profile elements

You can delete profile elements that are no longer required.

About this task

If you want to temporarily stop a profile element from running for a particular profile, consider clearing the **Active** check box instead of deleting the element.

Note: Deleting a profile element does not remove the monitoring schedule because the schedule is associated with the profile, not with the element.

Procedure

To delete a profile element:

1. In the left pane of the Internet Service Monitoring Configuration window, select the user profile containing the element to be stopped.
2. In the right pane, select the element by clicking in any of the element's mandatory parameters fields.
3. Click **Delete**.
4. Click **Yes** to confirm the deletion.
5. Click **Apply** to save.

Results

Note: The profile element remains visible until you refresh the ISM Configuration window. To refresh, click **OK** to exit the window and then re-open the window.

Deleting service level classifications

You can delete service level conditions specified in a `If` or `Else-if` statement or delete a complete statement.

About this task

When you have multiple statements, deleting a statement will move the statements following the deleted statement up a level.

Procedure

To delete a service level condition and statement:

1. In the left pane of the Internet Service Monitoring Configuration window, select the user profile containing the required element.
2. In the right pane, select the element by clicking in any of the element's mandatory parameters fields.
3. Select the **SLC** tab.
4. To delete a condition, select the condition and click **Delete Condition**. Confirm the deletion.
5. To delete an entire statement, click anywhere in the statement and click **Delete Group**. Confirm the deletion.
6. Click **Apply** to save.

Monitoring schedule

The monitoring schedule determines the days and times on which the service tests for a particular user profile are to run. If you do not specify a schedule, the monitoring tasks are run for all periods.

You can configure the profiles to only monitor at specific times. For example, you may have regularly scheduled downtimes for various services during which time it is not necessary to monitor them.

Profiles can be scheduled at 15 minute intervals in a 24 hour period, 7 days a week. Active monitoring periods are indicated in blue.

Creating monitoring schedules

Monitoring schedules define that dates and times at which service tests defined in user profiles are run. All profile elements within a user profile follow the defined schedule. If you do not specify any periods, the tasks are run for all periods (every 15 minutes, 7 days a week).

Procedure

To create a monitoring schedule:

1. In the left pane of the Internet Service Monitoring Configuration window, select the user profile to which you want to add a monitoring schedule.
2. In the right pane, select the **Scheduling** tab.
3. Left-click in a cell to select a single period; left-click and drag to select multiple periods. To cancel a selection, left-click or drag again.

   Note: Use the **Clear** button to cancel all periods, use the **All** button to select all periods.
4. Click **Apply** to save.

OID groups

Object Identifier (OID) groups are optional monitor specific parameters. They define sets of one or more OIDs of a device's Management Information Base (MIB) objects. The SNMP monitor uses the OID groups to retrieve data from those MIB objects whose OIDs appear in a specified OID group.

OID groups are defined globally outside the user profile environment. You select the group containing the required MIB objects when you create an SNMP profile element. For example, if you wish to use the SNMP monitor to poll general performance data, you might define an OID group containing OIDs from the `srSystem` group of MIB objects, such as `srSystemCPUUsageAverage`, `srSystemFreeMem`, and `srSystemSwapPercentUsed`. You would then select this OID group in each profile element you create for monitoring system performance.

The details of the MIB objects from which the monitor extract data are as follows:

- OID Value

  The numerical identifier of the MIB object instance expressed using either ASN.1 notation, for example `.1.3.6.1.2.1.1.2.0`, or the object's name, for example `sysObjectID.0`

  Note: When using ASN.1 notation, you must include the leading `.` character in the OID.

  Note: You may only use an object's instance name to specify the OID value if the MIB document that defines the name is accessible by the monitor. The default directory for MIB documents is `$ISMHOME/mibs`.
- OID Name

  The name of the MIB object, for example `sysObjectID`. This name is used in service level classifications and in `$oidName`*n* monitor elements.
- OID Unit

  The units of the data contained in the MIB object. For example, seconds, bytes, or bits per second (BPS). Set to BPS to enable bits per second calculation for the OID. Bits per second values are calculated as:

  ```
  current_poll_value - prev_poll_value) / poll_interval * 8
  ```
- Selector

  The index value of the MIB object. Table 17 on page 88 shows an example that results in the selector searching all the `ifDescr` rows for the value `FastEthernet0/1`, giving a row index of 2. Then the row `ifPhysAddress.2` is queried and the value `0:6:53:34:d2:a1` is returned. In this way the index 2 is not directly specified, so if the index for `FastEthernet0/1` changes, the OID groups do not need to be re-configured.

Table 17. Use of the index value	
MIB object	**MIB object value**
OID value	`ifPhysAddress`
OID name	`FastEthernet0/1PhysicalAddress`
OID unit	`string`
Selector	`ifDescr=FastEthernet0/1`

To obtain specific information about the MIB objects provided by an SNMP-enabled device, consult the device's MIB document.

Creating OID groups

OID groups are created globally and can be used by all user profiles that monitor SNMP-enabled devices.

Procedure

To create an OID group:

1. In the left pane of the Internet Service Monitoring Configuration window, click the **Profiles** folder.
2. In the right pane select the **OID Groups** tab.
3. Click on the blank row in the **OID Group Name** section and enter a name for the group.
4. Continue with steps 5-7 if you want to create the MIB objects for the group. Alternatively, you can create the MIB objects when creating an SNMP profile element.
5. Click on the blank row in the MIB section and enter the MIB name, value, unit, and selector.
6. Repeat step 5 for each required MIB object.
7. Click **Apply** to save.

Results

Note: When you change an OID group, the changes do not take effect until the monitor runs the next scheduled test that uses the OID group.

Creating MIB objects

You can create MIB objects when creating the OID group or when creating an SNMP element.

Procedure

To create a MIB object when creating an SNMP element:

1. In the Internet Service Monitoring Configuration window, select the **SNMP** profile element.
2. Enter the **server** name, **OID group** name, **community string**, and **description**.
3. Select the **OIDs** tab in the lower section.
4. Enter the **MIB name**, **value**, **unit**, and **selector**.
5. Click **Apply**.

Deleting MIB objects

MIB objects are contained in OID groups and used by the SNMP monitor to obtain data. You can delete individual MIB objects from an OID group or delete all MIB objects by deleting the entire OID group.

Procedure

To delete an individual MIB object:

1. In the left pane of the Internet Service Monitoring Configuration window, click the **Profiles** folder.
2. In the right pane select the **OID Groups** tab.

3. In the **OID Group Name** section, select the OID group containing the MIB object to be deleted.
4. In the MIB section, select the MIB object to be deleted.
5. Click **Delete**.
6. Click **Yes** to confirm the deletion.
7. Click **Apply** to save.

Deleting OID groups

OID groups contain MIB objects that are used by the SNMP monitor to obtain data. Deleting an OID group also deletes all MIB objects within it.

About this task

Note: When you delete an OID group, any SNMP profile elements currently using that group are no longer able to obtain test data from their target devices.

Procedure

To delete an OID group:

1. In the left pane of the Internet Service Monitoring Configuration window, click the **Profiles** folder.
2. In the right pane select the **OID Groups** tab.
3. In the top section of the right pane, select the group to be deleted.
4. Click **Delete**.
5. Click **Yes** to confirm the deletion.
6. Click **Apply** to save.

Internet Service Monitoring example

This example shows how to use Internet Service Monitoring to test the availability of a web page.

The actions listed here are described in more detail in subsequent sections of this guide.

In addition to IBM Tivoli Monitoring, the following products and components must also be running before you can start this activity:

- Internet Service Monitoring.
- Databridge with the IBM Tivoli Monitoring module.
- HTTP monitor.

The following procedures describe the steps required to test the availability of a web page.

To create the user profile and the monitor profile elements:

1. Open the Internet Service Monitoring user interface from within Tivoli Enterprise Portal.
2. Select **Create Profile**.
3. Enter a name for the profile and click **OK**.
4. Select the **HTTP** from the **Monitor Type** list and click **Add**.

   Note: The HTTP monitor is added to the profile as a profile element.
5. In the **server** field, type the name of the server hosting the web page. For example, `www.mycompany.com`.
6. In the **page** field, type the name of the web page. For example, `/index.htm`.
7. In the **description** field, accept the default.
8. Make sure that the **Active** check box is selected.
9. Click **Apply**.
10. Select the profile that you created in step 3.

11. Ensure that the **Distribution** tab is selected.
12. Select the systems to which you want to distribute the profile from the **Available Systems** list and click the right arrow to move them to the **Deployed Systems** list.
13. Click **Apply** to save.

To view the results of the tests in a workspace:

1. Select the Navigator **Physical** view in Tivoli Enterprise Portal.
2. Select the host to which you deployed the test.
3. Expand the default **Internet Service Monitors** workspace.
4. Select the **Monitor Status** workspace. From this workspace you can link to Monitor and Element history workspaces.

Internet Service Monitoring command-line interface

You can use either the Internet Service Monitoring Configuration command-line interface or **ismbatch** command on the command-line. The commands for both are similar and are described in this section.

The Internet Service Monitoring Configuration command-line interface mirrors the operations that you can complete with the Internet Service Monitoring Configuration user interface. Both of these interfaces update the Tivoli Enterprise Portal Server database.

You can use either the Internet Service Monitoring Configuration user interface or the Internet Service Monitoring Configuration command-line interface interchangeably to manage user profiles.

Tip: In ITCAM for Transactions V7.4 iFix 3 and later, multiple users can configure Internet Service Monitoring simultaneously. Both the Internet Service Monitoring Configuration user interface and the Internet Service Monitoring Configuration command-line interface can be run at the same time. See "Editing profiles with multiple administrators" on page 76 for more information.

The **ismbatch** command offers similar functionality to Internet Service Monitoring Configuration command-line interface. However, **ismbatch** commands are only run locally and do not update the Tivoli Enterprise Portal Server database.

