IBM Tivoli Composite Application Manager for Transactions
V7.4.0.1
for AIX, Linux, Solaris, and Windows

Guide to agentless transaction tracking

SC27-4377-02

Note
Before using this information and the product it supports, read the information in "Notices" on page 73.

This edition applies to V7.4 of IBM Tivoli Composite Application Manager for Transactions (product number 5724-S79) and to all subsequent releases and modifications until otherwise indicated in new editions.

Contents

Figures

Tables

About this publication

This guide describes how to install, configure, and use the agentless transaction tracking feature of ITCAM for Transactions (available in version 7.3 and later). Using agentless transaction tracking, you can install a minimal number of ITCAM for Transactions components and quickly view a topology of your IBM Tivoli Monitoring environment. With a combination of the topology and hotspots, you can start to identify problem areas in your environment.

Intended audience

This guide is for administrators who want a quick overview of their environment and identify problem areas. With this information, you can implement additional agent-based components to improve the monitoring of your environment.

You should be familiar with the following topics:

- IBM Tivoli Monitoring product
- Tivoli Enterprise Portal interface
- IBM application software

Publications

This section lists publications relevant to the use of the IBM Tivoli Composite Application Manager for Transactions. It also describes how to access Tivoli® publications online and how to order Tivoli publications.

Documentation library

The following documents are available in the IBM Tivoli Composite Application Manager for Transactions library:

- *IBM Tivoli Composite Application Manager for Transactions Administrator's Guide*

  This guide provides information about configuring elements of IBM Tivoli Composite Application Manager for Transactions.
- *IBM Tivoli Composite Application Manager for Transactions Installation and Configuration Guide*

  This guide provides information about installing and configuring elements of IBM Tivoli Composite Application Manager for Transactions.
- *IBM Tivoli Composite Application Manager for Transactions Quick Start Guide*

  This guide provides a brief overview of IBM Tivoli Composite Application Manager for Transactions.
- *IBM Tivoli Composite Application Manager for Transactions Troubleshooting Guide*

  This guide provides information about using all elements of IBM Tivoli Composite Application Manager for Transactions.
- *IBM Tivoli Composite Application Manager for Transactions SDK Guide*

  This guide provides information about the Transaction Tracking API.
- *IBM Tivoli Composite Application Manager for Transactions User's Guide*

  This guide provides information about the GUI for all elements of IBM Tivoli Composite Application Manager for Transactions.

- *IBM Tivoli Composite Application Manager for Transactions Installation and Configuration Guide for z/OS*

  This guide provides information about using IBM Tivoli Composite Application Manager for Transactions on z/OS.

Prerequisite publications

To use the information in this guide effectively, you must know about IBM Tivoli Monitoring products that you can obtain from the following documentation:

- *IBM Tivoli Monitoring Administrator's Guide*
- *IBM Tivoli Monitoring Installation and Setup Guide*
- *IBM Tivoli Monitoring User's Guide*

If you do not have IBM Tivoli Monitoring installed already you can do a basic IBM Tivoli Monitoring installation using the IBM Tivoli Monitoring Quick Start Guide as a guide.

See IBM Tivoli Monitoring Information Center for further information.

Accessing terminology online

The IBM® Terminology website consolidates the terminology from IBM product libraries in one convenient location.

You can access the Terminology website at the following web address:

http://www.ibm.com/software/globalization/terminology

Accessing publications online

IBM posts publications for all products, as they become available and whenever they are updated, to IBM Knowledge Center.

Access IBM Knowledge Center (http://www.ibm.com/support/knowledgecenter) using a browser.

Find supporting information on the Application Performance Management community (http://www.ibm.com/developerworks/servicemanagement/apm/index.html) and connect, learn, and share with experts.

Ordering publications

You can order many Tivoli publications online at the following website:

http://www.ibm.com/e-business/linkweb/publications/servlet/pbi.wss

You can also order by telephone by calling one of these numbers:

- In the United States: 800-879-2755
- In Canada: 800-426-4968

In other countries, contact your software account representative to order Tivoli publications. To locate the telephone number of your local representative:

1. Go to http://www.ibm.com/planetwide/.
2. In the alphabetic list, select the letter for your country and then click the name of your country. A list of numbers for your local representatives is displayed.

Accessibility

Accessibility features help users with a physical disability, such as restricted mobility or limited vision, to use software products. With this product, you can use assistive technologies to hear and navigate the interface. You can also use the keyboard instead of the mouse to operate most features of the graphical user interface.

For additional information, see Accessibility.

Tivoli technical training

For information about Tivoli technical training, see the following IBM Tivoli Education website:

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

Support information

If you have a problem with your IBM software, you want to resolve it quickly.

Online

Access the Tivoli Software Support site at http://www.ibm.com/software/sysmgmt/products/support/index.html?ibmprd=tivman. Access the IBM Software Support site at http://www.ibm.com/software/support/probsub.html .

IBM Support Assistant

The IBM Support Assistant is a free local software serviceability workbench that helps you resolve questions and problems with IBM software products. The Support Assistant provides quick access to support-related information and serviceability tools for problem determination. The IBM Support Assistant provides the following tools to help you collect the required information:

- Use the IBM Support Assistant Lite program to deploy the IBM Support Assistant data collection tool. This tool collects diagnostic files for your product.

  Tip: When you install the IBM Support Assistant data collection tool on 64-bit systems, use a 32-bit Java Runtime Environment to ensure that data collection functions as expected.
- Use the Log Analyzer tool to combine log files from multiple products in to a single view and simplify searches for information about known problems.

For information about installing the IBM Support Assistant software, see http://www.ibm.com/software/support/isa.

Troubleshooting Guide

For more information about resolving problems, see the *IBM Tivoli Composite Application Manager for Transactions Troubleshooting Guide*.

Conventions used in this guide

This guide uses several conventions for operating system-dependent commands and paths, special terms, actions, and user interface controls.

Typeface conventions

This guide uses the following typeface conventions:

Bold

- Lowercase commands and mixed case commands that are otherwise difficult to distinguish from surrounding text
- Interface controls (check boxes, push buttons, radio buttons, spin buttons, fields, folders, icons, list boxes, items inside list boxes, multicolumn lists, containers, menu choices, menu names, tabs, property sheets), labels (such as **Tip**, and **Operating system considerations**).
- Keywords and parameters in text

Italic

- Words defined in text
- Emphasis of words
- New terms in text (except in a definition list)
- Variables and values you must provide

`Monospace`

- Examples and code examples
- File names, programming keywords, and other elements that are difficult to distinguish from surrounding text
- Message text and prompts addressed to the user
- Text that the user must type
- Values for arguments or command options

Operating system-dependent variables and paths

This guide uses the UNIX system convention for specifying environment variables and for directory notation.

When using the Windows command line, replace **$***variable* with **%***variable***%** for environment variables. Replace each forward slash (**/**) with a backslash (\) in directory paths. The names of environment variables are not always the same in the Windows and UNIX environments. For example, %TEMP% in Windows environments is equivalent to $TMPDIR in UNIX environments.

Note: If you are using the bash shell on a Windows system, you can use the UNIX conventions.

Variables

The following variables are used in this documentation:

$CANDLE_HOME
The default IBM Tivoli Monitoring installation directory. On UNIX systems, the default directory is `/opt/IBM/ITM`.

%CANDLE_HOME%
The default IBM Tivoli Monitoring installation directory. On Windows systems, the default directory is `C:\IBM\ITM`.

$ALLUSERSPROFILE
On UNIX systems, `/usr`

%ALLUSERSPROFILE%
On Windows 7 and 2008, the default directory is `C:\ProgramData`.

Chapter 1. Introduction to agentless transaction tracking

ITCAM for Transactions version 7.3 and later provides *agentless transaction tracking*. With agentless transaction tracking, you can track transactions without the need for domain-specific or application-specific data collectors.

This type of monitoring extends the capabilities of existing ITCAM for Transactions features and functions in the following ways:

- Monitor generic TCP/IP based network flows.
- Visualize network flow data and dependencies using enhanced Tivoli Enterprise Portal workspaces.
- Visualize TCP-based application protocols and dependencies and the performance characteristics of those interactions.
- Create and modify configuration using additional capabilities in the Application Management Configuration Editor which enable you to monitor TCP/IP network-flow data.
- Combine data collected using agentless transaction tracking with data from existing domain-based data collectors, such as Data Collector for WebSphere Message Broker, to display monitored TCP/IP data in topology views.

Using these capabilities together, you can collect agentless transaction tracking data, display the resulting topology, and then successively deploy agent-based data collectors to obtain more detailed tracking information.

To implement agentless transaction tracking, you need to install and configure only the following ITCAM for Transactions components:

- Web Response Time (part of the Response Time component), which includes the capability to monitor the TCP/IP network-flow data.
- Transaction Reporter (part of the Transaction Tracking component), which takes the agentless data from Web Response Time, combines it with data from other agent-based data collectors if required, and displays the resulting topology. Transaction Tracking provides the topology workspaces that enable you to filter and display the information collected by agentless transaction tracking.

By installing and configuring only a minimal number of ITCAM for Transactions components, you can quickly view a topology of your IBM Tivoli Monitoring environment and start to identify problem areas.

Chapter 2. Installation overview for agentless transaction tracking

You can install agentless tracking in one of several ways.

To enable agentless transaction tracking the following components must be installed:

- Web Response Time, which functions as an aggregation agent for agentless transaction tracking.
- Transaction Reporter, which collects and stores the aggregated data from Web Response Time and sends the data to the Tivoli Enterprise Portal workspaces.

See the introductory information in the *Installation and Configuration Guide* and the rest of the product library for more information about these components and how they are used in ITCAM for Transactions.

Prerequisites

Be sure to read the planning information in the *Installation and Configuration Guide* before installing agentless transaction tracking. The information in this guide helps you understand how to set up an effective monitoring environment and incorporate ITCAM for Transactions into an existing IBM Tivoli Monitoring installation. Be sure to adhere to specific recommendations about deploying the Web Response Time and Transaction Reporter components into your environment.

See ITCAM for Transactions Prerequisites for additional information about operating system prerequisites and supported environments.

Consider installing the Application Management Console component. Although not a required prerequisite to display agent data, the Application Management Configuration Editor is required to configure all customizations such as transactions and filters. If the Application Management Console agent is not installed, the default profiles are used when capturing data.

You can install and upgrade ITCAM for Transactions components using the individual installers available for each component.

Installing agentless transaction tracking

As an alternative to using the ITCAM for Transactions installer to install agentless transaction tracking, you can use the individual installation programs for the Response Time and Transaction Tracking components to install the Web Response Time and Transaction Reporter subcomponents. This installation method is useful if you are installing agentless transaction tracking into an existing IBM Tivoli Monitoring environment.

Chapter 5 in the *Installation and Configuration Guide* describes the procedure for installing Response Time monitoring agents and related software, including Web Response Time. In the step-by-step procedure, at step 10 be sure to select the Web Response Time agent from the list of available Response Time agents.

Chapter 7 in the *Installation and Configuration Guide* describes the procedure for installing Transaction Tracking monitoring agents and related software, including Transaction Reporter.

Installing agentless transaction tracking silently

As an alternative to using the ITCAM for Transactions installer to install agentless transaction tracking, you can install the Web Response Time and Transaction Reporter subcomponents using the command-line installer. This installation method is useful if you are an Administrator installing agentless transaction tracking into an existing IBM Tivoli Monitoring environment on a UNIX system.

Chapter 5 in the *Installation and Configuration Guide* describes the procedure for installing Response Time monitoring agents and related software, including Web Response Time, using a silent response file. Modify the parameters in the response file to install the Web Response Time agent.

Chapter 7 in the *Installation and Configuration Guide* describes the procedure for installing Transaction Tracking monitoring agents and related software, including Transaction Reporter, using the silent installation method.

Installing agentless transaction tracking remotely

Chapter 10 in the *Installation and Configuration Guide* describes the procedure for deploying and configuring agents remotely. Follow these procedures to remotely deploy and configure the Web Response Time and Transaction Reporter subcomponents.

Chapter 3. Enabling agentless transaction tracking

To enable agentless transaction tracking, you must set TCP tracking and integrate Transaction Tracking with Web Response Time.

If you install agentless transaction tracking using the ITCAM for Transactions installer, TCP tracking is set and the components are integrated automatically.

If you install agentless transaction tracking using any other method, you must enable it.

Understanding Web Response Time transaction tracking and TCP tracking

The transaction tracking function of the Web Response Time monitoring agent was introduced in ITCAM for Transactions version 7.2.0.1. This function provides agent-based tracking that is correlated with other agent-based tracking data and displayed in the server, component, application, and transaction workspaces in the Transaction Reporter.

Using this function, you can see which HTTP and HTTPS applications and transactions are communicating with various other components in the monitored transaction flow. This tracking is based on individual transaction instances using Transaction Tracking API calls to the Transaction Tracking data collector. Using this instance-based data, you can examine tracking data and topologies for individual transaction instances.

The Web Response Time TCP tracking feature provided with ITCAM for Transactions V7.3 enables you to monitor the TCP interactions in your network environment. Using this function, you can quickly visualize the TCP-based application protocols and dependencies present in your IT infrastructure along with the performance characteristics of these interactions. Agentless transaction tracking provides more general tracking that is not based on individual transaction instances, but on aggregate data that is retrieved directly by the Transaction Reporter. This data is independent of the protocol over TCP which provides a broader range scope of interactions between computers. The data is not correlated directly to other agent-based data, but the agentless data can be displayed with (and linked to) other agent-based server data if the host and port information match.

This TCP tracking feature is not meant to replace the transaction tracking function, but to offer another method of tracking your transactions in the Web Response Time monitoring environment. If you are interested in application or transaction level tracking of your HTTP data, use the transaction tracking function. If you are looking for more generic TCP flow level tracking, use the TCP tracking feature.

How TCP tracking works

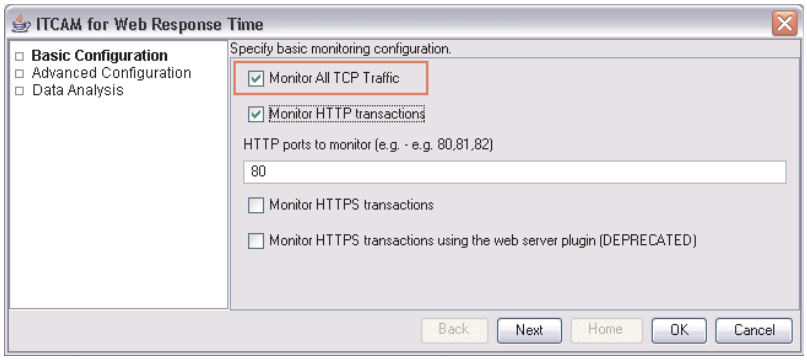
The collection of this TCP data occurs on the Web Response Time agent, and is disabled by default. After enabling the collection of TCP data on the Web Response Time agent, data is collected according to the filters and reporting properties of the *Component* definitions in the Application Management Configuration Editor.