Whether using the Internet Service Monitoring command line interface or the Internet Service Monitoring Configuration user interface, note that national language strings are not supported. You cannot specify profile names or descriptions, for example, in a language other than English.

Internet Service Monitoring Configuration command-line interface

The Internet Service Monitoring Configuration command-line interface mirrors the operations that you can perform with the Internet Service Monitoring Configuration user interface. Use the Internet Service Monitoring Configuration command-line interface to automate operations that you would otherwise use the Internet Service Monitoring Configuration user interface to complete.

Using the Internet Service Monitoring Configuration command-line interface you can create and manage profiles, and those profiles are reflected in the Internet Service Monitoring Configuration user interface. Similarly, profiles updated in the Internet Service Monitoring Configuration user interface are also updated in the Internet Service Monitoring Configuration command-line interface.

Internet Service Monitoring Configuration command-line interface is installed with Tivoli Enterprise Portal desktop or browser support to the locations listed in Table 18 on page 90.

Table 18. Locations to which Internet Service Monitoring Configuration command-line interface (ismconfig) is installed

Operating system	Tivoli Enterprise Portal desktop	Tivoli Enterprise Portal browser
Windows systems	`C:\IBM\ITM\CNP\`	`C:\IBM\ITM\CNB\classes\`
UNIX and Linux systems	`/opt/IBM/ITM/arch/cj/lib/`	`/opt/IBM/ITM/arch/cw/classes/`

To use the Internet Service Monitoring Configuration command-line interface, run it directly from the command-line. Internet Service Monitoring Configuration command-line interface operations consist of the command to be executed, and where appropriate, one or more parameters.

To run the Internet Service Monitoring Configuration command-line interface:

1. Run the command prompt.
2. Change directory to the installation location for your system, as described in Table 18 on page 90.
3. Run the command:
   - On Windows systems, **ismconfig.cmd**
   - On UNIX and Linux systems, **ismconfig.sh**

   For example, `/opt/IBM/ITM/arch/cj/lib/ismconfig.sh`

When you first log into Internet Service Monitoring Configuration command-line interface, you will be prompted for your Tivoli Enterprise Portal user credentials.

Note: You will require administrator access for some commands.

For example, on UNIX or Linux systems, run the following command to log in:

```
/opt/IBM/ITM/arch/cj/lib/ismconfig.sh [-u username] -command [parameter=value ...]
```

Tip: To update your password, delete the password entry from the `ismconfig.props` file. You will be prompted for your new password when you next log in.

Internet Service Monitoring Configuration command-line interface specific commands
In addition to the commands that **ismconfig** shares with **ismbatch** there are a number of Internet Service Monitoring Configuration command-line interface specific commands that you can use to update the database, deploy profiles, and synchronize monitors.

Internet Service Monitoring Configuration command-line interface database commands
Using **ismconfig** you can update and configure the Tivoli Enterprise Portal Server database.

Tivoli Enterprise Portal Server database commands

Table 19 on page 91 lists the commands you use to modify the Tivoli Enterprise Portal Server database.

Table 19. Internet Service Monitoring Configuration command-line interface database commands

Operation	Command
Print the current lock status. If the database is locked, the lock information is displayed. If the database is not locked, no information is displayed.	`-lockStatus`
Used in conjunction with other commands to configure Internet Service Monitoring.	`-config`

Table 20 on page 91 lists the commands required for troubleshooting and maintenance. You require Administrator access to use these commands.

Table 20. Internet Service Monitoring Configuration command-line interface database commands

Operation	Command	Arguments
Create Internet Service Monitoring tables in the Tivoli Enterprise Portal Server database.	`-createDB`	
Drop Internet Service Monitoring tables in the Tivoli Enterprise Portal Server database.	`-dropDB`	

Table 20. Internet Service Monitoring Configuration command-line interface database commands (continued)		
Operation	**Command**	**Arguments**
Unlock the configuration database access lock. Administrator access is required. Use arguments to unlock potentially unwanted locks generated when multiple users configure Internet Service Monitoring simultaneously. **Restriction:** Inappropriate use may result in corruption of the configuration information in the Tivoli Enterprise Portal Server database.	`-releaseLock`	`-profile` *profile_name* , to unlock a particular profile `-oidgroup` *oidgroup_name*, to unlock a particular OID group `-all`, to remove all locks `-user` *user_name*, to remove locks granted to a particular user `-system` *system_name*, to remove locks created on a particular system

Internet Service Monitoring Configuration command-line interface deployment operations

Using deployment operations, you can determine what profiles are deployed to a monitor and deploy or undeploy profiles.

Deployment operations

Table 21 on page 92 shows the deployment commands and the associated parameters. The table uses unnamed parameters. If you want to use named arguments, use the **`./ismconfig -help`** command to determine the argument names.

Table 21. Internet Service Monitoring Configuration command-line interface deployment operations		
Operation	**Command**	**Parameters**
List agents to which a profile is deployed	`-listdeployment`	*profile*
Deploy a profile to a monitor	`-deploy`	*profile agent*
Remove a profile from a monitor	`-undeploy`	*profile agent*

Tip: Ensure that you append `:IS` to agent names.

Samples

Deploy a profile named `ibm` to an agent:

```
./ismconfig -config -deploy ibm ismserver:IS
```

Undeploy the profile named `ibm` from an agent:

```
./ismconfig -config -undeploy ibm ismserver:IS
```

List all agents to which the profile named `ibm` is deployed:

```
./ismconfig -config -listdeployment ibm
```

Internet Service Monitoring Configuration command-line interface synchronization operations

Using synchronization operations, you can determine the configuration status of a monitor and ensure that the monitors are synchronized.

Synchronization operations

Table 22 on page 93 shows the synchronization commands and the associated parameters. The table uses unnamed parameters. If you want to use named arguments, use the **./ismconfig -help** command to determine the argument names.

Table 22. Internet Service Monitoring Configuration command-line interface synchronization operations

Operation	Command	Parameters
List the configuration status information for a monitor. If no agent is specified, the status for all agents is shown.	`-agentstatus`	*agent*
Synchronize a monitor	`-resync`	*agent*
Synchronize all monitors	`-resyncall`	

Tip: Ensure that you append `:IS` to agent names.

Samples

List the status of the an agent:

```
./ismconfig -config -agentstatus agent=ismsserver:IS
```

Resynchronize the profiles for an agent:

```
./ismconfig -config -resync agent=ismsserver:IS
```

Resynchronize the profiles for all agent:

```
./ismconfig -config -resyncall
```

Internet Service Monitoring Configuration properties file

Use the configuration properties file, `ismconfig.props` to configure Tivoli Enterprise Monitoring Server connection information, for example to a different host.

The configuration properties file, `ismconfig.props`, is installed to the same location as the Internet Service Monitoring Configuration command-line interface, as described in Table 18 on page 90.

You can open this file and edit the following properties

- **`TepsHost`**, host name of the Tivoli Enterprise Portal Server.
- **`TepsPort`**, port for connection to the Tivoli Enterprise Portal Server; default `1920`.
- **`UserUpdate`**, updates user credentials in the properties file when enabled; default 1 (on).
- **`TraceParams`**, RAS1 log parameters where `KIS` produces ISM logs, and `KISSQL` produces ISM logs about accessing the database. For example:
  - For general debugging, specify `"Error (UNIT:KIS ALL)"`
  - For detailed debugging, specify `"Error (UNIT:KIS ALL)(UNIT:KISSQL ALL)"`

User credentials are also stored in the configuration properties file. The first time the Internet Service Monitoring Configuration command-line interface is run, your username and encrypted password are stored and then updated if the **UserUpdate** parameter is set. Do not edit these properties.

ismbatch

Like the Internet Service Monitoring Configuration command-line interface, you can use **ismbatch** to automate many of the operations that you would otherwise perform using the Internet Service Monitoring user interface.

Using **ismbatch**, you can create and configure profiles, profile elements, including OID groups, and list the current configuration of these items. However, any changes that you make to profiles locally using **ismbatch** are not stored in the Tivoli Enterprise Portal Server database automatically and are not reflected in the Internet Service Monitoring user interface or Internet Service Monitoring Configuration command-line interface. Generally, you should use Internet Service Monitoring Configuration command-line interface in preference to **ismbatch**.

Tip: Use the XML-to-command-line-interface application (`xml2cli`) to migrate profiles created with **ismbatch** to a format suitable for use with the Internet Service Monitoring Configuration command-line interface. See "Converting profiles created with ismbatch to ismconfig operations" on page 104 for further information.

User profiles created using **ismbatch** are not visible in the Internet Service Monitoring Configuration window or to Internet Service Monitoring Configuration command-line interface. Deploying a user profile to a managed system on which **ismbatch** was used to create user profiles, or using the **Resync Agent** facility removes any existing profiles from that system.

Running ismbatch

To use the **ismbatch** commands, run them directly from the command-line.

Operations for **ismbatch** consist of the command to run, and where appropriate, one or more parameters.

To run **ismbatch** on UNIX, enter the following command:

```
$ISMHOME/bin/ismbatch -command [parameter=value ...]
```

To run **ismbatch** on Windows, use the command:

```
%ISMHOME%\platform\win32\bin\ismbatch -command [parameter=value ...]
```

You can prefix a command with either one or two hyphens (-).

ismbatch logs results of the operations that it performs to the file `$ISMHOME/log/ismbatch.log`.

Command-line syntax

To use the Internet Service Monitoring command-line interface commands, run them directly from the command-line.

Internet Service Monitoring command-line interface operations consist of the command to be executed, and where appropriate, one or more parameters.

To run Internet Service Monitoring command-line interface commands on UNIX, enter the following commands:

```
install_dir/ismconfig.sh -config -command [parameter=value ...]
```

```
install_dir/ismbatch -command [parameter=value ...]
```

To run Internet Service Monitoring command-line interface commands on Windows, enter the following command:

```
install_dir\ismconfig.cmd -config -command ["parameter=value" ...]
```

where *install_dir* is the location described in Table 18 on page 90.

```
install_dir\ismbatch -command ["parameter=value" ...]
```

where *install_dir* is the location described in “ismbatch” on page 94.

You can prefix a command with either one or two hyphens (-).

Log files

ismconfig logs results for the previous 10 operations to the file $CANDLE_HOME/logs/ismconfig.log.

ismbatch logs results of the operations that it performs to the file $ISMHOME/log/ism/ismbatch.log.

Command-line help

The Internet Service Monitoring command-line interface commands provide syntax help for each command and its parameters, which you can access directly from the command-line.

To obtain an overview of the syntax help available, enter:

```
./ISM command -help
```

To obtain information about a specific command, enter:

```
./ISM command -help command
```

To obtain a list of a monitor's parameters, enter:

```
./ISM command -help monitor_name
```

To list more details about a monitor's group parameters, add the expand option:

```
./ISM command -help monitor_name expand
```

In these commands:

ISM command is either: **ismconfig.sh -config** on UNIX systems; **ismconfig.cmd -config** on Windows systems; or **ismbatch**
command is the command for which you require syntax help
monitor_name is the monitor for which you require more information

In help listings, optional parameters are indicated by an asterisk (*) symbol.

Parameters

Parameters supply additional information for Internet Service Monitoring command-line interface commands.

The standard format of a parameter is *parameter=value*. For example, the command for listing all elements in a profile requires two parameters indicating the monitor and profile. To list all HTTP monitor elements in the profile named LocalWebServices, use the following command:

```
./ISM command -listelts monitor=http profile=LocalWebServices
```

where *ISM command* is either: **ismconfig.sh -config** on UNIX and Linux systems; **ismconfig.cmd -config** on Windows systems; or **ismbatch**

Parameter names are not case-sensitive. If required, you may omit parameter names and instead specify values for the parameters. For example, the previous command may be abbreviated to:

```
./ISM command -listelts http LocalWebServices
```

When omitting the parameter names you must specify their values in the order defined in the Internet Service Monitoring command-line help.

Every parameter associated with a command is either required or optional. When executing a command, you must always specify values for required parameters. Optional parameters may be omitted from the command entirely. If you omit an optional parameter, its default value is used, if one is defined.

Note: When specifying parameter values, it may be necessary to escape characters such as double quotes (") and brackets ([]) using backward slash characters (\) to prevent the operating system's command shell from interpreting those characters. Alternatively, add the commands to a text file and run that file using the `-file` command. See “Creating sequences of operations” on page 103 for further information.

Parameter groups

Some monitors provide extended or specialized types of testing in addition to the basic tests that they perform. For example the HTTP monitor provides features for testing proxy servers. When configuring a profile element that uses the extended testing options, you must specify additional parameters. Internet Service Monitoring command-line interface commands manage these additional parameters using parameter groups. For example, to use the proxy testing features of the HTTP monitor, you must specify values for additional parameters defined in the Proxy parameter group.

To obtain help about the parameter groups supported by a monitor, use the command:

```
/ISM command -help monitor expand
```

where *ISM command* is either: `ismconfig.sh -config` on UNIX systems; `ismconfig.cmd -config` on Windows systems; or `ismbatch`

To specify a parameter group in an `ismbatch` command, prefix the group name with the @ symbol, and then list each parameter in the group:

```
./ISM command -command parameter=value ... @parameter_group parameter=value ...
```

For example, to add an HTTP profile element to the profile `test_http` for testing the URL `www.xyz.com/home.html` over the proxy server `proxy.abc.com:3128`, use the following command:

```
./ISM command -add monitor=http profile=test_http server=www.xyz.com page=home.html
      @Proxy server=proxy.abc.com port=3128
```

If you want to specify further command parameters after the group that do not belong to the group, close the group using a single @ character. For example, the following commands have the same effect:

```
[1] ./ISM command -add monitor=http profile=test_http server=www.xyz.com
      page=home.html @Proxy server=proxy.abc.com port=3128 @ port=8080

[2] ./ISM command -add monitor=http profile=test_http server=www.xyz.com
      page=home.html port=8080 @Proxy server=proxy.abc.com port=3128
```

If you are using `ismbatch` on Microsoft PowerShell, add quotes to all parameters that use the at (@) symbol. For example, for `@DVC`, use `"@DVC"` instead.

Internet Service Monitoring command-line interface profile operations

Using profile operations, you can create, edit, modify, and delete profiles.

Profile operations

Table 23 on page 97 shows the profile operations commands and the associated parameters. The table uses unnamed parameters. If you want to use named arguments, use the `./ISM command -help`

command to determine the argument names, where *ISM command* is either: `ismconfig.sh -config` on UNIX systems; `ismconfig.cmd -config` on Windows systems; or `ismbatch`.

Table 23. Internet Service Monitoring command-line interface profile operations commands

Operation	Command	Parameters
Create a profile	`-new`	*new_profile* [active|inactive]
Delete a profile	`-deleteprofile`	*profile*
Delete all profiles	`-deleteallprofiles`	
List all profiles	`-listprofiles`	
Activate a profile	`-activateprofile`	*profile*
Activate all profiles	`-activateall`	
Deactivate a profile	`-deactivateprofile`	*profile*
Deactivate all profiles	`-deactivateall`	
Copy a profile	`-copy`	*profile new_profile* [active|inactive]
Rename a profile	`-rename`	*profile new_profile*
Validate all profiles *Deprecated*	`-validate`	
Update monitoring profile	`-monitoring`	*profile location periods*
Update all empty profile element fields for all profiles to include a default value. After older profiles are updated, they are compatible with newer Internet Service Monitoring versions.	`-updateall`	

Sample - Copying a profile

Copy a profile named `ibm`, name the copy `ibm2` and set the status of the copy to `inactive`:

```
./ismconfig.sh -config -copy ibm ibm2 inactive
```

Sample - Updating old profiles

Update all empty profile elements for all profiles to include a default value, repair broken profiles so that they conform to XML profile definitions, and provide information about which profiles are updated:

```
./ismconfig.sh -config -updateall
```

Note: When run with `ismbatch`, only the local XML profiles are updated and regenerated.

Tip: After you run the `./ismconfig.sh -config -updateall` command, run `./ismconfig.sh -config -resync` to propagate changes to the XML profiles deployed to the agents.

Internet Service Monitoring command-line interface profile element operations

Using profile element operations, you can create, edit, modify and delete profile elements and transactions steps.

Profile element operations

Table 24 on page 98 shows the profile element operations.

The operations listed here are described without parameter names. If you want to determine a parameter name, use the command `./`*ISM command* `-help` *command*, where *ISM command* is either: `ismconfig.sh -config` on UNIX systems; `ismconfig.cmd -config` on Windows systems; or `ismbatch`.

Table 24. Internet Service Monitoring command-line interface profile element operation commands

Operation	Command	Parameters
Create a profile element	`-add`	*monitorprofile* [active|inactive] *monitor_params* [@DVC] [@Params] [@SOAPInputs @SOAPOutputs] [@Regexp] [@Identifiers] *command*[@Body]
Modify a profile element	`-change`	*monitorprofile* element_index parameters [@DVC] [@Params] [@SOAPInputs @SOAPOutputs] [@Regexp] [@Identifiers]
Delete a profile element	`-delete`	*monitor profile element_index*
List the service level classifications in a profile element	`-showdvc`	*monitor profile element_index*
Activate a profile element	`-activate`	*monitor profile element_index*
Deactivate a profile element	`-deactivate`	*monitor profile element_index*
List all elements in a profile	`-listelts`	*monitor profile* **Tip:** You can use this command to obtain the *element_index* of a profile element or the *transaction_index* of a transaction step.
Add a transaction step	`-addstep`	*monitor profile transaction_index monitor_params* [@DVC] [@Params] [@SOAPInputs @SOAPOutputs] [@Regexp]

Table 24. Internet Service Monitoring command-line interface profile element operation commands (continued)

Operation	Command	Parameters
Modify a transaction step	`-changestep`	*`monitor profile transaction_index step_index monitor_params`* `[@DVC] [@Params] [@SOAPInputs @SOAPOutputs] [@Regexp]`
Delete a transaction step	`-deletestep`	*`profile transaction_index step_index`*
List the service level classifications in a transaction step	`-showdvc`	*`monitor profile transation_index step_ index`*
List all transaction steps	`-liststeps`	*`profile transaction_index`*

In Table 24 on page 98:

- Transaction steps apply only to TRANSX profile elements. SOAP inputs and outputs apply only to a SOAP profile elements.
- `@DVC` are values for the service level classification parameter group. For detailed information about service level classifications, see "Service level classification parameter group" on page 100.
- `@Params` are values for the Head/Form parameter group. Applies to the HTTP and HTTPS monitors.
- *`monitor_params`* are values for the monitor configuration fields specific to the selected monitor.
- `@Regexp` are values for the regular expression parameter group. Applies to the FTP, HTTP, HTTPS, IMAP4, NNTP, POP3, SOAP, and TCPPort monitors. For detailed information about regular expressions, see "Regular expression parameter group" on page 100.
- `@SOAPInputs @SOAPOutputs` are values for the SOAP input and output parameter groups. Applies to the SOAP monitor only. For detailed information about these groups, see "SOAP input and output parameter groups" on page 102.
- You can use either `element index` or `@Identifiers checksum`
- `@Identifiers` are values for setting unique identifiers for an element which would otherwise be automatically generated. Values must be unique for each element.

  Note: Do not specify these values unless it is necessary. Providing values that are not unique may interrupt monitoring.