Collected data can be viewed in a set of TCP-centric Tivoli Enterprise Portal workspaces, accessed from the Network node of the monitoring Web Response Time agent. The Transaction Reporter also includes consolidated workspaces for examining this TCP data, including topology views for displaying these TCP interactions across the entire set of Web Response Time agents in your environment.

Web Response Time agent configuration settings

Several agent configuration options are provided for the Web Response Time agent to enable and customize the way TCP data is collected and monitored:

- Enabling TCP Monitoring: To enable TCP monitoring on a Web Response Time agent, select the **Monitor All TCP Traffic** option in the agent configuration panel, as shown in the following example:



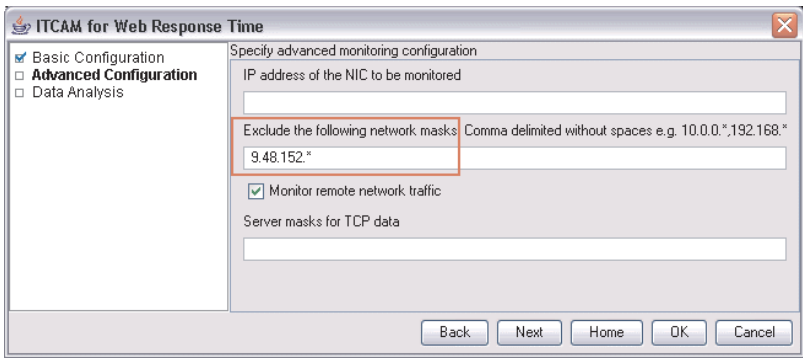
- Network Mask Exclusion: The **Advanced Configuration** portion of Web Response Time agent configuration includes an option for excluding TCP data from being monitored by the agent. Specify this exclusion with a list of IPv4 address mask entries for which TCP data is ignored. This exclusion occurs at the network traffic capture layer, so the exclusion list affects both TCP and HTTP data collection.

  There are two main reasons why you might want to use this network mask exclusion property:

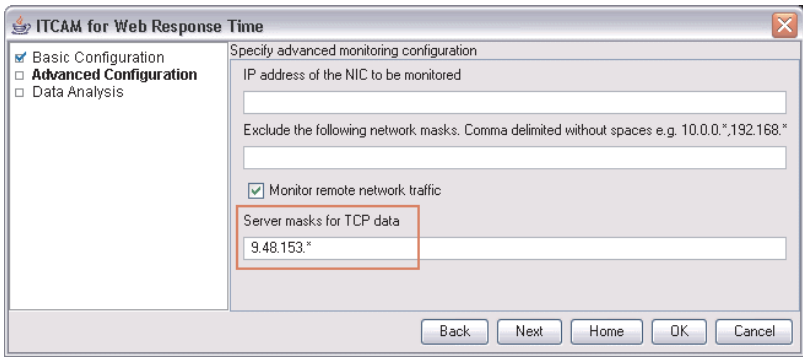
  – There might be a large amount of extraneous traffic visible on the device for which monitoring is not necessary, for example, when receiving packets from a switch with port spanning enabled. Large amounts of extra traffic can cause performance degradation in the agent processing. Excluding this data at the network level through the use of the exclusion mask setting prevents this unnecessary data from entering the processing flow of the agent.

  – You might need more than one Web Response Time agent to monitor all of the required TCP traffic in your environment. In this situation, if the same network data is visible on two different Web Response Time agents that are monitoring TCP traffic, use the exclude field to ensure that the duplicate traffic is only monitored once. For example, if one Web Response Time agent is monitoring TCP traffic on subnet 9.48.152.*, and another agent is monitoring traffic on 9.48.142.*, any traffic going between the 9.48.152.* and 9.48.142.* subnets is visible on both Web Response Time agents. However, if the agent on subnet 9.48.142.* uses the exclude mask `9.48.152.*`, the agent is prevented from monitoring the traffic between the two network segments, and monitoring of this traffic is the sole responsibility of the other Web Response Time agent.

  This configuration setting is shown in the following example:



- Monitoring remote network traffic: The options**Monitor Remote HTTP server** and **Monitor remote HTTPS server** available in previous releases have been replaced by the more generic **Monitor remote network traffic** option, as shown in the previous example. This option specifies that all traffic on the NIC can be monitored, regardless of the source and destination IP addresses. If you do not select this configuration option, only the traffic with the IP address of the NIC as the source or destination is monitored. This option is implemented at the packet capture layer of the product and affects the collection of TCP, HTTP, and HTTPS data.
- Specifying server masks: Specify an IP address or IP address mask in the **Server masks for TCP data** field to identify remote computers as servers. Those servers are then displayed as expected in the resulting TCP topology. If you do not identify servers, traffic associated with that server is bundled in a client group with other client traffic. Identify servers if two or more Web Response Time agents are being used to monitor and visualize a complete segment of a TCP topology. To recognize a computer in your monitored environment as an independent server, the Web Response Time agent must be able to see traffic coming into the server and recognize that traffic as belonging to the set for which monitoring has been enabled by the user. However, in an environment where there are two or more agents monitoring the traffic, one of the agents might be able to see only outbound traffic from a server on a different network segment. This configuration can result in multiple, disjoint TCP topologies being displayed in Tivoli Enterprise Portal workspaces, instead of one complete topology.



For more information about configuring the Web Response Time agent, see Chapter 6 in the *Installation and Configuration Guide*.

Application Management Configuration Editor settings

In ITCAM for Transactions V7.3 and later, the term *Component* is used to represent a process within the IT environment that accepts requests on one or more TCP ports on its host computer. The Application Management Configuration Editor includes the **Components** dialog, which you can use to define and customize component definitions that specify the way that TCP data is monitored and reported in ITCAM for Transactions. Many default component monitoring configurations are provided for common components such as HTTP Servers and LDAP Servers. You can use these defaults without further changes, customize them to reflect the TCP traffic in your environment, or create new component definitions for other TCP services of interest within your network environment.

The Application Management Configuration Editor includes the following settings for monitoring TCP traffic:

- Defining components: After selecting **Components** from the Application Management Configuration Editor navigation selection menu, you are presented with the current list of component definitions within the system. From here, you can create a new component definition or select an existing definition for modification. Because of complexities and possible overlap of the internal component configuration, the **Create Another Component** function is disabled within the Components dialog box. If you create a new component, you are directed to the **Create Component** definition panel, where you can name and the component (for example, `IBM HTTP Server`), and provide a text description.
- Defining component protocols: After selecting or defining your component definition, you select the **Protocols** tab to specify the different protocols that are used by the monitoring component. This dialog box shows the list of protocols for the component, each consisting of a name, an IP address mask representing the computers using the protocol, and a list of TCP ports used by the protocol. Use this dialog box to create, delete, or modify existing protocols. When adding or editing a protocol, you are presented with a dialog box to enter or modify the properties for each defined protocol:

  Name The display name of the protocol used in the Web Response Time agent workspaces, and in the transaction tracking TCP topology. You can enter this name directly or select an existing name from a list. Selecting an existing name does not populate **IP Address** or **Ports** fields.

  IP Address
  An IP address or IP address mask that defines one or more computers that are hosting the protocol. Wildcard characters are accepted, including asterisk (*).

  Ports A comma-separated list that defines the TCP ports used by this protocol.
- Defining reporting properties: As part of defining your component, you select the **Reporting** tab to modify the Application Management Configuration Editor reporting properties associated with the component. Use this dialog to edit the component name and server name that is displayed in the Web Response Time workspaces and the Transaction Tracking topology views. Similar to other Application Management Configuration Editor reporting properties, there are multiple TCP properties that you can use in these definitions (for example, the default server reporting name `$ShortHost$`, which resolves to the short DNS host name for the server that runs the component).

See Creating a component for more information about creating components, protocols, and reporting options for monitoring TCP traffic.

Web Response Time workspaces for TCP monitoring

The Web Response Time agent provides various workspaces for viewing collected TCP data. These workspaces provide many different contexts of monitored TCP data, from client and server level to network component and protocol level. By navigating these multiple levels of TCP traffic in the workspaces, you can identify TCP performance characteristics and possible bottlenecks in your network environment.

The following workspaces are included in ITCAM for Transactions to view TCP monitoring data:

- "Components" on page 19 workspace
- "Component Details" on page 21 workspace
- "Component Server Details" on page 26 workspace
- Server Dependencies workspace
- Client Dependencies workspace
- "Component History" on page 24 workspace
- Client Facing Components workspace

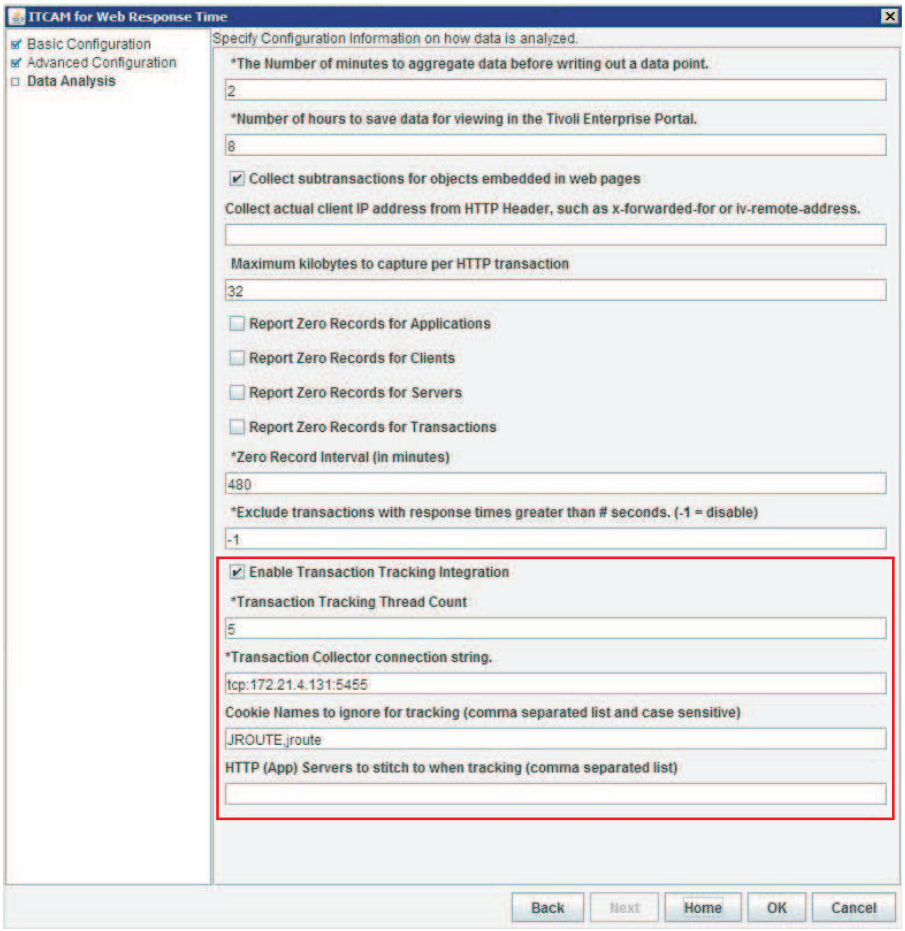
These workspaces are described in the *User's Guide*.

Enabling Transaction Tracking integration

To help you isolate problems in your monitoring environment, such as with WebSphere, and so on, enable transaction tracking to make Transaction Tracking API calls so that you can view Web Response Time topology information at a lower level.

By default, the Web Response Time agent does not make transaction tracking calls. Use the following procedure to enable Transaction Tracking integration:

1. In the **Manage Tivoli Enterprise Monitoring Services** window, right-click the Web Response Time agent and select **Reconfigure**.
2. Step through the configuration windows until you reach the **Data Analysis** window.



3. Select **Enable Transaction Tracking Integration** to cause the Web Response Time agent to send its data to the Transaction Collector agent using generated Transaction Tracking API events for transaction tracking integration. Accept the additional default values that are displayed, or specify your own values for the following parameters:
   - Transaction Tracking Thread Count (default is *5*)

     The **Transaction Tracking Thread Count** field is for performance tuning, and usually should not be changed from its default value of *5*. Consult your system administrator or see the IBM Software Support website for further information.
   - Transaction Collector connection string
   - A comma separated, case-sensitive string of cookie names to ignore during tracking

   Note: You cannot enable transaction tracking integration if local HTTPS (plugin mode) is enabled. The Web Response Time agent cannot obtain the necessary tracking information from transactions monitored by the HTTPS plugin in local mode.

   In local mode and appliance mode, the Web Response Time agent typically does not observe traffic between processes on the same machine, because this traffic goes through the loopback device and is not broadcast on the Network Interface Card (NIC). For example, to display stitching between IBM HTTP Server and WebSphere Application Server in a topology display, IBM HTTP Server and WebSphere Application Server must reside on separate computers in

order for Web Response Time to track the two processes. When IBM HTTP Server and WebSphere Application Server reside on the same computer, Web Response Time cannot see network traffic that is occurring when the two processes communicate with each other over sockets on the same physical computer, because the operating system never puts the traffic on the NIC. Typically, the traffic is sent between these processes using shared memory.

4. Click **OK**.

In the agent logging configuration, if you add `ERROR (UNIT:analyzer FLOW)` you can see enhanced logging for the topology in the Web Response Time log files. This log information includes metrics to help you isolate performance problems in the Web Response Time agent.

If the topology display shows the browser node connected to multiple pieces of the application (for example, the IBM HTTP Server, WebSphere Application Server, and TAM nodes) the Web Response Time agent was unable to collect the data for the first node (for example, TAM), and assumes the edge is against the next node (for example, IBM HTTP Server).

Chapter 4. Displaying information from agentless transaction tracking

Data collected by agentless transaction tracking is displayed in the Transaction Reporter and Web Response Time workspaces in the Tivoli Enterprise Portal.

Use the Transaction Reporter Transactions Overview workspace to view a topology of your enterprise derived from agentless transaction tracking data. Use the hotspots displayed in the topology to help you isolate problems.

Use the Web Response Time Network workspaces to display details about the TCP tracking data collected by agentless transaction tracking.

Transactions Overview

The Transactions Overview workspace combines metric information derived from TCP traffic by the Web Response Time agent (agentless transaction tracking), and agent-based data derived from data collector plug-ins into a single topology and interactions table.

Use the agentless transaction tracking approach to detect protocols and components. Add agent-based Transaction Tracking data collector plug-ins at those points where you need further information to help resolve problems.

Enabling agentless data in this workspace

See “Enabling this workspace” on page 16 for information about enabling agentless transaction tracking data in this workspace.

Using this workspace

The **Transactions Overview** workspace contains the following views in addition to the standard **Navigator** view:

- **Server Component Topology** - displays nodes detected by both agentless and agent-based tracking
- **Deviations** table - displays metrics for the links displayed in the topology detected by both agentless transaction tracking and agent-based tracking

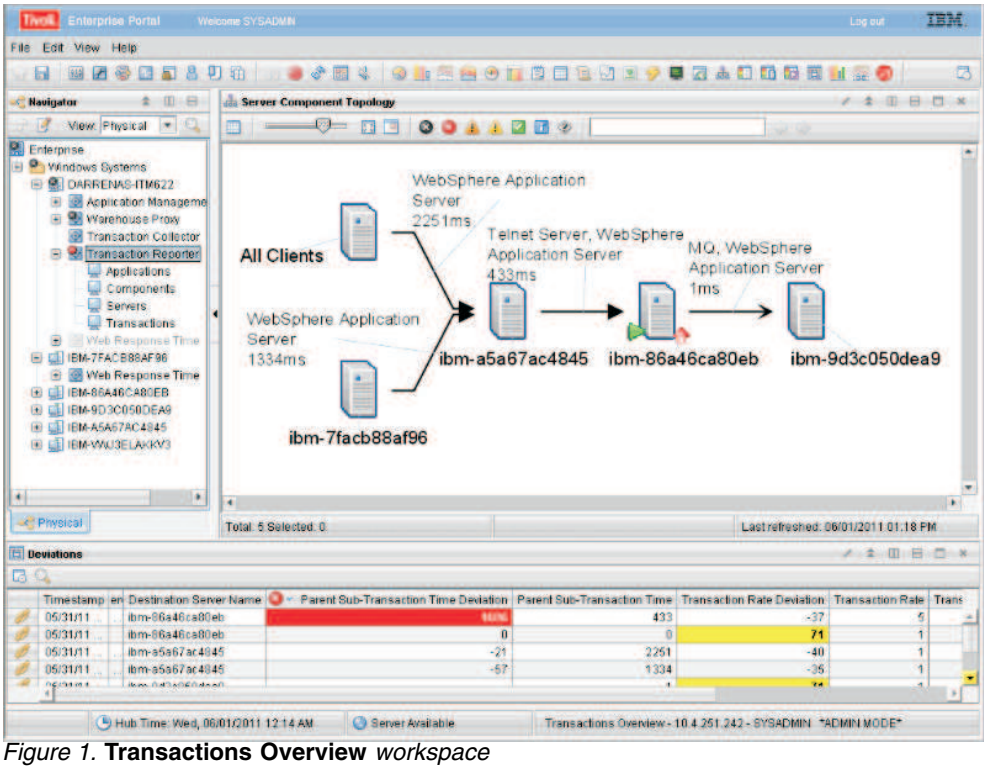


Figure 1. **Transactions Overview** *workspace*

Server information is displayed in a tooltip when you hover the mouse over a node. If the node represents a source server in all detected interactions, the tooltip displays only the Server name. Otherwise, the tooltip displays the Server name and if this information is available, the Parent Sub-Transaction Time, Baseline, and Deviation.

Component information is displayed on the links in the topology. Links between nodes display the Parent Sub-Transaction Time in milliseconds.

Tip: If you require more information about a particular node and it was detected using the agentless transaction tracking method, consider installing an agent-based data collector for that node. You can then use the Applications, Components, Servers, and Transactions workspaces to access detailed information.

Use the Deviations table to view information about servers or components on your network detected using either Web Response Time (agentless transaction tracking) or data collector plug-ins (agent-based). Table 1 describes the columns in this table.

Table 1. Deviations table

Column	Description
Timestamp	Local time when the data was collected.
Source Server Name	Name of the server that originated the transaction or TCP traffic. The name is either that of the client group configured in the Application Management Configuration Editor, or if the server has already been identified as a destination, that host name is used.
Destination Server Name	Host name of the server to which the transaction or TCP traffic is flowing.

Table 1. Deviations table (continued)

Column	Description
Parent Sub-Transaction Time Deviation	Percentage deviation of the Parent Sub-Transaction Time from the baseline.
Parent Sub-Transaction Time	Average subtransaction time, in milliseconds, of transactions in the destination aggregate as seen from transactions in the source aggregate. Also known as the Average Response Time.
Transaction Rate	Average number of transactions per minute for transactions that make up the aggregate.
Transaction Rate Deviation	Percentage deviation of the Transaction Rate from the baseline.
Transaction Count	For TCP traffic, the number of request/reply transactions during the aggregate interval.
Failed Percent	Percentage of transaction instances that failed.
Slow Percent	Percentage of transaction instances that were slow.
Good Percent	Percentage of transaction instances that were good.

Note: Metrics are only displayed if there is traffic related to those metrics.

Tip: Set thresholds in the Properties window on the **Thresholds** tab to highlight values in the table for times or deviations that are outside the required performance parameters for your system.

Accessing this workspace

To access this workspace, select **Transaction Reporter** in the **Navigator** view.

Links to other workspaces

From the topology, right-click on a node or link and select **Link to** to link to the following workspaces:

- For nodes detected by Web Response Time (agentless):
  - **Client Dependencies** workspace (**Web Response Time** > **Network** > **Workspace** > **Client Dependencies**)
  - **Server Dependencies** workspace (**Web Response Time** > **Network** > **Workspace** > **Server Dependencies**)
- For links detected by Web Response Time (agentless), **Component Server Details** workspace (**Web Response Time** > **Network** > **Workspace** > **Component Server Details**).

  If you link to **Component Server Details** from a link between nodes which represents multiple components, a row is displayed for each protocol of each component in the **Protocol Breakdown** table of the **Component Server Details** workspace. If the link between nodes represents only a single component, only the protocols observed for that component are shown in the **Protocol Breakdown** table. Similarly, if the links are expanded (see Displaying multiple links between nodes) only the protocols for the component on the selected link are shown in the **Protocol Breakdown** table.
- For nodes detected by Transaction Tracking data collector plug-ins, **Servers** (**Transaction Reporter** > **Servers**).

From the Deviations table, select the link icon:

- For data detected by Web Response Time, link to **Component Server Details** workspace (**Web Response Time** > **Network** > **Workspace** > **Component Server Details**).
- For data detected by Transaction Tracking data collector plug-ins, link to **Servers** workspace (**Transaction Reporter** > **Servers**).

Agentless Data

The Agentless Data workspace displays topology and metric information derived from TCP traffic on the network monitored by the Web Response Time agent. You can customize the way in which this data is displayed in the workspace.

Enabling this workspace

To enable the display of agentless transaction tracking data in Transaction Tracking workspaces, you must configure the Web Response Time (T5) agent to monitor TCP traffic.

To enable monitoring of TCP data:

1. In the Manage Tivoli Enterprise Monitoring Services, right-click Web Response Time and select **Configure**.
2. On the Basic Configuration window, select **Monitor All TCP data**.
3. On the Advanced Configuration window, ensure that **Monitor remote network traffic** is selected.
4. Click **OK**.

The TCP data is displayed in the Web Response Time, **Network** workspaces (see Component for more information about the default workspace displayed from the Network node along with additional workspaces that display TCP data) and is interpreted by Transaction Tracking for display in the Transactions Overview and Agentless Data workspaces. The Transaction Reporter uses standard IBM Tivoli Monitoring ports to query the Web Response Time agents.

Using this workspace

The **Agentless** workspace contains the following views in addition to the standard **Navigator** view:

- **Network Topology** - displays server interactions detected using agentless tracking, including details about servers and components
- **Network Interactions** table - displays metrics for server interactions

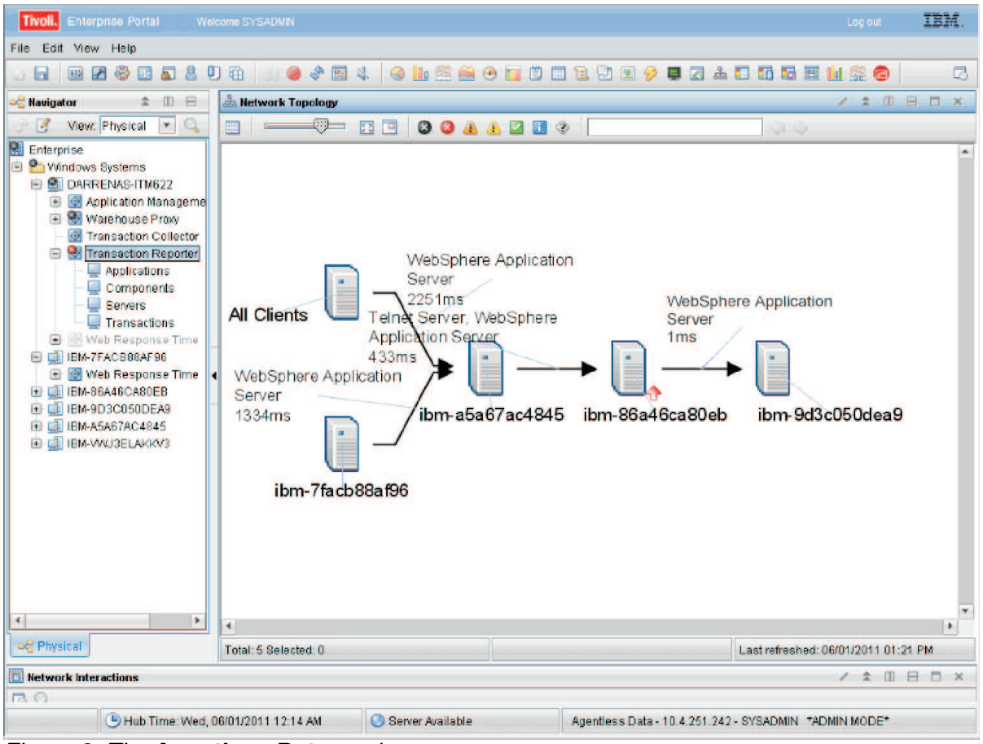


Figure 2. The **Agentless Data** *workspace*

Server information is displayed in a tooltip when you hover the mouse over a node. If the node represents a source server in all detected interactions, the tooltip displays only the Server name. Otherwise, the tooltip displays the Server name and if this information is available, the Parent Sub-Transaction Time, Baseline, and Deviation.

Links between nodes display component information and the Parent Sub-Transaction Time in milliseconds.

Use the Network Interactions table to view information about interactions between the nodes on your network. The following table describes the fields in this table.

Table 2. Network Interactions table

Column	Description
Timestamp	Local time when the data was collected.
Source Server Name	Name of the server that originated the TCP traffic. The name is either that of the client group configured in the Application Management Configuration Editor, or if the server has already been identified as a destination, that host name may be used.
Destination Server Name	Host name of the server to which the TCP traffic is flowing.
Parent Sub-Transaction Time	Average sub-transaction time, in milliseconds, of transactions in the destination aggregate as seen from transactions in the source aggregate. Also known as the Average Response Time.
Parent Sub-Transaction Time Deviation	Percentage deviation of the Parent Sub-Transaction Time from the baseline.

Table 2. Network Interactions table (continued)

Column	Description
Child Response Time	For TCP traffic, the average of the time, in milliseconds, between the last request packet and the first reply packet in a TCP transaction. Also known as the Average Server Time.
Child Response Time Deviation	Percentage deviation of the Child Response Time from the baseline.
Average Network Time	For TCP traffic, the average in milliseconds of the time between the last request packet and the first request packet, plus the time between the first reply packet and the last reply packet in a TCP transaction.
Average Network Time Deviation	Percentage deviation of the Average Network Time from the baseline.
Transaction Count	For TCP traffic, the number of request/reply transactions during the aggregate interval.

Note: Metrics are only displayed if there is traffic related to those metrics.

Tip: Set thresholds in the Properties window on the **Thresholds** tab to highlight values in the table for times or deviations that are outside the required performance parameters for your system.

Accessing this workspace

To access this workspace, right-click **Transaction Reporter** and select **Workspace** > **Agentless Data** in the **Navigator** view.

Links to other workspaces

From the topology, right-click on a node or link and select **Link to** to link to the following workspaces:

- For nodes detected by Web Response Time (agentless):
  - **Client Dependencies** workspace (**Web Response Time** > **Network** > **Workspace** > **Client Dependencies**)
  - **Server Dependencies** workspace (**Web Response Time** > **Network** > **Workspace** > **Server Dependencies**)
- For links detected by Web Response Time (agentless), **Component Server Details** workspace (**Web Response Time** > **Network** > **Workspace** > **Component Server Details**).

  If you link to **Component Server Details** from a link between nodes which represents multiple components, a row is displayed for each protocol of each component in the **Protocol Breakdown** table of the **Component Server Details** workspace. If the link between nodes represents only a single component, only the protocols observed for that component are shown in the **Protocol Breakdown** table. Similarly, if the links are expanded (see Displaying multiple links between nodes) only the protocols for the component on the selected link are shown in the **Protocol Breakdown** table.

From the Network Interactions table, select the link icon and link to **Component Server Details** workspace (**Web Response Time** > **Network** > **Workspace** >

Component Server Details).

Components

This workspace provides a summary overview of TCP tracking data collected by the agentless transaction tracking feature for all components.

This workspace is the default workspace displayed from the Network node in the Navigator view, and is a companion to the Client Facing Components workspace. The Components workspace provides an aggregated view of many TCP-centric metrics at the component level. Some of these metrics include response times, bandwidth statistics, and connection information. The data in this workspace provides an overall view of the TCP characteristics of Components across the entire environment. To view more detailed server and protocol level detail of the component, use the "Component Details" on page 21 link in the All Components table.

This workspace displays summary graphs for the following metrics:

- Historical trend of latency time
- Historical trend of average response time
- Real time send and receive bandwidth, in kilobytes
- Real time number of connections

In addition to the chart views, this workspace also includes a table view showing detailed data aggregated by component for all network flows.

This workspace displays a set of bar charts or line graphs in each view, similar to the following example.

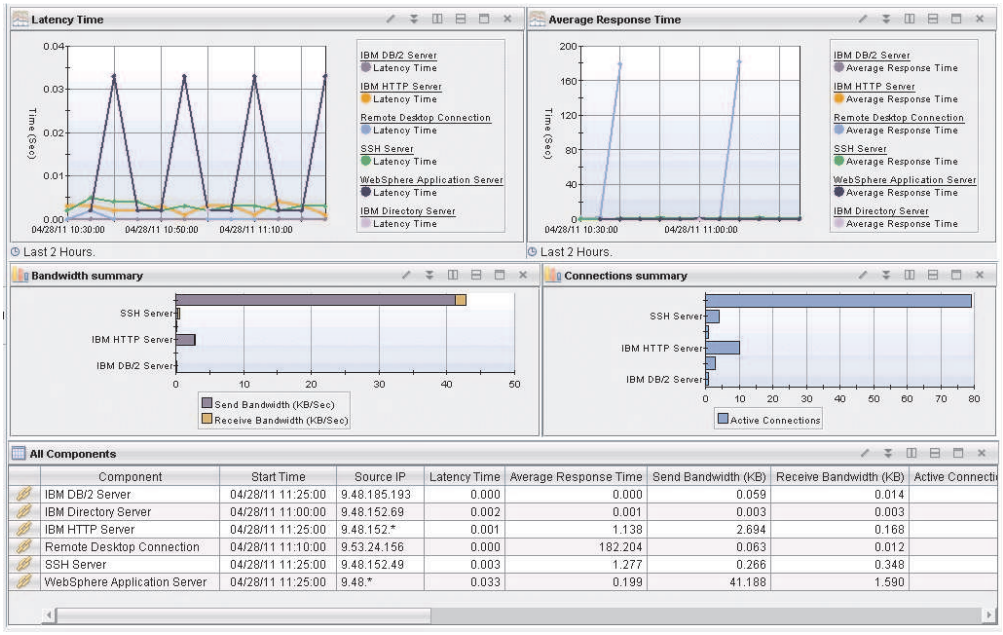


Figure 3. Components workspace

This workspace has the following views:

Latency Time

This view displays a multiple-line graph (one line per component) that

shows the historic trend of latency time, in seconds, for each component over the specified time interval (default is the last 8 hours). Latency is a measure of the time it takes a client to get a 0-byte TCP response after sending a 0-byte TCP request packet. This latency measurement typically occurs during the first two steps of the TCP handshake process.