  Use the following format:

```
@Identifiers [checksum] [datalog] [updated]
   [checksum]    ::=   ['checksum='] checksum_value
   [datalog]     ::=   ['datalog='] datalog_value
              [updated]                ::=        ['updated='] updated_time
```

  Where *checksum_value* and *datalog_value* identify the element and *updated_time* is the timestamp of the last change, in seconds.

  Note: The values *datalog_value* and *updated_time* apply only to ismbatch.

  For example:

```
    ismbatch -add ... @Identifiers myChecksum myDatalog
      1234 @...
    ismbatch -change .. @Identifiers myChecksum myDatalog
        1234 @...
```

```
ismbatch -add ... @Identifiers checksum=myChecksum
    datalog=myDatalog updated=1234 @...
ismbatch -change .. @Identifiers checksum=myChecksum
    datalog=myDatalog updated=1234 @...
```

You can specify any combination of `checksum`, `datalog`, or `updated` parameters in a command. Each `checksum` remains the same after repeated changes to an element unless specifically set. Each `datalogpath` is regenerated after each change from the element's current values unless specifically set. Each `updated` is set to the current time after each change from the element's current values unless specifically set.

- `@Body` are values for the command POST request only. Applies to the HTTP and HTTPS monitor only. For more information, see "Body" on page 84.
- If you are using `ismbatch` on Microsoft PowerShell, add quotes to all parameters that use the at (@) symbol. For example, for `@DVC`, use `"@DVC"` instead.

Sample - Creating a profile element

Create a profile element in the profile `ibm` that configures the HTTP monitor to check the availability of the web page `http://www.ibm.com/index.html`. Use default settings for monitor configuration fields:

```
./ismconfig.sh -config -add monitor=HTTP profile=ibm server=www.ibm.com
    page=index.html description="IBM home page"
```

Regular expression parameter group
The `Regexp` parameter group defines regular expressions for profile elements and transaction steps. You can use this group with the FTP, HTTP, HTTPS, IMAP4, NNTP, POP3, and TCP Port monitors.

The parameter group has the following format:

```
@Regexp {1 "regex1"} [{2 "regex2"} ...]
```

- *regexn* defines the regular expression. See Appendix F, "Regular expression syntax in Internet Service Monitoring," on page 123 for a list of operators supported.
- Maximum number of regular expressions is 50.
- Results of regular expression matching can be used in service level classifications by testing the values of the `regexpMatch`*n* and `regexpStatus`*n* elements.

Service level classification parameter group
The `DVC` parameter group defines the service level classification for a profile element or transaction step.

The parameter group has the following format:

```
@DVC default_status statement_count {if_statement ...}
```

- *default_status* defines the default status of the service level classification; either `GOOD`, `MARGINAL`, or `FAILED`.
- *statement_count* indicates the total number of service level classification `If` statements.
- *if_statement* defines a single service level classification `If` statement.

Note: The DVC group must not contain a naming syntax. For example, `@DVC GOOD 2` is valid, however `@DVC=GOOD statement_count=2` is not.

`If` statements have the following format:

```
id status{GOOD|MARGINAL|FAILED} expression_count {test_expression ...}
```

- *id* is a number identifying each `If` statement.
- *status* is the service level classification value associated with the `If` statement; either `GOOD`, `MARGINAL`, or `FAILED`.

- *expression_count* indicates the total number of test expressions.
- *test_expression* defines a service level classification test expression.

Test expressions have the following format:

```
monitor_element comparison_operator threshold_value
```

- *monitor_element* is the name of the monitor element used in the classification.
- *comparison_operator* is the test applied to the value of the monitor element; either GT, LT, EQ, GT_EQ, LT_EQ, NEQ, BETWEEN, OUTSIDE, CONTAINS, or NCONTAINS.
- *threshold_value* is the threshold value for the service level.

Sample - Modifying a service level classification

Modify the service level classification for the first transaction step in the profile WebTransx to the following:

```
If totalTime > 20 then status FAILED
else if totalTime > 10 then status MARGINAL
else status GOOD
```

Use the command:

```
./ismconfig.sh -config -changestep monitor=HTTP profile=Transx element=1 step=1
@DVC GOOD 2 1 FAILED 1 totalTime GT 20 2 MARGINAL 1 totalTime GT 10
```

OID group operations

Using OID group operations, you can create, edit, modify, manage, and delete OID groups which are required for performing tests with the SNMP monitor.

Table 25 on page 101 shows the OID group operations and the associated parameters. All operations described here are listed without parameter names. To determine a parameter name, use the command: `./`*ISM command* `-help` *command*, where *ISM command* is either: `ismconfig.sh -config` on UNIX systems; `ismconfig.cmd -config` on Windows systems; or `ismbatch`.

Table 25. Internet Service Monitoring Configuration command-line interface OID group operations

Operation	Command	Parameters
Create an OID group	-addoidgroup	*OID_group*
Delete an OID group	-deleteoidgroup	*OID_group*
Delete all OID groups	-deletealloidgroups	
List all OID groups	-listoidgroups	
Add an OID to an OID group	-addoid	*OID_groupOID_name OID_value OID_unit [OID_selector]*
Modify an OID in an OID group	-editoid	*OID_group element_index* [new_element_name] [new_element_value] [OID_name] [new_element_unit] [new_element_selector]
Delete an OID from an OID group	-deleteoid	*OID_group element_index*

Table 25. Internet Service Monitoring Configuration command-line interface OID group operations (continued)		
Operation	**Command**	**Parameters**
List all OIDs in an OID group	`-listoids`	*OID_group*

SOAP input and output parameter groups
The SOAPInputs parameter group defines the data names, data types, attributes, and *assigned* values that the SOAP monitor sends to a SOAP interface during a service test. The SOAPOutputs parameter group defines the data names, data types, attributes, and *expected* values that the target SOAP interface will return to the SOAP monitor during the test.

Run the command *ISM command* `-help SOAPParams` to display a list of supported SOAP parameters.

The SOAPInputs parameter group has the following format:

```
@SOAPInputs [dataname:datatype=assigned_value,
 dataname:datatype=assigned_value, ...]
```

The SOAPOutputs parameter group has the following format:

```
@SOAPOutputs [dataname:datatype[=expected_value],
 dataname:datatype[=expected_value],     ...]
```

The variable *expected_value* is optional in the output group.

Note: Ensure that you enter the data names exactly as they appear in the local Web Service Definition Language (WSDL) file and that the data types also match. The WSDL file to be used for the SOAP monitor is specified by the `wsdl` parameter of the profile element.

Data types may be simple, array or user-defined. Simple data types include integer, string, and Boolean. A full list of supported simple types is provided in the SOAP monitor guidelines. Array and user-defined data types may contain simple data types as well as other array and user-defined data types.

Simple type format:

```
[dataname:simple_type=value,dataname:simple_type=value,...]
```

Example:

```
@SOAPInputs [in0:integer=123, in1:string=\"xyz\"]
```

Array format:

```
[dataname:simple_type[]=[value,value,...]]
```

Example:

```
@SOAPInputs [count:integer[]=[1,2,3]]
```

User-defined:

```
[dataname:{identifier:simple_type,identifier:simple_type, ...}
    ={identifier=value,identifier=value, ...}]
```

Example 1:

```
@SOAPInputs [contact:{name:string,phone:integer}={name=\"JSMITH\",phone=55512346}]
```

Example 2, including optional attributes in parentheses, marked in bold:

```
@SOAPInputs [ outer:{item1:string,item2:string}(aaa:string='bbb')=
 {item1(attr:string='ccc')='',item2(attr:string='ddd',attr2:string='eee')='fff'} ]
@SOAPOutputs [ return:double(brand:string='TIVOLI',product:string='ISM')=\"42\" ]
```

Note: String values that contain a space must be enclosed in an additional set of double quotes ("). For example, `"\"xyz company\""`.

Creating sequences of operations

You can create sequences of operations for executing more than one Internet Service Monitoring command-line interface operation.

To define a sequence, create a text file and list each required operation on a new line. To run the operations, use the command:

```
./ISM command -file operations_file
```

where:

ISM command is either: `ismconfig.sh -config` on UNIX systems; `ismconfig.cmd -config` on Windows systems; or `ismbatch`
operations_file is the name of the text file containing the command sequence (include the full path name of the file)

Sample - Executing a sequence of operations

Create a sequence of operations to perform the following tasks:

1. Create a profile named `ibm`, and add a profile element for the HTTP monitor that checks the availability of the web page `http://www.ibm.com/index.html`. Use default settings for monitor configuration fields.
2. Create a profile element for the FTP monitor that checks the availability of the FTP server `ftp.ibm.com` by downloading the file `/sales/prodlist.tar.Z` to `/temp/ftp-test.tar.Z`. Use default settings for monitor configuration fields.

To perform these tasks, create a text file named `ibmOps` containing the following:

```
[1]-add monitor=HTTP profile=ibm server=www.ibm.com page=index.html
   formname=HEAD description="HTTP test"
[2]-add monitor=FTP profile=ibm server=ftp.ibm.com
   localfile=/sales/prodlist.tar.Z remotefilename=/temp/ftp-test.tar.Z
   description=FTP test
```

Run the operations using the command:

```
./ismconfig.sh -config -file ibmOps
```

Profile scheduling operations

Using Internet Service Monitoring command-line interface you can create or modify profile schedules.

Profile scheduling operations have the format:

```
./ISM command -monitoring profile periods
```

The *ISM command* parameter is either: `ismconfig.sh -config` on UNIX systems; `ismconfig.cmd -config` on Windows systems; or `ismbatch`

The *profile* parameter determines the profile being scheduled. Specifying ALL in place of a profile name affects the schedule of all profiles.