Average Response Time
This view displays a multiple-line graph (one line per component) that shows the historic trend of average response time, in seconds, for each component over the specified time interval (default is the last 8 hours).

Bandwidth Summary
This view displays a bar chart that shows the send and receive bandwidth, in kilobytes per second, for each monitored component (such as IBM HTTP Server, WebSphere Application Server, IBM DB2 Server, and others). Each bar shows the total send bandwidth and total receive bandwidth during the monitoring interval for each unique component.

Connections Summary
This view displays a bar chart that shows the number of connections for each monitored component (such as IBM HTTP Server, WebSphere Application Server, IBM DB2 Server, and others). Each bar shows the total number of connections during the monitoring interval for each unique component.

All Components
This view displays a table with more details about all components, aggregated by unique component name.

In the tables, the *column names* are the same as the attributes that supply the information to this workspace. For a definition of a particular column, see Response Time - Attributes listed alphabetically. Rows in the tables are highlighted in yellow for response times greater than one second. Links from these tables take you to additional workspaces containing more detail as appropriate.

Accessing the workspace

You can link to this workspace from the Navigator Physical view:

1. Click  beside the operating system for the computer on which the monitoring agent is located to display a list of monitored nodes, if necessary.
2. Click  beside the name of the node on which the Web Response Time monitoring agent is located, if necessary.
3. Click **Web Response Time**
4. Click **Network**.

   Alternatively, you can right-click the **Network** node and select **Components** from the list of available workspace links.

Linking to related workspaces

From this workspace you can link to the following workspaces:

- The "Component Details" on page 21 workspace, using any of the following methods:
  - Click the link icon  next to a table row in the All Components view.

- Right-click a table row in the All Components view, and select **Component Details** from the list of available links.

- The "Component History" on page 24 workspace, using any of the following methods:
  - Right-click a table row in the All Components view, and select **Component History** from the list of available links.

Component Details

This workspace provides details about a selected component in the TCP tracking data collected by the agentless transaction tracking feature.

This workspace provides additional details about component data for a specific component selected from either the"Components" on page 19 workspace or the Client Facing Components workspace.

The Component Details workspace provides a more in-depth look at the servers hosting the selected component, and the clients that use it. In addition to graphs showing timing, bandwidth and connection trend information, this workspace provides a Clients table view and a Component Servers table view.

This workspace displays summary graphs for the following metrics:

- Historical trend of active and terminated connections
- Historical trend of the total number of transactions and average response time
- Historical trend of send and receive bandwidth, in kilobytes per second

In addition to the chart views, this workspace also includes table views showing detailed data for the selected component, clients using the selected component, and servers that are hosting the selected component.

The Clients table provides a breakout of the TCP traffic for each client that is accessing the selected component. You can see what IP addresses or subnets are accessing the component, and the TCP metrics for the traffic coming from each individual client. From this table, you can link to the Client Dependencies workspace for a detailed look at other components, servers and protocols on which the client depends.

The Component Servers table shows the TCP metrics for each server hosting the component. Note that although the metrics are shown at the server level, the metrics only represent the TCP data going to and from the selected component, and do not reflect the total TCP traffic on the server. To see a more detailed look at the protocol and client TCP activity of these servers, use the "Component Server Details" on page 26 link for the desired server.

This workspace displays the bar charts and line graphs in each view, similar to the following example.

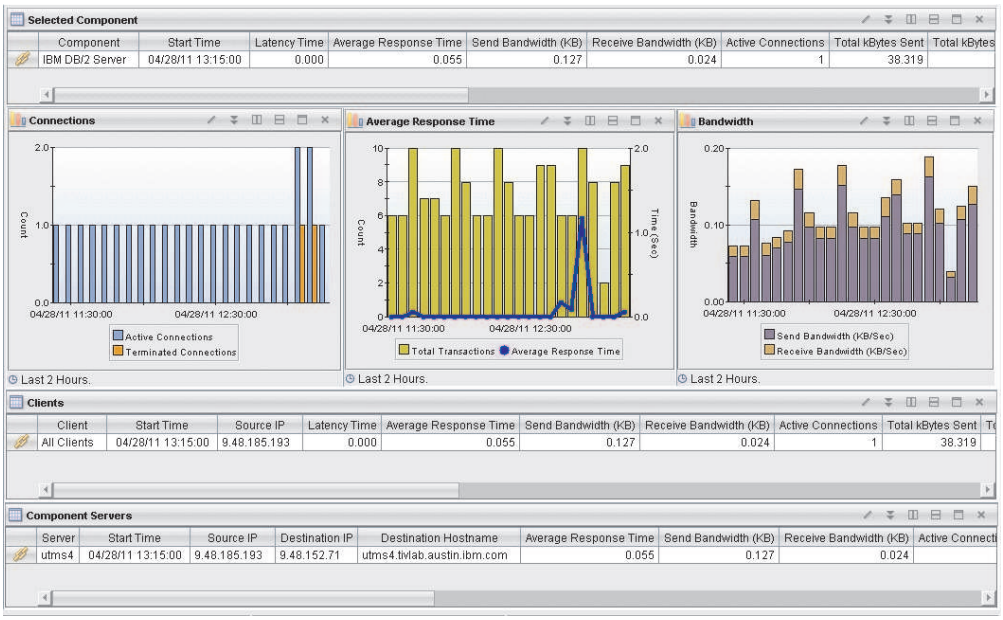


Figure 4. Component Details workspace

This workspace has the following views:

Average Response Time
This view displays a combined bar chart and line graph, showing the historic trend in average response time (line graph) and the historic trend in the total transaction time, in seconds (bar chart) for the selected component during the specified reporting time interval (default is the last 2 hours).

Bandwidth
This view displays a stacked vertical bar chart showing the historic trend in send bandwidth and receive bandwidth, in kilobytes per second, for the selected component (such as IBM HTTP Server, WebSphere Application Server, IBM DB2 Server, and others) during the specified reporting interval (the default is the last two hours).

Clients
This view displays a table with more details about the clients that are using the selected component.

Component Servers
This view displays a table with more details about the servers that are hosting the selected component.

Connections
This view displays a multi-bar chart that shows the historic trend of the number of connections (such as active, and terminated) for the selected component (such as IBM HTTP Server, WebSphere Application Server, IBM DB2 Server, and others) during the reporting interval (the default is the last 2 hours).

Selected Component
This view displays a table with more information about the monitored component that was selected previously to access this workspace.

Limitation on one-way traffic: It is not possible to measure average response time, server time, or network time for one-way traffic (such as

FTP-DATA network flows) without a protocol aware packet analyzer. As a result, the values in these columns of the table are always displayed as *0.000*.

In the tables, the *column names* are the same as the attributes that supply the information to this workspace. For a definition of a particular column, see Response Time - Attributes listed alphabetically. Rows in the tables are highlighted in yellow for response times greater than one second. Links from these tables take you to additional workspaces containing more detail as appropriate.

Accessing the workspace

You can link to this workspace from the following associated workspaces:

- From the "Components" on page 19 workspace, you can use either of the following methods:
  - Click the link icon  next to a table row in the All Components view.
  - Right-click a table row in the All Components view, and select **Component Details** from the list of available links.
- From the Client Facing Components workspace, you can use the following method:
  - Right-click a table row in the Client Facing Components view, and select **Component Details** from the list of available links.

Linking to related workspaces

From this workspace you can link to the following workspaces:

- The "Component History" on page 24 workspace, using any of the following methods:
  - Click the link icon  next to a table row in the Selected Component view.
  - Right-click a table row in the Selected Component view, and select **Component History** from the list of available links.
- The Client Dependencies workspace, using any of the following methods:
  - Click the link icon  next to a table row in the Clients view.
  - Right-click a table row in the Clients view, and select **Client Dependencies** from the list of available links.
- The "Component Server Details" on page 26 workspace, using any of the following methods:
  - Click the link icon  next to a table row in the Component Servers view.
  - Right-click a table row in the Component Servers view, and select **Component Server Details** from the list of available links.

Component History

This workspace provides an historical summary of the selected component in TCP tracking data collected by the agentless transaction tracking feature.

This workspace provides recent historical information about a component selected from either the "Components" on page 19 workspace or the "Component Details" on page 21 workspace. The granularity of this data is determined by the value of the Over Time Interval configuration parameter for the Web Response Time agent (see the *Installation Guide* for more information about configuring the Web Response Time agent).

Though the Component History workspace is the only default historical workspace provided for TCP data, TCP data is warehoused at many different aggregation levels. This allows you to create custom workspaces to examine historical TCP data at the component, server, client, and protocol levels. When creating queries for the WTP_TCP_Status ODI table, the Agg_By column filter determines what aggregation level is used for the resulting data. This same idea holds true when creating queries to be used in historical workspaces.

The following values are valid for the Agg_By column:

- All (0) : Data is aggregated on client, server, component, protocol and destination port.
- Server (1) : Data is aggregated on server.
- Client (2) : Data is aggregated on client.
- ClientByServer (3) : Data is aggregated on client and server.
- ClientByComponent (4) : Data is aggregated on client and component.
- ProtocolByServer (5) : Data is aggregated on protocol and server.
- Component (6) : Data is aggregated on component.
- ComponentByServer (7) : Data is aggregated on component and server.
- ComponentByServerByClient (8) : Data is aggregated on component, server and client.

This workspace displays summary graphs for the following metrics:

- Historical trend of active and terminated connections
- Historical trend of the total number of transactions and average response time
- Historical trend of send and receive bandwidth, in kilobytes per second

In addition to the chart views, this workspace also includes table views showing detailed information about the selected component and a table view of component history for each monitoring interval over the reporting interval (default is the last 8 hours).

This workspace displays a set of bar charts or line graphs in each view, similar to the following example.

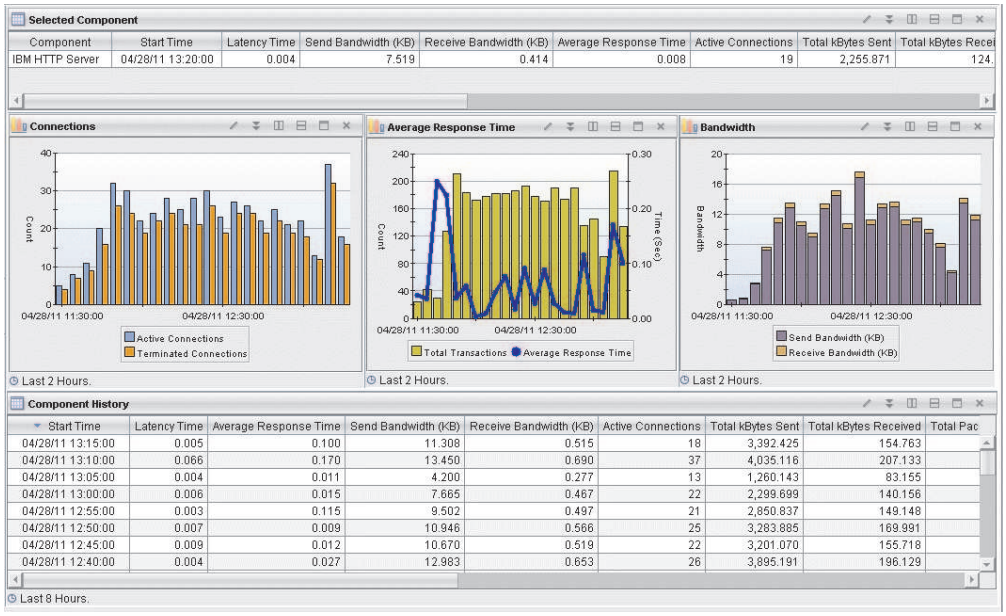


Figure 5. Component History workspace

This workspace has the following views:

Average Response Time

This view displays a combined bar chart and line graph, showing the historic trend in average response time (line graph) and the historic trend in the total transaction time, in seconds (bar chart) for the selected component during the specified reporting time interval (default is the last 2 hours).

Bandwidth

This view displays a stacked vertical bar chart showing the historic trend in send bandwidth and receive bandwidth, in kilobytes per second, for the selected component (such as IBM HTTP Server, WebSphere Application Server, IBM DB2 Server, and others) during the specified reporting interval (the default is the last two hours).

Component History

This view displays a table with more details about the selected component. Each row in the table contains data for each monitoring interval over the reporting period (default is the last 8 hours).

Connections

This view displays a multi-bar chart that shows the historic trend of the number of connections (such as active, and terminated) for the selected component (such as IBM HTTP Server, WebSphere Application Server, IBM DB2 Server, and others) during the reporting interval (the default is the last 2 hours).

Selected Component

This view displays a table with more information about the monitored component that was selected previously to access this workspace.

Limitation on one-way traffic: It is not possible to measure average response time, server time, or network time for one-way traffic (such as FTP-DATA network flows) without a protocol aware packet analyzer. As a result, the values in these columns of the table are always displayed as *0.000*.

In the tables, the *column names* are the same as the attributes that supply the information to this workspace. For a definition of a particular column, see Response Time - Attributes listed alphabetically. Rows in the tables are highlighted in yellow for response times greater than one second. Links from these tables take you to additional workspaces containing more detail as appropriate.

Accessing the workspace

You can link to this workspace from the following associated workspaces:

- From the "Components" on page 19 workspace, you can use either of the following methods:
  - Right-click a table row in the All Components view, and select **Component History** from the list of available links.
- From the "Component Details" on page 21 workspace, you can use the following method:
  - Right-click a table row in the Selected Component view, and select **Component History** from the list of available links.

Linking to related workspaces

There are no links available from this workspace.

Component Server Details

This workspace provides more details about a selected server that is hosting a particular component in the TCP tracking data collected by the agentless transaction tracking feature.

This workspace provides an in-depth view of the client and protocol breakdown for the component server selected from the "Component Details" on page 21 workspace.

This workspace displays summary graphs for the following metrics:

- Historical trend of active and terminated connections
- Historical trend of the total number of transactions and average response time
- Historical trend of send and receive bandwidth, in kilobytes per second

In addition to the trend graphs containing response time, bandwidth and connection information, this workspace provides a Clients table and a Protocol Breakdown table for viewing the TCP metrics for the component server, calculated at the client and protocol level.

The Clients table shows each client that accesses the component on the selected server, and the TCP metrics associated with each client's TCP communication to the server. To see more detailed information on which components and servers a client accesses, select the link to the Client Dependencies workspace.