The *periods* parameter defines a scheduling period during which monitoring is either active or inactive.

```
state~days[xtimes][=days[xtimes]]
```

- *state* determines whether monitoring is active during the monitoring period: ON|OFF
- *days* specifies the days of the week covered by the monitoring period:

```
ALL|{day[-day][,day[-day]]}
```

  day selects a day of the week: SU|MO|TU|WE|TH|FR|SA

  The first day of the week is set to Sunday. If you want to change this, set the following propery:

```
StartingDay : day
```

  where *day* is the full name of the required starting day.

  – For ismconfig, set the property in ismconfig.props which is installed to the directory listed in Table 18 on page 90.
  – For ismbatch, create a text file called ismbatch.props in $ISMHOME/etc/props and set the property
- *xtimes* (x is a separator) specifies the start and end times of the monitoring period in 24-hour format:

```
start_time-end_time[,start_time-end_time]
```

  – *start_time* has the format 0[:00]|*mid_time*
  – *end_time* has the format 24[:00]|*end_time*
  – *mid_time* has the format {1..23}[:{00..59}]

Sample - Profile scheduling

Disable monitoring of all profiles on Saturdays:

```
./ismconfig.sh -config -monitoring ALL OFF~SA
```

Enable monitoring of all profiles between 6:00am and 6:15am on Wednesdays, and 1:45pm and 5pm on Sundays:

```
./ismconfig.sh -config -monitoring ALL ON~WEx6:00-6:15=SUx13:45-17:00
```

Converting profiles created with ismbatch to ismconfig operations

You can convert XML monitor profiles created using ismbatch to Internet Service Monitoring Configuration command-line interface (ismconfig) commands using the xml2cli application.

Using xml2cli, you create a text file which saves the monitor profiles created with ismbatch as a set of operations. You can then run those operations as a sequence using Internet Service Monitoring Configuration command-line interface. In this way profiles originally created with ismbatch can be sent to the Tivoli Enterprise Portal Server, distributed across your enterprise, or used with the Internet Service Monitoring Configuration command-line or user interfaces as required.

xml2cli syntax

The xml2cli application uses the following command syntax:

```
xml2cli [PARAMETER] ...
```

The parameter can be one of the following:

-m *monitor*, specify a monitor name for conversion
-p *profile*, specify a profile for conversion
-f *output*, specify an output file

Running xml2cli

The xml2cli application is installed to the same directory as ismbatch. To use the xml2cli command, run it directly from the command-line with the required parameter.

To run `xml2cli` on UNIX systems and convert all XML monitor profiles in the default location to standard screen output, enter the following command:

```
$ISMHOME/bin/xml2cli
```

To run `xml2cli` on Windows systems and convert all XML monitor profiles in the default location to standard screen output, use the command:

```
%ISMHOME%\platform\win32\bin\xml2cli.exe
```

To display help information for the `xml2cli` command, run the following command:

```
./xml2cli -help
```

Samples

To convert the profile `IBM` on UNIX systems, run the following command:

```
./xml2cli -p IBM
```

To convert all HTTP monitor profiles on UNIX systems, run the following command:

```
./xml2cli -m HTTP
```

To convert the HTTP IBM profile on UNIX systems, run the following command:

```
./xml2cli -m HTTP -p IBM
```

To convert all XML monitor profiles to the file `output.txt` on UNIX systems, run the following command:

```
./xml2cli -f output.txt
```

Alternatively, you can run `./xml2cli > output.txt`.

To convert all XML monitor profiles to the file `output.txt`, and then run the operations using Internet Service Monitoring Configuration command-line interface, run the following commands:

```
$ISMHOME/bin/xml2cli -f output.txt
CANDLE_HOME/arch/cj/lib/ismconfig.sh -config -file output.txt
```

Tip: Use the **-u** parameter to specify the user name in each **ismconfig** command:

```
$CANDLE_HOME/arch/cj/lib/ismconfig.sh [-u username] -command[parameter=value ...]
```

Tip: On Windows systems, if `ismconfig` fails to process the path name, ensure that the argument `-file` for the input file name does not contain any spaces in the file path or file name. Also try using double backslashes (\\) instead of single backslashes (\).

Tip: You can use this approach to migrate Internet Service Monitoring tables to a newly migrated Tivoli Enterprise Portal Server database. Copy the `output.txt` file generated by the `xml2cli` command to the new Tivoli Enterprise Portal Server before you run the `ismconfig` command to recreate the Internet Service Monitoring profile table content. Ensure you then resynchronize the agents so that the existing profiles are updated.

Appendix A. Installing and uninstalling the language pack

By default, ITCAM for Transactions is enabled for the English language. If you want to use the product in another language, you must install the translated language pack. The language packs are available on the language support image for each component.

ITCAM for Transactions provides language packs in the following languages:

- Brazilian
- French
- German
- Hungarian
- Italian
- Japanese
- Korean
- Polish
- Portuguese
- Russian
- Simplified Chinese
- Spanish
- Traditional Chinese

The National Language Support resources for ITCAM for Transactions agent are provided on a separate CD that is shipped with ITCAM for Transactions.

Note: Before you can install a language pack, you must install the components of ITCAM for Transactions in English.

Installing and uninstalling a language pack on Windows systems

Before you begin installing the language pack, make sure that you comply with the following requirements:

- Install the English version of ITCAM for Transactions.
- Determine the installation directory of ITCAM for Transactions on the computer where you plan to run the language pack installation program. You must install the language packs in the same directory.
- The default installation directory for the Tivoli Enterprise Portal Server and the Tivoli Enterprise Management Agent is `C:\IBM\ITM`.
- The Language Pack installation requires Java Runtime Environment (JRE) 1.4.x or above. Use the JRE that was installed by IBM Tivoli Monitoring (on the Tivoli Enterprise Portal) or the JRE installed by the base product driver. The default path for that JRE is `C:\Program Files\IBM\Java142`.

Use one of the following methods for installing or uninstalling a language pack on Windows:

- "Installing a language pack on Windows systems" on page 108
- "Silently installing a language pack on Windows" on page 108
- "Uninstalling a language pack on Windows systems" on page 109

Install separate language packs for each of the ITCAM for Transactions subcomponents:

- Internet Service Monitoring

- Response Time
- Transaction Tracking

Installing a language pack on Windows systems

The language pack installation programs are provided on the *ITCAM for Transactions Language Support* CD.

The language pack must be installed on the computer running the Tivoli Enterprise Portal and the computer running the agent.

Note: If the agent is installed on the same computer as the Tivoli Enterprise Monitoring Server, install the language pack on both the Tivoli Enterprise Portal Server and the Tivoli Enterprise Monitoring Server.

To install the language pack:

1. Run `lpinstaller.exe` from the Language Pack CD.
2. Select the language of the installer and click **OK**.
3. Click **Next** on the Introduction window.
4. Click **Add/Update** and then click **Next**.
5. Select the folder in which the National Language Support package (`NLSPackage`) files are located and click **Next**.
6. Select the language support for the required agent and click **Next**.

   Tip: Hold down the Ctrl key to select multiple entries.
7. Select the languages that you want to install and click **Next**.
8. Verify the installation summary page and click **Next** to begin the installation.
9. Click **Next**.
10. When the installation is complete, click **Finish** to exit the installer.
11. Restart the agent and any relevant IBM Tivoli Monitoring components installed on the computer.

Silently installing a language pack on Windows

To install the language pack using the silent installation procedure, use a response file. The response file enables you to run the installation in silent mode without user interaction. The ITCAM for Transactions language pack provides you with the `ITM_Agent_LP_silent.rsp` template response file that you can customize to reflect the correct installation directories.

To run a silent installation, perform the following steps:

1. Copy `ITM_Agent_LP_silent.rsp` to the directory where `lpinstaller.bat` is located (that is, the IBM Tivoli Monitoring agent language pack build location.)
2. Modify the response file so that it is correct for your environment. For example, set the following parameters in the response file:

   ```
   INSTALLER_UI;
   CHOSEN_INSTALL_SET;
   NLS_PACKAGE_FOLDER;
   PROD_SELECTION_PKG;
   BASE_AGENT_FOUND_PKG_LIST;
   LANG_SELECTION_LIST
   ```
3. From a command line run the following command:

   ```
   lpinstaller.bat -f responseFileName
   ```

   Where, *responseFileName* is the fully qualified path to the response file (either the `ITM_Agent_LP_silent.rsp` default file or one that you customize) containing the installation options.

For example, `lpinstaller.bat -f ITM_Agent_LP_silent.rsp`.

Uninstalling a language pack on Windows systems

Before uninstalling a language pack, ensure that ITCAM for Transactions, IBM Tivoli Monitoring, the Java runtime environment and the language pack are still installed.

Follow these steps to remove the language pack:

1. Run `lpinstaller.exe` from the Language Pack CD.
2. Select the language of the installer and click **OK**.
3. Click **Next** on the Introduction window.
4. Click **Remove** and then click **Next**.
5. Select the language support for the required agent, and click **Next**.

   Tip: Hold down the Ctrl key to select multiple entries.
6. Select the languages that you want to uninstall and click **Next**.
7. Verify the installation summary page and click **Next** to begin uninstalling.
8. When the process is complete, click **Finish** to exit the installer.
9. Restart the agent and any relevant IBM Tivoli Monitoring components installed on the computer.

Installing and uninstalling a language pack on Linux or UNIX systems

Before you begin installing the language pack, complete the following tasks:

- Install the English version of ITCAM for Transactions.
- Verify the installation directory of ITCAM for Transactions on the computer where you plan to run the language pack installation program. You must install the language packs to the same directory.
- Verify that the default installation directory for the Tivoli Enterprise Portal and the Tivoli Enterprise Management Agent is: `/opt/IBM/ITM`.
- The Language Pack installation requires Java Runtime Environment (JRE) 1.4.x or above. Use the JRE that was installed by IBM Tivoli Monitoring (on Tivoli Enterprise Portal Server) or the JRE installed by the base product driver. The default path for that JRE is `/opt/IBM/ITM/JRE`.

Choose one of the following methods for installing or uninstalling a language pack on Linux or UNIX:

- "Installing a language pack on Linux or UNIX systems" on page 109
- "Silently Installing a language pack on Linux or UNIX" on page 110
- "Uninstalling a language pack on Linux and UNIX systems" on page 111

Install separate language packs for each of the ITCAM for Transactions subcomponents:

- Internet Service Monitoring
- Response Time
- Transaction Tracking

Installing a language pack on Linux or UNIX systems

The language pack installation programs are provided on the *ITCAM for Transactions, Language Support CD*.

The language pack must be installed on both the computer running the Tivoli Enterprise Portal and the computer running the agent.

Note: If the agent is installed on the same computer as the Tivoli Enterprise Monitoring Server, install the language pack on both the Tivoli Enterprise Portal Server and the Tivoli Enterprise Monitoring Server.

To install the language pack:

1. Run the following command to create a temporary directory on the computer. Make sure that the full path of the directory does not contain any spaces: `mkdir dir_name`
2. Mount the language pack CD to the temporary directory you just created.
3. Run the following command to start the installation program:

   ```
   cd dir_name
   lpinstaller.sh -c ITM Home Directory [-i install_mode]
   ```

   Where:

   ITM Home Directory is where you installed IBM Tivoli Monitoring, usually `/opt/IBM/ITM` for AIX and Linux systems.
   install_mode is either `gui`, `console`, or `silent`. For Turkish, use `GUI` instead of`gui`.
4. Select the language of the installer and click **OK**.
5. Click **Next** on the Introduction window.
6. Click **Add/Update** and then click **Next**.
7. Select the folder in which the National Language Support package (`NLSPackage`) files are located and click **Next**.
8. Select the language support for the required agent and click **Next**.

   Tip: Hold down the Ctrl key to select multiple entries.
9. Select the languages that you want to install and click **Next**.
10. Verify the installation summary page and click **Next** to begin the installation.
11. Click **Next**.
12. When the installation is complete, click **Finish** to exit the installer.
13. Restart the agent and any relevant IBM Tivoli Monitoring components installed on the computer.

Silently Installing a language pack on Linux or UNIX

To install the language pack using the silent installation procedure you use a response file. The response file enables you to run the installation in silent mode without user interaction. The ITCAM for Transactions language pack provides you with the `ITM_Agent_LP_silent.rsp` template response files. This is the template response file that you can customize to reflect your correct installation directories.

Note: Before installing a language pack using silent mode, ensure that you have already installed the product in English.

To run a silent installation, perform the following steps:

1. Copy `ITM_Agent_LP_silent.rsp` to the directory where `lpinstaller.sh` is located (that is, the IBM Tivoli Monitoring agent language pack build location.)
2. Modify the response file so that it is correct for your environment. For example, set the following parameters in the response file:

   INSTALLER_UI;
   CHOSEN_INSTALL_SET;
   NLS_PACKAGE_FOLDER;
   PROD_SELECTION_PKG;
   BASE_AGENT_FOUND_PKG_LIST;
   LANG_SELECTION_LIST
3. Run the following command to create a temporary directory, ensuring that the full directory path does not contain any spaces:

   ```
   mkdir dir_name
   ```
4. Mount the language pack CD to the temporary directory that you just created.

5. Run the following command to launch the installation program:

```
cd dir_name
 lpinstaller.sh -c $CANDLE_HOME -i silent -f responseFileName
```

   Where:

   - $CANDLE_HOME is the directory to which IBM Tivoli Monitoring is installed. For example, `/opt/IBM/ITM` for AIX and Linux.
   - *responseFileName* is the fully qualified path to the response file (either the default `ITM_Agent_LP_silent.rsp` file or a file that you customize) containing the installation options.
6. Restart the agent and any relevant IBM Tivoli Monitoring components installed on the computer.

Uninstalling a language pack on Linux and UNIX systems

Before uninstalling a language pack, ensure that ITCAM for Transactions, IBM Tivoli Monitoring, the Java runtime environment and the language pack are still installed.

Follow these steps to remove the language pack:

1. Run the following command to create a temporary directory on the computer. Make sure that the full path of the directory does not contain any spaces: `mkdir dir_name`
2. Mount the language pack CD to the temporary directory you just created.
3. Run the following command to start the installation program:

```
cd dir_name
./lpinstaller.sh -c ITM Home Directory [-i install_mode]
```

   Where:

   ITM Home Directory is where you installed IBM Tivoli Monitoring, usually `/opt/IBM/ITM` for AIX and Linux systems.
   install_mode is either `gui`, `console`, or `silent`. For Turkish, use `GUI` instead of`gui`.
4. Select the language of the installer and click **OK**.
5. Click **Next** on the Introduction window.
6. Click **Remove** and then click **Next**.
7. Select the language support you want to uninstall and click **Next**.

   Tip: Hold down the Ctrl key to select multiple entries.
8. Select the languages that you want to uninstall and click **Next**.
9. Verify the installation summary page and click **Next** to begin uninstalling.
10. When the process is complete, click **Finish** to exit the installer.
11. Restart the agent and any relevant IBM Tivoli Monitoring components installed on the computer.

Appendix B. Internet Service Monitoring open ports

Internet Service Monitoring opens ports on the host computer when it is installed.

Table 26 on page 113 lists the ports opened on the host machine.

Table 26. Default ports for Internet Service Monitoring

Connection	Default Port	Configuration
Databridge to Internet service monitoring agent	`9520/tcp`	To change the default port, edit the `TEMAPort` property in the `kisagent.props` file. See Table 8 on page 48 for further information.
Service monitors to Databridge	`9510/tcp`	To change the default port, edit the `SocketPort` property in the `bridge.props` file. See "Databridge properties and command line options" on page 42 for further information.

Appendix C. Internet Service Monitoring directory structure

Internet Service Monitoring installs to a subdirectory of the ITM directory structure, known as `ISMHOME`. On Windows systems, `ISMHOME` is `c:\IBM\ITM\tmaitm6\ism`; on Linux and UNIX systems it is `/opt/IBM/ITM/arch/is`.

Table 27 on page 115 lists the directory structure for Internet Service Monitoring version Internet Service Monitoring version V7.2 and explains the purpose of each directory.

Table 27. Internet Service Monitor directory structure

Directory	**Purpose**
`$ISMHOME/certificates`	Directory for the Databridge SSL certificate files.
`$ISMHOME/datalogs`	Root directory for datalog files that are generated by the Datalog module.
`$ISMHOME/datalogs/default`	Directory for the default datalog files that are used by the Datalog module.
`$ISMHOME/etc/props`	Directory for system properties files. Properties file control the operation of the system components including the Internet service monitors.
`$ISMHOME/etc/rules`	Directory for rules files that are used by the ObjectServer module and the Internet service monitors to convert events into IBM Tivoli Netcool/OMNIbus alerts.
`$ISMHOME/log`	Directory for system log files as well as error files (`.err`).
`$ISMHOME/mibs`	Directory for MIB files that are used by SNMP-based Internet service monitors.
`$ISMHOME/objectserver/bin`	Directory for the interfaces file that is used to connect the ObjectServer module to an ObjectServer on UNIX systems.
`$ISMHOME/objectserver/etc`	Directory for the connections data file (`omni.dat`) that is used to connect the ObjectServer module to an ObjectServer on UNIX systems.
`$ISMHOME/platform/arch/bin`	Directory for system executable files and the command line configuration utility (`ismbatch`). *Arch* is the name of the platform. For example, Win32 for Windows systems.
`$ISMHOME/profiles`	Root directory used for profiles.
`$ISMHOME/profiles/active`	Directory used for active profiles.

Table 27. Internet Service Monitor directory structure (continued)	
Directory	**Purpose**
`$ISMHOME/profiles/default`	Directory used for default profile templates.
`$ISMHOME/profiles/deleted`	Directory used for deleted profiles and profiles that are corrupt.
`$ISMHOME/profiles/inactive`	Directory used for inactive profiles.
`$ISMHOME/profiles/obsolete`	Directory used for profiles that are no longer compliant with the current version of Internet Service Monitoring .
`$ISMHOME/scripts`	Directory used for the Internet Service Monitoring script files.
`$ISMHOME/scripts/SAA`	Directory used for the SAA monitor script files.
`$ISMHOME/scripts/RPING`	Directory used for the RPING monitor script files.
`$ISMHOME/var`	Directory for the Raw Capture file that is used by the ObjectServer, also the directory for the Store and Forward file that is used by the Databridge.
`%ISMHOME%\objectserver\ini`	Directory for the connections data file (`sql.ini`) that is used to connect the ObjectServer module to an ObjectServer on Windows systems.
`%CANDLE_HOME%\TMAITM6`	Directory for the connection information that connects the Internet service monitoring agent to the IBM Tivoli Monitoring module on Windows systems.

Appendix D. Tivoli Enterprise Console event mapping

Generic event mapping provides useful event class and attribute information for situations that do not have specific event mapping defined. Each event class corresponds to an attribute group in the monitoring agent. For a description of the event slots for each event class, see the tables described in this appendix. For more information about mapping attribute groups to event classes, see the Tivoli Enterprise Console product documentation.

Configuring the Tivoli Enterprise Console

To configure the Tivoli Enterprise Console, complete the following procedure:

1. Ensure sure that the TEC IF is configured to point to the correct Tivoli Enterprise Console server with the correct host port information.
2. Install the `om_tec.baroc` and `kt<n>.baroc` files into a rule base for Tivoli Enterprise Console and activate it.