The Protocol Breakdown table shows the component's TCP metrics for each component protocol that is hosted by the selected server. This protocol-level data provides the destination IP address, hostname, port and metrics for the associated TCP traffic.

This workspace displays a set of bar charts or line graphs in each view, similar to the following example.

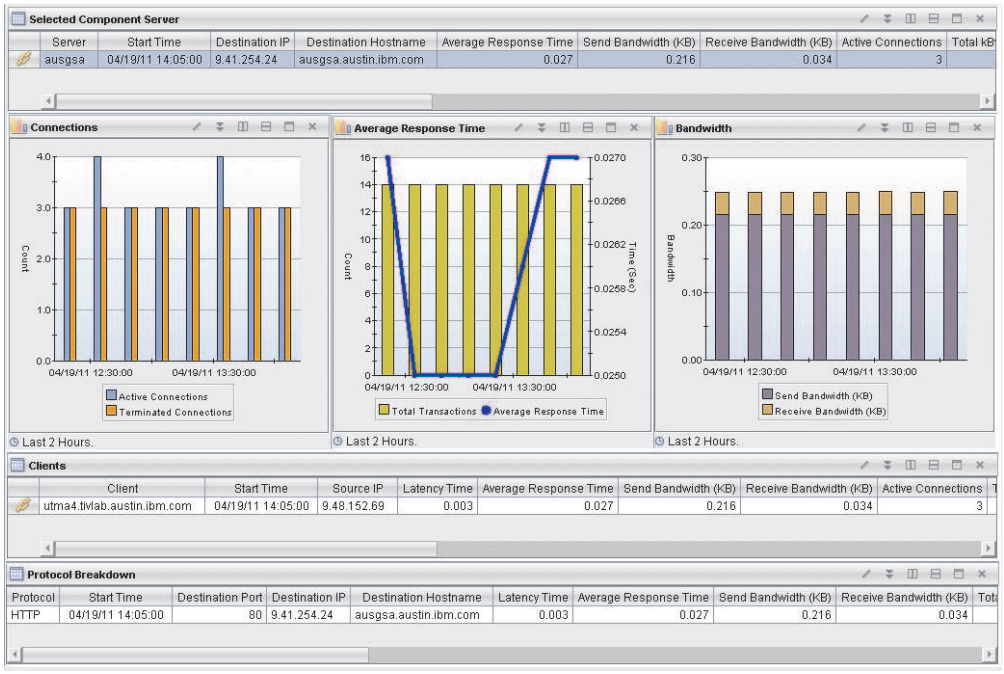


Figure 6. Components Server Details workspace

This workspace has the following views:

Average Response Time
: This view displays a combined bar chart and line graph, showing the historic trend in average response time (line graph) and the historic trend in the total transaction time, in seconds (bar chart) for the selected component server during the specified reporting time interval (default is the last 2 hours).

Bandwidth
: This view displays a stacked vertical bar chart showing the historic trend in send bandwidth and receive bandwidth, in kilobytes per second, for the selected component server during the specified reporting interval (the default is the last two hours).

Clients
: This view displays a table with more details about the clients connecting to the selected component server.

Connections
: This view displays a multi-bar chart that shows the historic trend of the number of connections (such as active, and terminated) for the selected component server during the reporting interval (the default is the last 2 hours).

Protocol Breakdown
: This view displays a table with more details about the protocol of the monitored traffic associated with the component on the selected server.

Selected Component Server
This view displays a table with more information about the server hosting a particular component, that was selected previously to access this workspace.

In the tables, the *column names* are the same as the attributes that supply the information to this workspace. For a definition of a particular column, see Response Time - Attributes listed alphabetically. Rows in the tables are highlighted in yellow for response times greater than one second. Links from these tables take you to additional workspaces containing more detail as appropriate.

Accessing the workspace

You can link to this workspace from the following associated workspace:

- From the "Component Details" on page 21 workspace, you can use either of the following methods:
  - Click the link icon  next to a table row in the Component Servers view.
  - Right-click a table row in the Component Servers view, and select **Component Server Details** from the list of available links.

Linking to related workspaces

From this workspace you can link to the following workspaces:

- The Server Dependencies workspace, using any of the following methods:
  - Click the link icon  next to a table row in the Selected Component Server view.
  - Right-click a table row in the Selected Component Server view, and select **Server Dependencies** from the list of available links.
- The Client Dependencies workspace, using any of the following methods:
  - Click the link icon  next to a table row in the Clients view.
  - Right-click a table row in the Clients view, and select **Client Dependencies** from the list of available links.

Chapter 5. Customizing the presentation of data in the topology

You can customize the data displayed in the topology in a number of ways.

Creating custom topology views

You can create new, custom Aggregate or Instance topology views:

- Aggregate topology
  - Use with Flexible Context
  - Display one or more attributes from Server Name, Component Name, Application Name, Transaction Name, depending on how you want to group your data
  - Customize the attribute and metrics displayed on links between nodes
  - Apply filters to limit the information displayed in the topology
- Instance topology
  - Use with Fixed Context
  - Server Name, Component Name, Application Name, Transaction Name are displayed and cannot be customized
  - Links in the topology cannot be customized
  - Topology filters cannot be applied

To create a new topology view:

1. In the Tivoli Enterprise Portal, click **Topology**  in the menu bar and click in the workspace to which you want to add a view.

   Tip: Remember that the default workspaces are read-only. Work within a workspace that is similar to what you want to create. You will be prompted to save the workspace under a new name.
2. In the Select Topology Source window, select the type of topology you want to create based on the information above, and click **OK**.
3. Click **Edit Properties**  and specify how you want your data displayed. See the following sections for more information.

Matching the agentless topology and your network schematic

If after you install and enable agentless transaction tracking, the topology presented in the Transactions Overview workspace or Agentless Data workspace does not match what you know to be your network topology, you may need to customize your components or filters.

Components

ITCAM for Transactions includes a number of default component definitions for standard protocols. These protocols are listed in the following table.

Table 3. Default component definitions for standard protocols

Component	Name (where applicable)	Default Port
Apache Tomcat	HTTP	8080
	HTTPS	8443
CICS TG		2006
DB2 Connect		446
FTP Server	FTP	20, 21
	FTPS	989, 990
IBM AnyNet	SNA over TCP	397
IBM DB2 Server		50000
IBM Directory Server	LDAP	389
	LDAPS	636
IBM HTTP Server	HTTP	80
	HTTP Admin	8008
	HTTPS	443
IMS Connect		8887
Lotus Domino Server		1352
Mail Server	IMAP	143
	IMAPS	993
	POP3	110
	POP3S	995
	SMTP	25
	SMTPS	465
Microsoft .NET	HIS SnaBasePort	1477
	HIS SnaServerPort	1478
	MSMQ	1801
Microsoft Active Directory Server		3268
Microsoft SQL Server		1433
MySQL Server		3306
Oracle Application Server	Oracle HTTP Server	7777
	Oracle HTTPS Server	4443
SAP NetWeaver Application Server	HTTP	8000
	SAP Dispatcher	3200
	SAP Gateway	3300
	SAP Message Server	3600
	SAP Message Server HTTP	8100
	Secured SAP Gateway	4800
Siebel Application Server		2321
SSH Server		22
Telnet Server		23

Table 3. Default component definitions for standard protocols (continued)

Component	Name (where applicable)	Default Port
WebSphere Application Server	HTTP	9080, 9082
	HTTP Admin	9060
	HTTPS	9443
	HTTPS Admin	9043
	Internal JMS Server	5557
	MQ Endpoint	5558
	MQ Endpoint secure	5578
	SOAP Connector	8880
WebSphere DataPower	DataPower Console	9090
	DataPower SOA	5550
WebSphere Message Broker	HTTP	7080, 7800-7842
	HTTPS	7083, 7843-7884

If you use different ports for standard protocols in your network, you must edit the component definitions in the Application Management Configuration Editor to include these ports. Similarly, if you use protocols which are not common, you must add them and the ports they use as new components if you want them to be displayed in the agentless topology. For more information, see "Creating components."

Filters

Filtering can be customized in any of the following ways:

- By filters defined for the topology. For more information, see "Filtering data in topologies" on page 39.
- By filters defined in the Application Management Configuration Editor. For more information, see Using filters in the Administrator's Guide.
- By parameters specified in the `kfcmenv` file.

  Ensure that the IP addresses and port numbers of the servers that you want to see are included in the **KFC_RESTRICT_HOST** parameter in the `kfcmenv` file, in the format *ip_address1*:*port1*, *ip_address2*:*port2*,.... Alternatively, ensure that the `kfcmenv` file does not contain a **KFC_RESTRICT_HOST** parameter, so that all traffic is monitored. For more information, see Web Response Time Analyzer parameters in the Administrator's Guide.

Creating components

You can use the Application Management Configuration Editor to create and manage components for TCP transaction traffic that you want to monitor.

You can use the Components feature of Application Management Configuration Editor to define the components and protocols to be monitored, and to provide a descriptive reporting name for all TCP traffic associated with a given components entry.

For example, you might define an entry for all traffic to servers 9.48.152.129 and 9.48.152.128 on port 82 and 445 to belong to the component named *Production HTTP(S)*, and therefore should be monitored. Using the Create Component

window in the Application Management Configuration Editor, you define your components similarly to how you define clients.

This section includes the following topics:

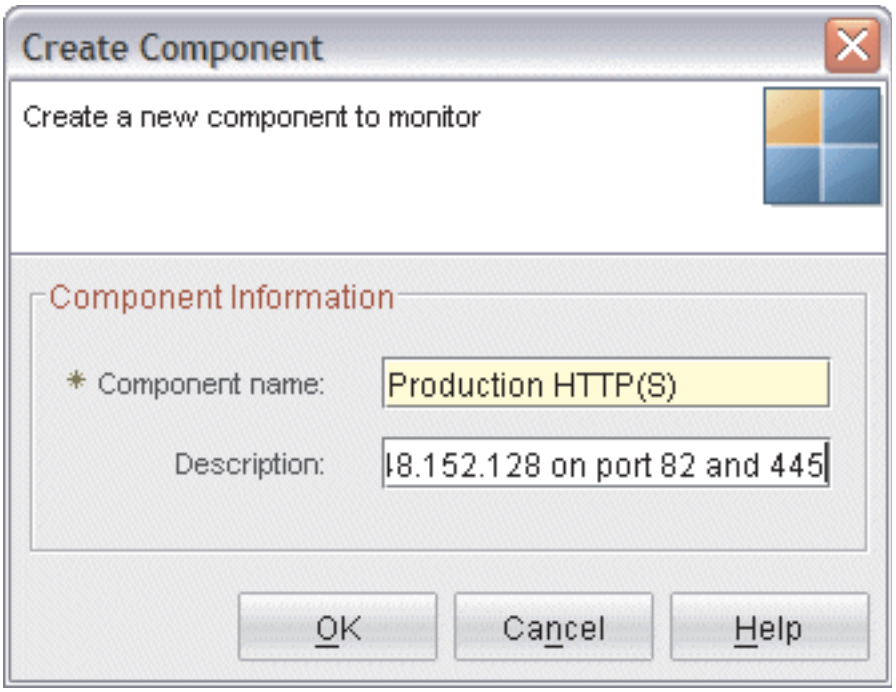
- Creating a component
- Defining protocols for your component
- Modifying an existing protocol
- Removing a protocol from your component
- Deleting a component

Procedure: Creating a component

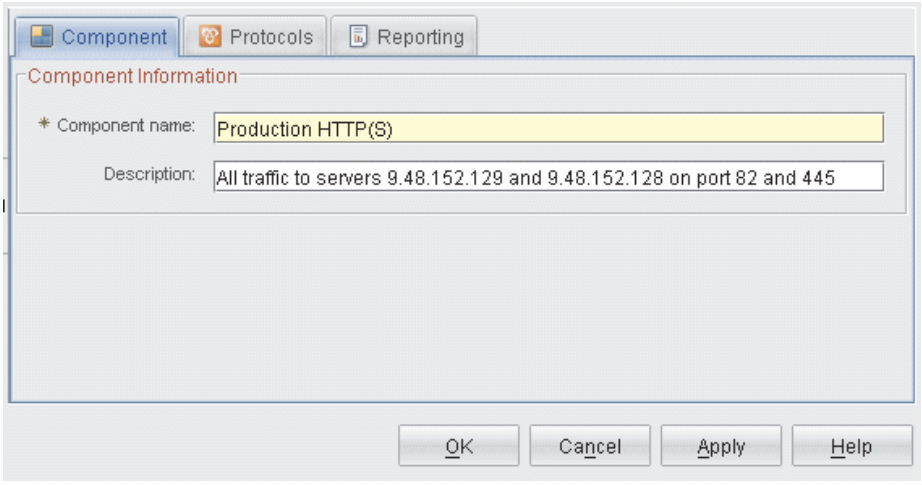
1. Access the Component view.
   a. Access the Tivoli Enterprise Portal.
   b. Click  in the toolbar.
      Previously defined applications, transactions, clients, profiles, and components are retrieved from the repository and loaded into the Application Management Configuration Editor. The Application Management Configuration Editor is displayed in a separate window.
   c. By default, the list of applications is displayed when the Application Management Configuration Editor is first opened. Click  and select **Components** to display the list of predefined components in the navigation view.
2. Create a new component.
   - To create a new component, click  .

     Note: The ability to create a new component by using an existing component as a template is not supported.

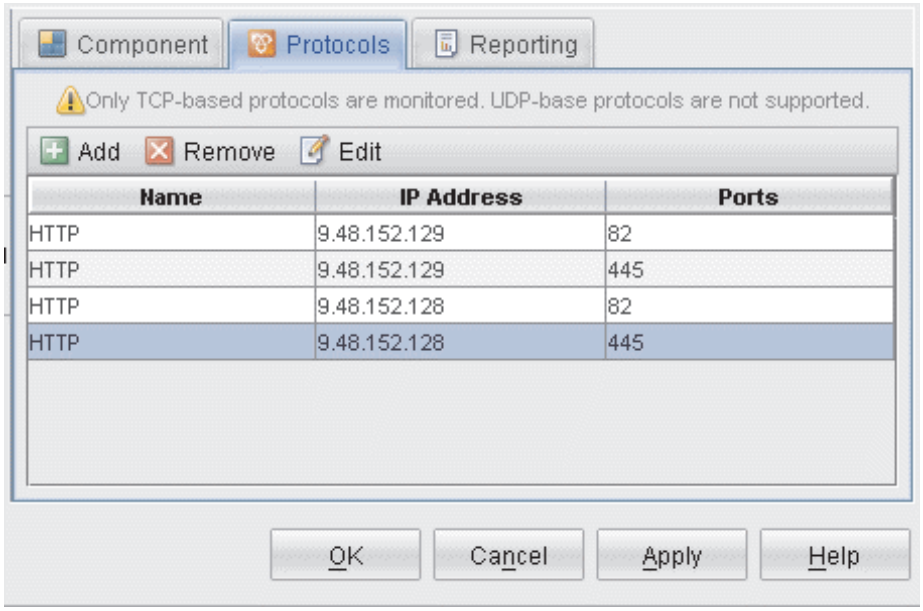
   The Create Component window is displayed.



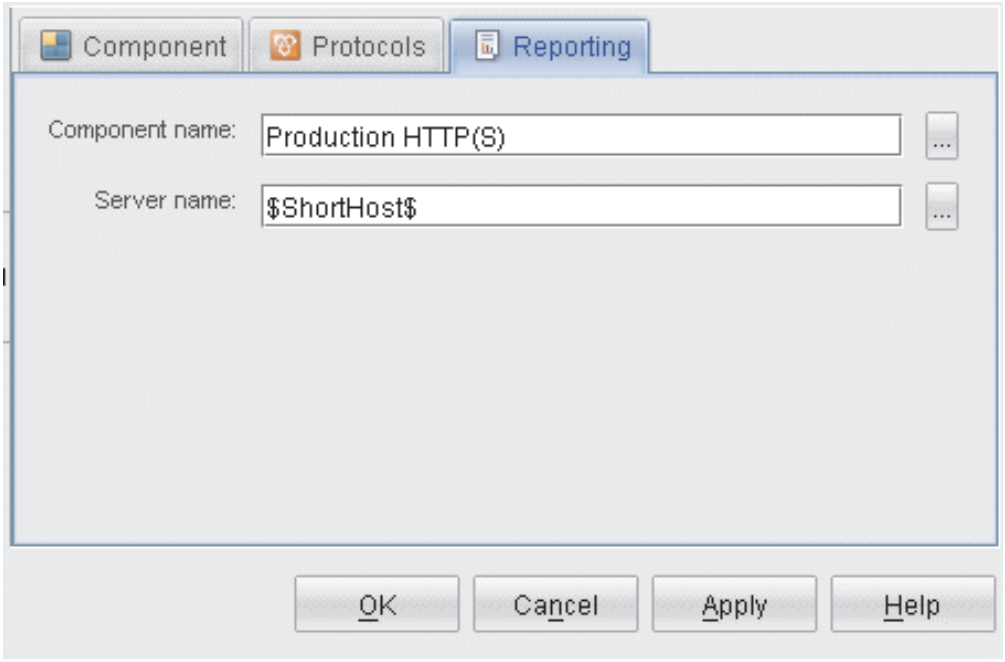
3. Define the new component.
   a. In the **Component name** field of the Create Component window, type the name of the new component.
   b. *Optional*: In the **Description** field, type the description text for the new component.
   c. Click **OK**. The **Component** tab is displayed on the right pane of the Application Management Configuration Editor, similar to the following example:



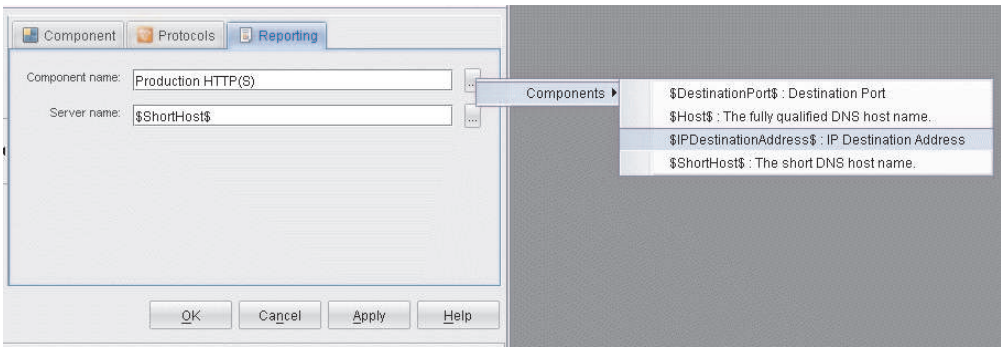
   The name and optional description you provided for the new component are displayed in the **Component Information** section at the top. You can modify these fields by typing over the content if needed.
   d. Click the **Protocols** tab to display the protocol table for the component. For a new component, this table is initially empty. Click **Add** to add one or more protocol definitions to the component. For more information about defining protocols, see Defining protocols. In this example, the resulting protocols defined for this new component might look similar to the following example:



e. Click the **Reporting** tab to display the reporting rules that the software uses to name the collected data that is displayed in the workspaces. The current reporting rules for the selected transaction are displayed in the Reporting tab, similar to the following example:



Click  to the right of each field to display an additional menu of selections, similar to the following example, and choose from that selection.



This procedure for defining reporting rules for components is similar to the procedure for clients. For more information about defining reporting rules, see Defining reporting rules.

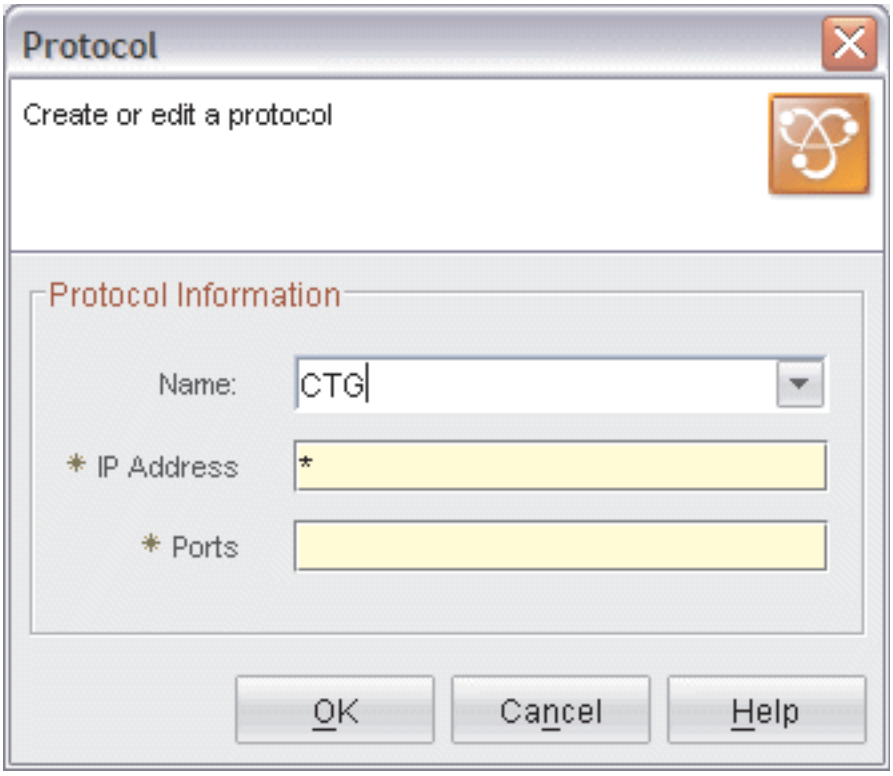
f. Click **Apply** to save your changes and continue using the Application Management Configuration Editor.

g. When you are finished, click **OK** to close the Application Management Configuration Editor.

Procedure: Defining protocols

Use the following procedure to define protocols for your components.

1. If you have not already done so, access the component for which you want to create a protocol. (See Procedure: Modifying an existing transaction)
2. If you have not already done so, click the **Protocols** tab.
3. Click  . The Protocol window is displayed, similar to the following example:



4. By default, an existing protocol name is displayed in the **Name** field. To select a different protocol, click  in the **Name** field and choose a protocol from the list of available protocols, or you can type over the name in this field to create a new protocol name.
5. In the **IP Address** field, type the IP address (for example, 192.168.1.10) or address pattern (for example, 192.168.1.*) to match on for this protocol. You can include asterisk (*) characters in the value to act as wildcard characters:
   - If you include an * at the beginning of the string, then everything that follows the * must match the transaction.
   - If you include an * at the end of the string, then everything that precedes the * must match the transaction.
   - If you include an * at the beginning and end of the string, then everything between the two * characters must match the transaction.
   - If you include an * anywhere else, then the string being matched must contain an * in that position for the match to succeed.

   Format checking is performed on this field, and an error message is displayed if you specify the IP address or pattern in an unacceptable format. You can specify only one IP address or matching pattern in this field.
6. In the **Ports** field, type one or more port numbers to be matched for this protocol. Specify multiple port numbers using comma separated values (for example, 80, 85), or a range of ports (for example, 80-85), or a combination of both (for example, 80-85, 9081, 9085).

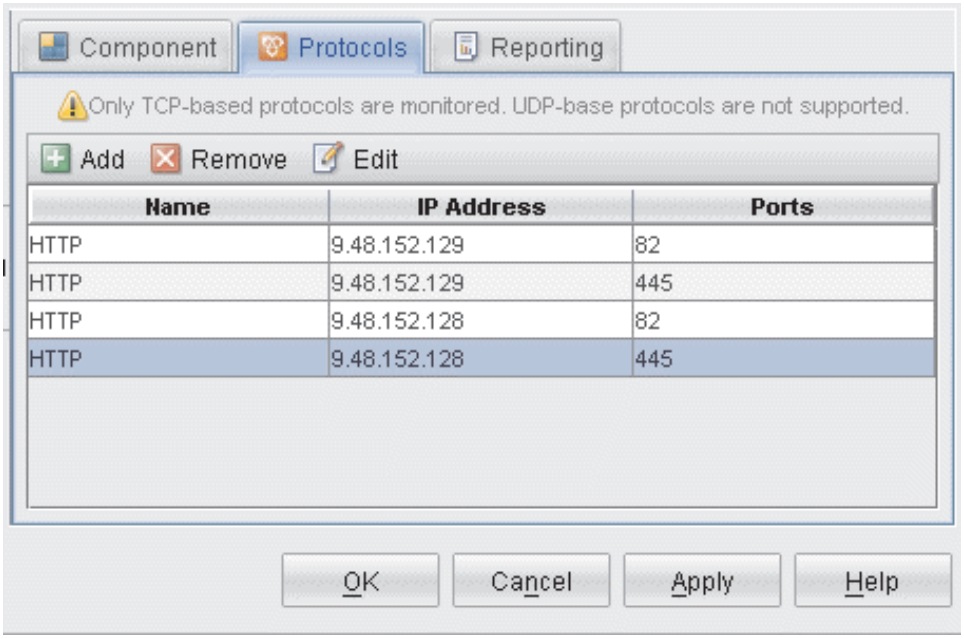
7. Click **OK**. The Protocol window is closed, and the protocol is added to the table in the **Protocols** tab.

   Avoid overlapping protocols: A protocol is defined as the combination of a specific IP address (or pattern) and one or more port numbers. Protocols cannot overlap. If you define a protocol that includes the same IP Address or pattern match and port number as an existing protocol definition, perhaps because asterisk wild card characters are being used in either or both protocols, when you click OK, an error message is displayed that indicates you have set up overlapping protocols. The conflicting component and protocol name is identified. You will need to correct your protocol definition to remove the overlap conflict.
8. Click **Apply** to save your changes and continue using the Application Management Configuration Editor.
9. When you are finished, click **OK** to close the Application Management Configuration Editor.

Procedure: Modifying an existing protocol in the component definition

Use the following procedure to modify previously defined protocols in your components.

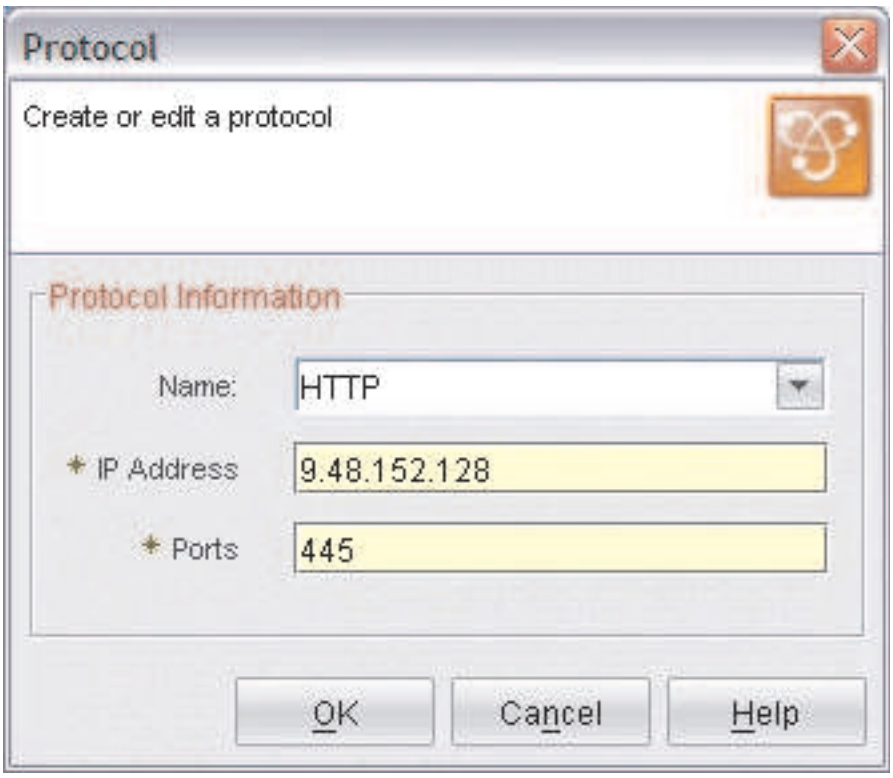
1. If you have not already done so, access the component for which you want to modify a protocol.
2. If you have not already done so, click the **Protocols** tab.
3. A table showing the list of defined protocols is displayed in the **Protocols** tab:



   You can sort the list of filters by clicking on the **Name**, **IP Address**, or **Ports** column headers in the title bar.

4. After selecting a protocol to modify, click 

. The selected protocol is displayed in the Protocol window.

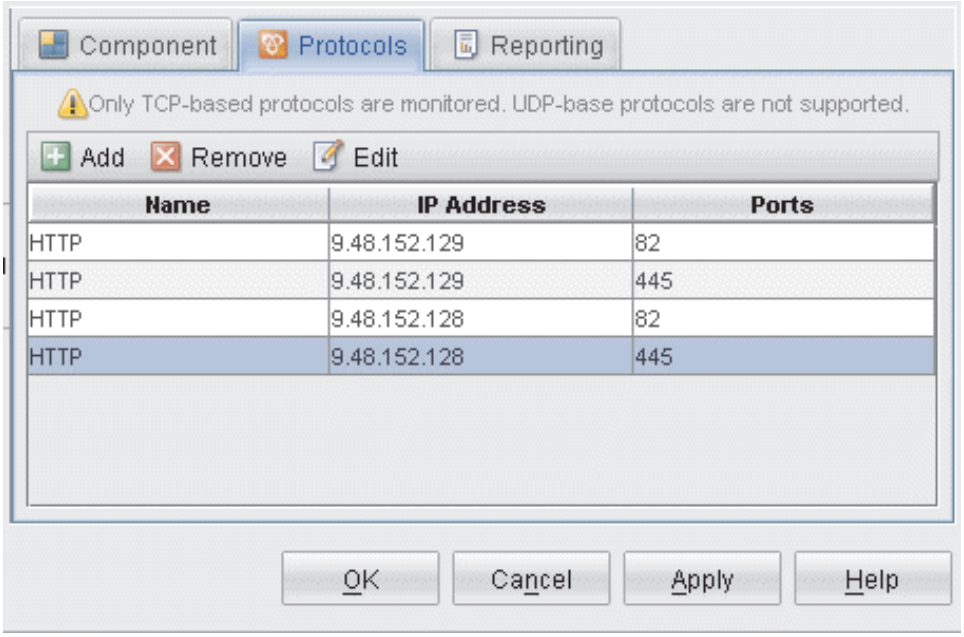


5. Edit the protocol definition as needed. You can change the name, IP Address, and port information. Click **OK** to save your changes.
6. Click **Apply** to save your changes and continue using the Application Management Configuration Editor.
7. When you are finished, click **OK** to close the Application Management Configuration Editor.