   Note: When you install Tivoli Enterprise Monitoring Server support, the installation places the baroc files into one of the following directories, depending on your operating system:

   - On Windows systems: `%CANDLE_HOME%\CMS\teclib`
   - On UNIX systems: `$CANDLE_HOME/tables/`*`TEMS_NAME`*`/TECLIB`

   The following `kt`*`n`*`.baroc` files are available:

   - `kt3.baroc`, for the Application Management Console event classes.
   - `kt5.baroc`, for the Web Response Time event classes.
   - `kt6.baroc`, for the Robotic Response Time event classes.
3. In this same directory, edit the `tecserver.txt` file to add the situations for which you want to see events, using the following format:

   ```
   SituationName=*,SEVERITY=CRITICAL|WARNING|UNKNOWN
   ```
4. Restart the Tivoli Enterprise Monitoring Server.

Specifying attributes to include in events

Event data forwarded to Tivoli Enterprise Console is defined by the content of the following two file types in the Tivoli Enterprise Monitoring Server file system:

- Baroc files
- Event Mapping files

Baroc files, sometimes referred to as *event class definition* files, define different types of classes of events that an event server can receive. Event class definitions are generally structured as shown in the following example (keyword syntax is in upper case):

```
TEC_CLASS: class_name ISA super_class_name
DEFINES {
attribute_definitions;
};
END
```

The syntax for baroc files is case sensitive. The baroc files supplied with the various ITCAM for Transactions agents have *attribute_definitions* comprising an attribute name and data type. The following data types are used in these baroc files:

- STRING - A string value
- REAL - A real value

- ENUM - A value of an enumeration
- INT32 - A 32-bit integer value
- INTEGER - A 29-bit integer value

Detailed information regarding Event Classes and Attributes can be found in the Rule Developers Guide, located at the following website:`http://publib.boulder.ibm.com/infocenter/tivihelp/v3r1/index.jsp?topic=/com.ibm.itecruledev.doc/ecodmst.htm`

Event Mapping files are XML files that specify how situation events data is mapped to baroc file event classes and attributes. Event mapping files are located in the same directory as the baroc files, and are similarly named:

- `kt3.map`, for the Application Management Console event classes.

The event mapping file has the following format:

```
<itmEventMapping:agent>
  <id>xx</id>
  <version>n.n</version>
  <event_mapping>
    <attributeTable>
      <class/>
      <slot>
        <mappedAttribute/>
        or
        <mappedAttributeEnum/>
      </slot>
      :.......... one or more slot tags
    </attributeTable>
    :.......... one or more attributeTable tags
  </event_mapping>
</itmeventMapping:agent>
```

The syntax and usage of the tags in the mapping file are described as follows:

<attributeTable>
Syntax: `<attributeTable name="attribute_table_name" [freeSpace="nnnn"]>`, where *nnnn* is an integer value.

Usage: The freeSpace="*nnnn*" parameter is the maximum free space available in the TEC event buffer for additional slots after all of the slots that are defined in this event map are built.

<slot>
Syntax: `<slot name="slot_name">`

Usage: Defines a slot in the TEC event. The name of the slot is *slot_name*.

<mappedAttribute>
Syntax: `<mappedAttribute name="attribute_name" [multiplier="nnn"]>`

Usage: Specifies the attribute name that is mapped to the slot being defined. If *attribute_name* is not included in the event data, a null value is used. If the optional `multiplier=` parameter is specified and the value of the attribute is numeric, the value assigned for the slot is the attribute value multiplied by the number specified in the `multiplier=` parameter.

<mappedAttributeEnum>
Syntax: `<mappedAttributeEnum name="attribute_name">`

Usage: similar to the <mappedAttribute> tag, except if the attribute is defined as an enumerated value in the attribute file, the external enumerated string is used as the slot value instead of the attribute value. If there is no external enumerated string defined that matches the attribute value, the attribute value is used instead.

By default, not every attribute is included in events that are sent to Tivoli Enterprise Console. See the Attribute Groups section of the Response Time chapter in the *User's Guide* for an indication of which attributes in each group are preselected to be forwarded in events to Netcool/OMNIbus or Tivoli Enterprise Console.

Appendix E. Historical data collection

To view data in the history workspaces, you need to first set up historical data collection.

Setting up historical data collection

In order to view data in the history workspaces, you first need to configure historical data collection and distribute historical data collection attribute groups to your managed systems.

The history data collection settings apply to both short-term (up to 24 hrs) and long-term (indefinite) reporting. History data collection includes summarization and pruning settings for long-term data that is stored in the Tivoli Data Warehouse. Specify history data collection through the History Collection Configuration feature in the Tivoli Enterprise Portal. (You must have `Configure History` permission to see and use this feature.)

Tip: No historical data is posted to the Tivoli Data Warehouse until you configure summarization and pruning intervals for that metric.

The following components of IBM Tivoli Monitoring should already be installed to support historical data collection:

- Data warehouse located on a supported DB2, Oracle, or Microsoft SQL database.
- Warehouse Proxy agent, used to collect the information that is stored in the data warehouse.
- Warehouse Summarization and Pruning agent, used to perform aggregation and pruning functions on the data.

For more information about these components, see your IBM Tivoli Monitoring documentation.

Setting up historical data collection - general procedure

Use the following general procedure to configure your ITCAM for Transactions agents for historical data collection:

1. Log on to the Tivoli Enterprise Portal.
2. From the Tivoli Enterprise Portal menu bar, click History Configuration icon to display the **History Collection Configuration** window, similar to the History Collection Configuration window.
3. In the **Monitored Applications** list, select the collection setting that you want to configure, such as Internet Service Monitors. Configure one collection setting for each historical attribute group.
4. On the **Basic** tab, in the Configuration section, set the collection settings:
   a. In the **Description** field, enter a description for the collection setting.
   b. In the **Collection Interval** field, leave the default collection interval of `5 minutes`.
   c. In the **Collection Location** field, leave the collection location as the agent (TEMA)
   d. In the **Warehouse Interval** field, set the warehouse interval to `1 hour`.

   Tip: The name of the binary history file for the selected attribute group is displayed in the information bar, for example KT6_T6APPCS.
5. On the **Distribution** tab, leave the default to collect historical data on the agent (**Managed System (Agent)**) and select the managed systems to which you want to distribute the historical data collection.
6. Click **Apply** to save your distribution changes. The icon for the collection setting name in the Monitored Applications list changes to green. A gray icon indicates that the attribute group for that historical data collection has not yet been distributed to a managed system.
7. In the **Monitored Applications** list, select the component for which you want to set summarization and pruning, such as **Robotic Response Time**.
8. In the **Select Attribute Groups** pane, select an attribute group to configure for warehousing.

9. In the **Summarization** section of the **Configuration controls** pane, set how often you want a summary of the data. You can set multiple intervals which should match the Pruning intervals.
10. In the **Pruning** section of the **Configuration controls** pane, set how often you want the data purged. You can set multiple intervals which should match the summarization intervals
11. Click **Apply**.
12. Repeat steps 3-11 for each agent group you want to configure.

Tip: Ensure that if you set summarization and pruning for an attribute group, you also configure a collection setting to distribute that attribute group to a managed system.

Setting up historical data collection for Internet Service Monitoring

The history data collection settings apply to both short-term (up to 24 hrs) and long-term (indefinite) reporting. History data collection includes summarization and pruning settings for long-term data that is stored in the Tivoli Data Warehouse.

Historical data collection is specified through the History collection configuration feature in the Tivoli Enterprise Portal. You must have Configure History permission to see and use this feature.

In the **History Collection Configuration** window, select **Internet Service Monitors** in the **Monitored Applications** list to configure history data settings.

Configure historical data collection for both individual monitors and for attribute groups to populate specific history workspace views. The following table shows:

- Attribute group - the name of the attribute group that must be configured and distributed to the Internet Service Monitoring agents so that you can view:
  - Historical data using the Time Span option in status and statistics views
  - Data in history views
- Short Term History file - the name of the file used on the agent or TEMS to store data to be warehoused for the corresponding attribute group

Workspace/View	Attribute Group	Short Term History file
Internet Service Monitors / Service Status	KIS SERVICE STATISTICS	KISSSTATS
Host Statistics/Hosts Select Host > Link to Host Elements	KIS HOST STATISTICS KIS SERVICE INSTANCE STATISTICS	KISHSTATS KISSISTATS
Monitor Status/Services Select Service Type (for example, http) > Link to Service Type Select Any row > Link to Element History	KIS MONITOR STATUS KIS *monitor*, for example KIS HTTP KIS *monitor*, for example KIS HTTP	KISMSTATS KIS*monitor*, for example KISHTTP KIS*monitor*, for example KISHTTP

Workspace/View	Attribute Group	Short Term History file
Profile Statistics/Profiles Select Profile > Link to Services Select Service > Link to Elements Select Any row > Link to *monitor* Element History Select Any row > Link to Service Level History	KIS SERVICE INSTANCE STATISTICS KIS SERVICE INSTANCE STATISTICS KIS SERVICE INSTANCE STATISTICS KIS *monitor*, for example KIS HTTP KIS SERVICE INSTANCE STATISTICS	KISSISTATS KISSISTATS KISSISTATS KIS*monitor*, for example KISHTTP KISSISTATS
Service Statistics / Services	KIS SERVICE STATISTICS	KISSSTATS

See the *IBM Tivoli Monitoring User's Guide* for detailed information about historical data collection.