Procedure: Removing protocols from the component definition

Use the following procedure to remove protocols from defined components.

1. If you have not already done so, access the component for which you want to remove a protocol.
2. If you have not already done so, click the **Protocols** tab.
3. A table showing the list of defined protocols is displayed in the **Protocols** tab:



You can sort the list of filters by clicking on the **Name**, **IP Address**, or **Ports** column headers in the title bar. You can select multiple protocols by holding down the **Ctrl** key as you click each protocol.

4. After selecting one or more protocols to remove, click Remove. The selected protocols are removed from the table.
5. Click **Apply** to save your changes and continue using the Application Management Configuration Editor.
6. When you are finished, click **OK** to close the Application Management Configuration Editor.

Procedure: Deleting a component

To delete a component, perform the following steps:

1. Select the navigator item of the component that you want to remove from the view.
2. Click , or right-click the item in the tree and choose **Delete Component**.
3. Click **Yes** to confirm the operation.
4. Click **Apply** to save your changes and continue using the Application Management Configuration Editor.
5. When you are finished, click **OK** to close the Application Management Configuration Editor.

Filtering data in topologies

You can customize the information that is displayed in the Agentless topology using filter elements and operands which describe how to manipulate the data.

You can adjust the information displayed in a Transaction Tracking topology using one or more filter elements. Table columns from the Interaction Metrics table corresponding to source and destination contexts and metrics can be used as filter elements. Table 4 lists the most commonly used filter elements.

Table 4. Common filter elements

Filter element	Description
Destination Agent	Use to specify the agents from which to display data.
Destination Component Name	Use to limit the data displayed to particular components, such as IBM HTTP Server, orWebSphere Application Server.
Numerical interaction metric columns. For example, Received Bandwidth	Use to display data only above or below a particular threshold.

For each filter element, use an operand described in Table 5 together with a value to limit the data displayed in the topology.

Table 5. Filtering operands for Agentless topologies

Description	String	Numerical
Include only the data that matches the specified value.	==	==
Exclude data that matches the specified value.	!=	!=
Include only data that contains the specified value.	LIKE	
Exclude data that contains the specified value.	!LIKE	
Include data with a value greater than that specified.		>
Include data with a value less than that specified.		<
Include data with a value greater than or equal to that specified.		>=
Include data with a value less than or equal to that specified.		<=

Tip: When specifying filters in the Properties window, the filters that you have set are displayed in the **Formula** text box.

As for other Tivoli Enterprise Portal adapters, all filter conditions defined on a single row are combined in an AND statement, and filters on separate rows are added as OR statements.

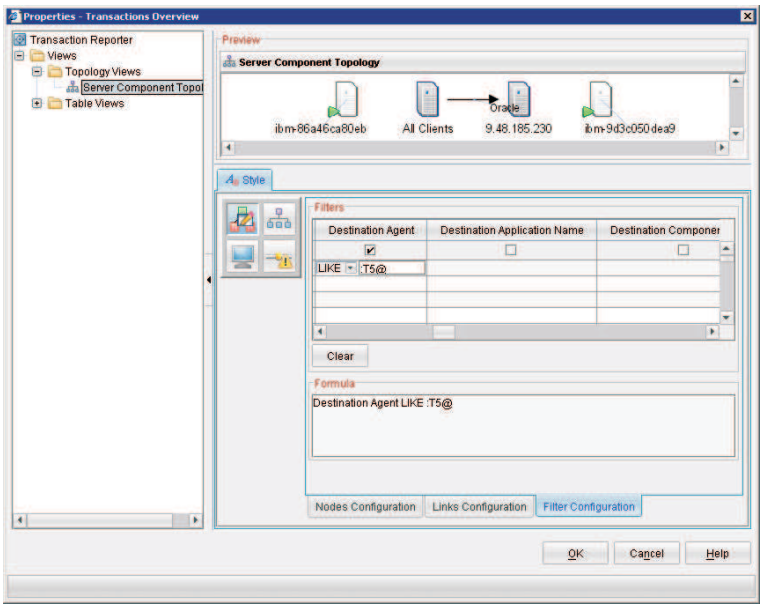
Described next are some common filters that you might want to apply.

You can also filter Web Response Time data, such as IP addresses and URLs, before it reaches the topology presentation layer. See Using filters.

Specifying a data source

To limit the data shown in the topology to data gathered by a particular agent:

1. In the topology, click  **Edit Properties**.
2. On the **Filter Configuration** tab, in the **Filters** pane, specify a data source:



   a. Scroll across and select **Destination Agent**.

      Note: Metrics are only displayed if there is traffic related to those metrics.

   b. Click in the row and select `LIKE`.

   c. Enter the agent code of the required destination agent and any additional text that might help isolate the correct agent. Ensure that the value is unique by including additional characters. For example, if you specify `T5` for Web Response Time, the value might also match `HOST5`. Because the agent context is *`host`*`:T5@`*`TEMS`* (where *host* is the hostname, T5 is the product code, and *TEMS* is the name of the Tivoli Enterprise Monitoring Server) you can instead enter `:T5@` to match this agent.

3. Click **OK**.
4. Press F5 to refresh the topology and display your changes.

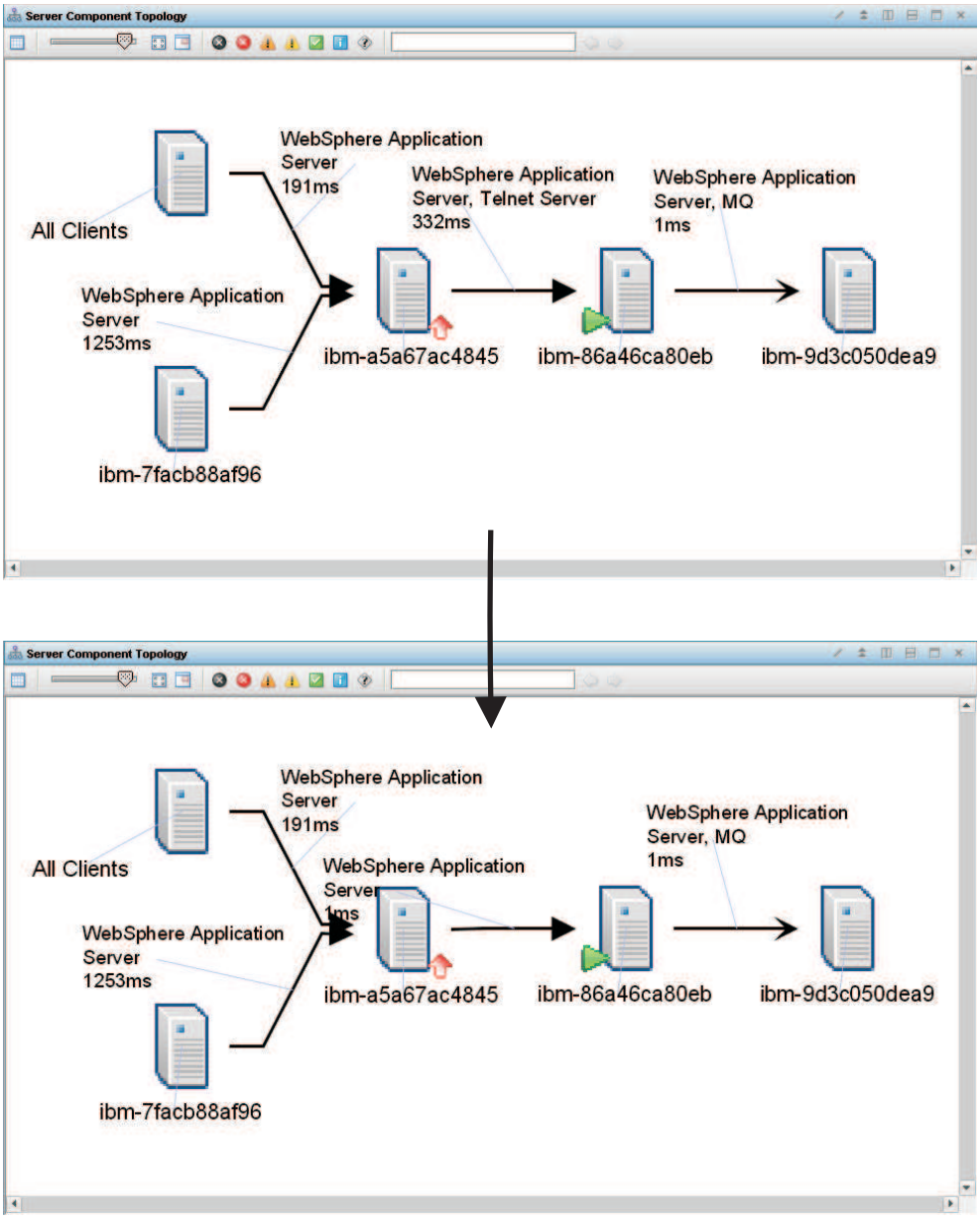
Displaying data for a single component

You can filter the data so that only the data for a particular component is displayed in the topology. You can either exclude data for those components that you are not interested in, or include only data for those components in which you are interested.

To filter the data so that only the data for a particular component is displayed in the topology:

1. In the topology, click  **Edit Properties**.
2. On the **Filter Configuration** tab, in the **Filters** pane, specify the component:
   a. Scroll across and select **Destination Protocol**.

      Note: Metrics are only displayed if there is traffic related to those metrics.
   b. To include only IBM HTTP Server, MQ, andWebSphere Application Server:
      - Click in a row, select ==, and enter `IBM HTTP Server`.
      - Click in the next row, select ==, and enter `MQ`.
      - Click in the next row, select ==, and enter `WebSphere Application Server`.
3. Click **OK**.
4. Press **F5** to refresh the topology and display your changes.



Removing links for which there is no traffic

To display only those links between nodes for which there is traffic:

1. In the topology, click  **Edit Properties**.
2. On the **Filter Configuration** tab, in the **Filters** pane, specify the amount of traffic that you want to monitor:
   a. Scroll across and select **Received Bandwidth**.

      Note: Metrics are only displayed if there is traffic related to those metrics.
   b. Click in the row and select >.
   c. Enter the value 0.
3. Click **OK**.
4. Press F5 to refresh the topology and display your changes.

Removing all filters

To remove all filters, in the **Filters** pane of the Properties window, click **Clear**.

Displaying protocols on links

The Network Topology in the default Agentless Data workspace shows servers on nodes and components on links between nodes. You can change this so that protocols instead of components are displayed on the links between nodes.

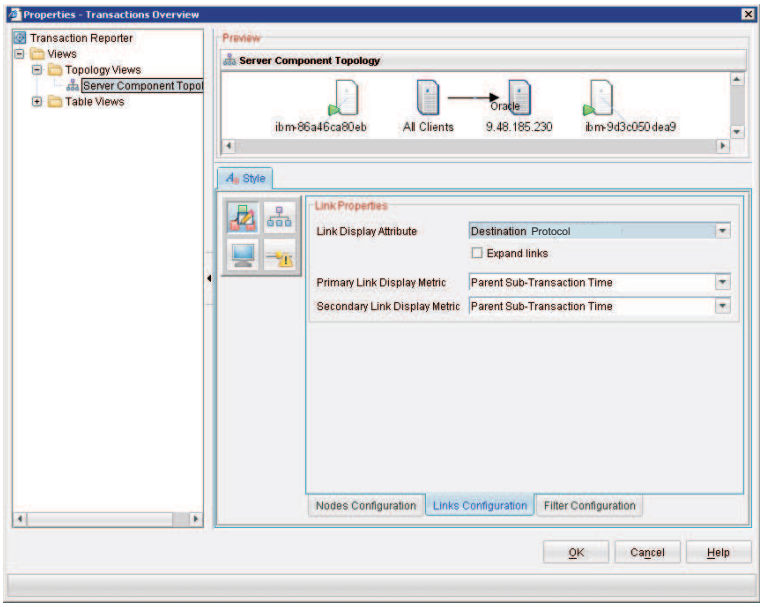
About this task

Use the **Properties** window to customize how the agentless information is displayed in the workspace.

Procedure

To add a component topology:

1. In the topology, click  **Edit Properties**.
2. On the **Nodes Configuration** tab, in the **Properties** pane, select **Flexible Contexts**.
3. On the **Links Configuration** tab, in the **Link Display Attribute** list, select **Destination Protocol**.



Note: There must be traffic for all selections in the **Link Display Attribute** list to be available.

4. Click **OK**.
5. Press F5 to refresh the topology and display your changes.

What to do next

To switch back to displaying components on links:

1. In the Topology, click  **Edit Properties**.
2. In the **Properties** pane, select **Flexible Contexts**.
3. On the **Links Configuration** tab, in the **Link Display Attribute** list, select **Destination Component Name**.
4. Click **OK**.
5. Press F5 to refresh the topology and display your changes.

Chapter 6. Including agentless transaction tracking data in events

To include agentless transaction tracking data in events, use the Transaction Tracking situations included in ITCAM for Transactions V7.3 and later.

See Chapter 4 of the *User's Guide* for further information.

Chapter 7. Best practices and tutorials

The latest best practices, tutorials, and videos are posted to IBM developerWorks.

See ITCAM for Transactions on developerWorks for further information.

Appendix A. WRT TCP Status

This attribute group provides information about low level TCP data.

Active Connections The total number of active TCP socket connections created during the current aggregate interval.

Aggregate By Specifies how the Web Response Time monitoring agent aggregates its collected low level TCP data, by client, server, component, protocol, or a combination of these groups.

Average Network Time The average elapsed time, in seconds, spent transmitting all required data through the network. This is a calculated time. For instance data, this field is an absolute value, not an average.

Average Response Time The average response time, in seconds, for a single transaction instance that was observed during the monitoring interval. During each monitoring interval, minimum, maximum, and average response times for the aggregate records are recorded. Use these attributes to analyze the range of response times for the transaction.

Average Server Time The average elapsed time, in seconds, that a transaction spends running on the server during the current monitoring interval. For a transaction instance, this value is an absolute time, not an average.

Client The name of the client that initiated the request (or transaction).

Component The component name of the monitored traffic as specified in the Component definition in the Application Management Configuration Editor.

Data Interval The frequency, in seconds, that indicates how often the monitoring agent collects data.

Destination Hostname The destination hostname of the transaction.

Destination IP The destination IP address of the transaction.

Destination Port The destination IP port of the transaction.