To confirm that historical data collection has been distributed to the agent, check the contents of the ISM agent operations log:

- For UNIX and Linux systems, *ITM_HOME*/logs/*hostname*_IS.LG0
- For Windows systems, *ITM_HOME*\tmaitm6\logs*hostname*_IS.LG0

For each attribute group configured and distributed, the UADVISOR entries are similar to the following excerpt:

```
1150225121949875KRAIRA000 Starting Enterprise situation UADVISOR_KIS_KISICMP
<2972714144,831522646> for KIS.KISICMP
1150225121949906KRAIRA000 Starting Enterprise situation UADVISOR_KIS_KISHTTP
<2972714319,831522581> for KIS.KISHTTP
1150225125209375KRAIRA000 Starting Enterprise situation UADVISOR_KIS_KISHSTATS
<3270511205,858785474> for KIS.KISHSTATS.
1150225125210390KRAIRA000 Starting Enterprise situation UADVISOR_KIS_KISMSTATS
<273680449,917505731> for KIS.KISMSTATS
1150225125211375KRAIRA000 Starting Enterprise situation UADVISOR_KIS_KISSSTATS
<2865758970,844105408> for KIS.KISSSTATS
1150225130212422KRAIRA000 Starting Enterprise situation UADVISOR_KIS_KISSISTATS
<930089818,900728511> for KIS.KISSISTATS
```

Binary history files

Binary history files are created for each historical data collection attribute. The Warehouse Proxy Agent and the Summarization and Pruning Agent work together to collect and process historical data.

The Warehouse Proxy Agent reads data from binary history files that are collected at the Tivoli Enterprise Monitoring Server or the Tivoli Enterprise Management Agent. These files are sometimes referred to as short-term history files. Either the Warehouse Proxy Agent or the Tivoli Enterprise Management Agent inserts this data into tables in the Tivoli Data Warehouse. If the data is more than 24 hours old and has been successfully inserted into the Tivoli Data Warehouse, the data is removed from the binary history files.

If the insert operation fails, the binary history file continues to grow. Setting the Warehouse Interval to OFF in the History Collection Configuration panel for an attribute group has the same effect: data in the binary history file is not added to the Tivoli Data Warehouse, and the size of the binary history file continues to grow. If the Tivoli Enterprise Management Agent was moving the binary files into the Tivoli Data Warehouse, log messages written in the agents' logs.

The Summarization and Pruning agent creates summarized data from the data available in the Tivoli Data Warehouse. This agent adds the data to tables in the Tivoli Data Warehouse that are named for the active Historical Data Collection attribute groups, and reflects the summarization period. For example, Daily summarized data for RRT Transaction Over Time data is stored in the RRT_Transaction_Over_Time_D table.

The Summarization and Pruning agent deletes records in the Tivoli Data Warehouse tables according to the pruning interval configured for those attribute groups. The summarization and pruning intervals should match to ensure that one table does not continuously grow.

Tip: The Summarization and Pruning agent does not recover database space. The database administrator needs to run a recovery operation to compact the database.

Binary history files

A unique pair of binary history files is created for each historical data collection attribute: a data file, and a header file. The data file and the header file share the same filename and the header filename includes a `.HDR` extension and are saved to the same directory. The files may have different timestamps because the header file timestamp is only updated at agent startup.

Binary history filenames

Table 28 on page 122 lists the binary history filenames for each attribute group.

Table 28. Binary history filenames for Attribute Groups

Agent	Attribute Group	Binary history filename
Application Management Console	ERT Agent Messages	T3AGNTMSGS
	AMC Agent	T3SNAGENT
	AMC Application	T3SNAPPL
	AMC Client	T3SNCLIENT
	AMC Client Agents	T3SNCLTAGT
	AMC Server	T3SNSERVER
	AMC Server Agents	T3SNSVRAGT
	AMC Transaction	T3SNTRANS

Location of binary history files

Binary history files collected at the Tivoli Enterprise Management Agent are saved to the following directories:

- On Windows systems, `CANDLE_HOME\TMAITM6\logs`
- On Linux and UNIX systems, `CANDLE_HOME/`*`architecture`*`/`*`product-code`*`/hist`

For example, `/opt/IBM/ITM/aix523/t6/hist`

A log entry is created each time an agent starts. This log indicates which situations and historical data collection attributes have started and stopped on the agent. The filename and location are platform-specific:

- On Windows systems, `CANDLE_HOME\TMAITM6\logs\`*`hostname_product-code`*`.LG0`
- On Linux and UNIX systems, `CANDLE_HOME/logs/`*`hostname`*`:`*`product-code`*`.LG0`

In the log file, UADVISOR messages indicate that historical data collection is starting or stopping for a specific attribute. For example, the following UADVISOR message indicates that historical data collection has started for the Robotic Response Time attribute T6APPOT (RRT Application Over Time):

```
1090717181915344KRAIRA000 Starting UADVISOR_KT6_T6APPOT <711983735,3482322845>
for KT6.T6APPOT.
```

Appendix F. Regular expression syntax in Internet Service Monitoring

Regular expressions perform string matching on content downloaded during service tests. These expressions may contain one or more regular expression operators, which determine what content is matched by the expression.

Note: Regular expression syntax can be used to match strings on single lines only. Internet Service Monitoring cannot match strings which include new lines or carriage returns. Use multiple regular expressions to match strings which cover multiple lines. You can also use SLC rules to raise alarms based on the result of multiple regular expressions.

Table 29. Regular expression operators

Character	Description
`.`	Matches any single character. For example the regular expression `r.t` matches the strings `rat`, `rut`, `r t`, but not `root`.
`$`	Matches the end of a line. For example, the regular expression `dog$` matches the end of the string `it's a dog` but not the string `There are a lot of dogs`.
`^`	Matches the beginning of a line. For example, the regular expression `^When in` matches the beginning of the string `When in the course of human events` but would not match `What and When in the`.
`*`	Matches zero or more occurrences of the character immediately preceding. For example, the regular expression `.*` matches any number of any characters.
`\`	Treats the subsequent character as an ordinary character. For example, `\$` matches the dollar sign character ($) rather than the end of a line. Similarly, the expression `\.` matches the period character rather than any single character.
`[]`	Matches any one of the characters between the brackets. For example, the regular expression `r[aou]t` matches `rat`, `rot`, and `rut`, but not `rit`. Specify ranges of characters by using a hyphen. For example, the regular expression `[0-9]` matches any digit. You can also specify multiple ranges. For example, the regular expression `[A-Za-z]` matches any upper or lower case letter.
`|`	Matches phrases containing either of the conditions specified. For example `him|her` matches the line `it belongs to him` and the line `it belongs to her`, but does not match the line `it belongs to them`.

Appendix G. Summary of RFCs

The protocols underlying many of the Internet services that you can monitor with Internet Service Monitoring are formally defined in Internet Engineering Task Force (IETF) Request For Comment (RFC) documents.

Table 30 on page 125 lists the RFCs relevant to the services that Internet Service Monitoring monitors.

Table 30. Monitors and RFCs

Monitor	**RFC**
DHCP	2131
DNS	1034, 1035
FTP	959, 1123, 1639, 2228, 2389, 2428, 2577, 2640
HTTP	1945 (HTTP 1.0), 2616 (HTTP 1.1)
HTTPS	2660
ICMP	792, 2598 (Jitter)
IMAP4	2060
LDAP	2251, 2252, 2253, 2254, 2255, 2256
NNTP	977
NTP	1305
POP3	1939
RADIUS	2865, 2868
RPING	2925
RTSP	2326
SAA	not applicable
SIP	3261
SMTP	821, 1869
SNMP	1157
SOAP	not applicable
TCP PORT	793
TFTP	1350, 1785, 2090, 2347, 2348, 2349, 3617

Table 30. Monitors and RFCs (continued)	
Monitor	**RFC**
TRANSX	not applicable

RFCs are available on the Internet.

Notices

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

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785 U.S.A.

For license inquiries regarding double-byte (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan Ltd.
19-21, Nihonbashi-Hakozakicho, Chuo-ku
Tokyo 103-8510, Japan

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law:

INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement might not apply to you.

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

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

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

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

IBM Corporation
2Z4A/101
11400 Burnet Road
Austin, TX 78758 U.S.A.

Such information may be available, subject to appropriate terms and conditions, including in some cases payment of a fee.

The licensed program described in this document and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement or any equivalent agreement between us.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurement may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

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

All statements regarding IBM's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

All IBM prices shown are IBM's suggested retail prices, are current and are subject to change without notice. Dealer prices may vary.

This information is for planning purposes only. The information herein is subject to change before the products described become available.

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. You may copy, modify, and distribute these sample programs in any form without payment to IBM for the purposes of developing, using, marketing, or distributing application programs conforming to IBM‘s application programming interfaces.

Each copy or any portion of these sample programs or any derivative work, must include a copyright notice as follows:

© IBM 2009. Portions of this code are derived from IBM Corp. Sample Programs. © Copyright IBM Corp. 2009. All rights reserved.

If you are viewing this information in softcopy form, the photographs and color illustrations might not be displayed.

Trademarks

IBM, the IBM logo, and ibm.com® are trademarks or registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the web at Copyright and trademark information (www.ibm.com/legal/copytrade.shtml).

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

Java and all Java-based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates.

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

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

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

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

Privacy policy considerations

IBM Software products, including software as a service solutions, ("Software Offerings") may use cookies or other technologies to collect product usage information, to help improve the end user experience, to tailor interactions with the end user or for other purposes. In many cases no personally identifiable information is collected by the Software Offerings. Some of our Software Offerings can help enable you to collect personally identifiable information. If this Software Offering uses cookies to collect personally identifiable information, specific information about this offering's use of cookies is set forth below.

Depending upon the configurations deployed, this Software Offering may use session cookies that collect each user's user name for purposes of session management, authentication, and single sign-on configuration. These cookies cannot be disabled.

If the configurations deployed for this Software Offering provide you as customer the ability to collect personally identifiable information from end users via cookies and other technologies, you should seek your own legal advice about any laws applicable to such data collection, including any requirements for notice and consent.

For more information about the use of various technologies, including cookies, for these purposes, See IBM's Privacy Policy at http://www.ibm.com/privacy and IBM's Online Privacy Statement at http://www.ibm.com/privacy/details the section entitled "Cookies, Web Beacons and Other Technologies" and the "IBM Software Products and Software-as-a-Service Privacy Statement" at http://www.ibm.com/software/info/product-privacy.

Index

H

I

L

M

N

O

P

R

S

T

U

W

X

0000-0000-00