End Time The aggregation end time when the monitoring agent stopped collecting data (using the format MM/DD/YY HH:MM:SS), in Greenwich Mean Time (GMT).

Latency Time The time it takes for a client to receive a 0-byte TCP response packet after sending a 0-byte TCP request packet.

New Connections The total number of new TCP socket connections created during the current aggregate interval.

Number of Retransmissions The number of packets retransmitted.

Origin Node The name of the host subnode.

Protocol The user-defined networking protocol used for the TCP Transaction.

Receive Bandwidth The average number of kilobytes per second received by a server from a client during the current monitoring interval.

Send Bandwidth The average number of kilobytes per second sent by a server to a client during the current monitoring interval.

Server The name or IP address of the server for the TCP Transaction.

Source Hostname The source hostname for the transaction.

Source IP The source IP address for the transaction.

Start Time The time (during the last 8 hours) when the monitoring agent started collecting data (using the format MM/DD/YY HH:MM:SS), in Greenwich Mean Time (GMT).

Terminated Connections The total number of terminated TCP socket connections created during the current aggregate interval.

Total kBytes Received The total number of kilobytes of data received by the server during the current aggregate interval.

Total kBytes Sent The total number of kilobytes of data sent by the server during the current aggregate interval.

Total Packets Received The total number of IP packets received by the server during the current aggregate interval.

Total Packets Sent The total number of IP packets sent by the server during the current aggregate interval.

Total Transactions The total number of request and response sequences observed by the monitoring agent during the current aggregate interval.

Appendix B. Context information for aggregates

The Aggregate Context (TOAGGCTX) table contains context information about an aggregate, including vertical context and caller types, which the Transaction Reporter uses to identify the source of aggregates and records.

Table_Name Context information for aggregates

System_Name Managed system name of the Transaction Reporter that provides this information.

Timestamp Start time of the period of aggregation.

Aggregate_ID Identifier of the aggregate.

Context_Name Identifier of the aggregate context name.

Description Identifier of the aggregate context value.

Appendix C. Interaction definitions

The Interactions (TOINTERTN) table defines the interactions between aggregates.

Table_Name Interaction definitions

System_Name Managed system name of the Transaction Reporter that provides this information.

Timestamp Start time of the period of aggregation.

Source_Aggregate_ID Identifier of the source aggregate.

Destination_Aggregate_ID Identifier of the destination aggregate.

Interaction_Type Interaction type.

Appendix D. String map

The String Map (TOSTRMAP) table contains the string values used by the TOAGGCTX table.

Table_Name String map

System_Name Managed system name of the Transaction Reporter that provides this information.

Timestamp Start time of the period of aggregation.

String_ID Identifier of the string.

String_Length Remaining length of the string.

String_Value Value of the string.

Appendix E. Metric units

The Metric Units (TOUNITTYPE) table describes the units of metrics.

Table_Name Metric units

System_Name Managed system name of the Transaction Reporter that provides this information.

Timestamp Start time of the period of aggregation.

Unit_ID Identifier of the metric unit.

Unit_String String representation of the metric unit.

Appendix F. Metric types

The Metric Types (TOMETTYPE) table stores the metric types for display in table views.

Table_Name Metric types

System_Name Managed system name of the Transaction Reporter that provides this information.

Timestamp Start time of the period of aggregation.

Type_ID Identifier of the metric type.

Type_String String representation of the metric type.

Unit Identifier of the metric unit.

Appendix G. Aggregate gauge metrics

The Aggregate Gauge Metrics (TOAGGGMET) table stores gauge metrics for an aggregate, that is, range-based numeric data with an aggregation type of MIN, MAX, or AVG.

Table_Name Aggregate gauge metrics

System_Name Managed system name of the Transaction Reporter that provides this information.

Timestamp Start time of the period of aggregation.

Aggregate_ID Identifier of the aggregate.

Type Identifier of the metric type.

Gauge_Value Value of the metric.

Sample_Count Sample count of the metric.

Appendix H. Aggregate count metrics

The Aggregate Count Metrics (TOAGGCMET) table stores count metrics for an aggregate, that is metrics with an aggregation type of TOT, HI, LOW, or LAT.

Table_Name Aggregate count metrics

System_Name Managed system name of the Transaction Reporter that provides this information.

Timestamp Start time of the period of aggregation.

Aggregate_ID Identifier of the aggregate.

Type Identifier of the metric type.

Count_Value Value of the metric.

Appendix I. Interaction gauge metrics

The Interaction Gauge Metrics (TOINTGMET) table stores gauge metrics for an interation, that is, range-based numeric data with an aggregation type of MIN, MAX, or AVG.

Table_Name Interaction gauge metrics

System_Name Managed system name of the Transaction Reporter that provides this information.

Timestamp Start time of the period of aggregation.

Source_ID Identifier of the source aggregate.

Destination_ID Identifier of the destination aggregate.

Interaction_Type Interaction type.

Type Identifier of the metric type.

Gauge_Value Value of the metric.

Sample_Count Sample count of the metric.

Appendix J. Interaction count metrics

The Interaction Count Metrics (TOINTCMET) table stores count metrics for an interation, that is metrics with an aggregation type of TOT, HI, LOW, or LAT.

Table_Name Interaction count metrics

System_Name Managed system name of the Transaction Reporter that provides this information.

Timestamp Start time of the period of aggregation.

Source_ID Identifier of the source aggregate.

Destination_ID Identifier of the destination aggregate.

Interaction_Type Interaction type.

Type Identifier of the metric type.

Count_Value Value of the metric.

Appendix K. Aggregate Situations

The Aggregate Situations (TOAGGSIT) table stores metrics for an aggregate, in a format suitable for defining situations.

Table_Name Aggregate Situations

System_Name Managed system name of the Transaction Reporter that provides this information.

Timestamp Start time of the period of aggregation.

Aggregate_ID Identifier of the aggregate.

Filter_Value Configurable formatted column for filtering on.

Filter_Format Format specification for the filter value column.

Metric_Name Name of the metric type.

Metric_Value Value of the metric.

Display_Format Format specification for the display text column.

Display_Value Configurable text to display for situations.

Appendix L. Interaction Situations

The Interaction Situations (TOINTSIT) table stores metrics for an interation, in a format suitable for defining situations.

Table_Name Interaction Situations

System_Name Managed system name of the Transaction Reporter that provides this information.

Timestamp Start time of the period of aggregation.

Source_ID Identifier of the source aggregate.

Destination_ID Identifier of the destination aggregate.

Interaction_Type Interaction type.

Filter_Value Configurable formatted column for filtering on.

Filter_Format Format specification for the filter value column.

Metric_Name Name of the metric type.

Metric_Value Value of the metric.

Display_Format Format string for the display text.

Display_Value Configurable text to display for situations.

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 grant 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 may not apply to you.

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

Any references in this information to non-IBM websites are provided for convenience only and do not in any manner serve as an endorsement of those websites. The materials at those websites are not part of the materials for this IBM product and use of those websites 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 want 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 information 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 measurements 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.

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.

If you are viewing this information softcopy, the photographs and color illustrations may not appear.

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" at http://www.ibm.com/legal/copytrade.shtml.

Adobe, the Adobe logo, PostScript, and the PostScript logo are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States, and/or other countries.

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

Java and all Java-based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates.

Linux is a trademark of Linus Torvalds 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.

This Software Offering does not use cookies or other technologies to collect personally identifiable information.

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.

Glossary

agent Software installed to monitor systems. The agent collects data about an operating system, a subsystem, or an application.

agent group
A group of management agents that run the same policy or policies. Each management agent is associated with one or more listening and playback components.

agentless
A method a data collection where data is collected from traffic on networks monitored by Web Response Time rather than a domain-specific agent or Data Collector plug-in.

aggregate
(1) An average of all response times detected by the monitoring software over a specific time period. (2) In Transaction Tracking, a node in a transaction topology.

aggregate record
A summary of instance data from all transactions that match a defined pattern.

aggregate topology
A transaction topology that displays all known and implied transactions which may not all be related. See also instance topology.

Aggregation agent
An agent that stores the tracking data from more than one Data Collector plug-in and other monitors and computes aggregates for use by the Transaction Reporter. The Transaction Collector and Web Response Time agent are examples of a Aggregation agent.

aggregation period
The time period, measured in minutes, over which monitoring occurs.

alert A message or other indication that signals an event or an impending event.

application
One or more computer programs or software components that provide a function in direct support of a specific business process or processes.

application pattern
A rule that determines what transactions to monitor and how to group them.

arithmetic expression
A statement that contains values joined together by one or more arithmetic operators and that is processed as a single numeric value. See also arithmetic operator.

arithmetic operator
A symbol, such as + or -, that represents a fundamental mathematical operation. See also arithmetic expression.

ARM-instrumented application
An application in which ARM calls are added to the source code to enable the performance of the application to be monitored by management systems.

attribute
The application properties that are measured and reported on, such as the amount of memory used or a message ID. See also attribute groups.

attribute group
A set of related attributes that can be combined in a data view or a situation.

availability
The successful execution of a monitored transaction over a specified period of time.

client A software program or computer that requests services from a server.

client pattern
A method to define which clients to monitor, and how to group them for reporting.

client time
The time it takes to process and display a web page in a browser.

condition
A test of a situation or state that must be in place for a specific action to occur.

configuration
The manner in which the hardware and software of an information processing system are organized and interconnected.

context
The means used to group tracking data as part of a transaction flow.

Data Collector plug-in
The monitoring component that records the transaction data.

data interval
A time period in minutes for the summary data record. See also summary data.

data source
An application, server, transaction, or other process from which raw data is gathered.

domain
A part of a network that is administered as a unit with a common protocol.

down time
See mean time to recovery.

edge
In transaction monitoring, the point at which a transaction first comes in contact with the monitoring instrumentation.

event An occurrence of significance to a task or system. Events can include completion or failure of an operation, a user action, or the change in state of a process. See also situation.

failure
An individual instance of a transaction that did not complete correctly. See also incident.

firewall
A network configuration, typically both hardware and software, that prevents unauthorized traffic into and out of a secure network.

horizontal
Pertaining to data that is tracked between applications in a domain. See also vertical.

horizontal context
A method of identifying a transaction flow within a transaction which is used to group interactions based on the application supplying the tracking data.

host A computer that is connected to a network and that provides an access point to that network. The host can be a client, a server, or both a client and a server simultaneously.

hot spot
A graphical device used in topologies to highlight the part of an end-to-end transaction that has crossed specified thresholds and has a significant transaction time deviation.

incident
A failure or set of consecutive failures over a period of time without any successful transactions. An incident concerns a period of time when the service was unavailable, down, or not functioning as expected.

instance
A single transaction or subtransaction.

implied node
A node that is assumed to exist and is therefore drawn in the Transaction Tracking topology. An implied node is created when an aggregate collected in an earlier aggregation period is not collected for the current aggregation period.

instance algorithm
A process used by the Transaction Reporter to track composite applications with multiple instances.

instance topology
A transaction topology that displays a specific instance of a single transaction. See also aggregate topology.

interval
The number of seconds that have elapsed between one sample and the next.

linking
In Transaction Tracking, the process of tracking transactions within the same domain or from data collector plugins of the same type.

load time
The time elapsed between the user's request and completion of the web page download.

managed system
A system that is being controlled by a given system management application.

Management Information Base
(1) In the Simple Network Management

Protocol (SNMP), a database of objects that can be queried or set by a network management system. (2) A definition for management information that specifies the information available from a host or gateway and the operations allowed.

mean time between failures
The average time in seconds between the recovery of one incident and the occurrence of the next one.

mean time to recovery
The average number of seconds between an incident and service recovery.

metric A measurement type. Each resource that can be monitored for performance, availability, reliability, and other attributes has one or more metrics about which data can be collected. Sample metrics include the amount of RAM on a PC, the number of help desk calls made by a customer, and the mean time to failure for a hardware device.

metrics aggregation
A process used by the Transaction Collector to summarize tracking data using vertical linking and stitching to associate items for a particular transaction instance. Metrics aggregation ensures that all appropriate tracking data is aggregated.

MIB See Management Information Base.

monitor
An entity that performs measurements to collect data pertaining to the performance, availability, reliability, or other attributes of applications or the systems on which the applications rely. These measurements can be compared to predefined thresholds. If a threshold is exceeded, administrators can be notified, or predefined automated responses can be performed.

monitoring agent
See agent.

monitoring schedule
A schedule that determines on which days and at what times the monitors collect data.

MTBF See mean time between failures.

MTTR
See mean time to recovery.

network time
Time spent transmitting all required data through the network.

node A point in a transaction topology that represents an application, component, or server whose transaction interactions are tracked and aggregated by Transaction Tracking.

over time interval
The number of minutes the software aggregates data before writing out a data point.

parameter
A value or reference passed to a function, command, or program that serves as input or controls actions. The value is supplied by a user or by another program or process.

pattern
A process used to group data into manageable pieces.

platform
The combination of an operating system and hardware that makes up the operating environment in which a program runs.

predefined workspace
A workspace that is included in the software which is optimized to show specific aspects of the collected data, such as agentless data.

probe A monitor that tests a transaction and then detects and reports any errors that were generated during that test.

profile element
An element or monitoring task belonging to a user profile. The profile element defines what is to be monitored and when.

pseudo node
A node that represents an untracked part of a transaction where information about a remote node is provided by a Data Collector plug-in, but that remote node is not itself tracked.

query In a Tivoli environment, a combination of statements that are used to search the configuration repository for systems that meet certain criteria.

regular expression
A set of characters, meta characters, and operators that define a string or group of strings in a search pattern.

reporting rule
A rule that the software uses for naming the collected data that is displayed in the workspaces.

request
See transaction.

response time
The elapsed time between entering an inquiry or request and receiving a response.

round-trip response time
The time it takes to complete the entire page request. Round-trip time includes server time, client, network, and data transfer time.

robotic script
A recording of a typical customer transaction that collects performance data which helps determine whether a transaction is performing as expected and exposes problem areas of the web and application environment.

SAF See Store and Forward.

sample
The data that the product collects for the server.

schedule
A planned process that determines how frequently a situation runs with user-defined start times, stop times, and parameters.

SDK Software Development Kit.

server A software program or a computer that provides services to other software programs or other computers.

server time
The time it takes for a web server to receive a requested transaction, process it, and respond to it.

service
A set of business processes (such as web transactions) that represent business-critical functions that are made available over the internet.

service level agreement
A contract between a customer and a service provider that specifies the expectations for the level of service with respect to availability, performance, and other measurable objectives.

service level classification
A rule that is used by a monitor to evaluate how well a monitored service is performing. The results form the basis for service level agreements (SLAs).

service recovery
The time it takes for the service to recover from being in a failed state.

situation
A set of conditions that, when met, create an event.

SLA See service level agreement.

status The state of a transaction at a particular point in time, such as whether it failed, was successful, or slow.

stitching
The process of tracking transactions between domains or from different types of data collector plugins.

store and forward
The temporary storing of packets, messages, or frames in a data network before they are retransmitted toward their destination.

subtransaction
An individual step (such as a single page request or logging on to a web application) in the overall recorded transaction.

summary data
Details about the response times and volume history, as well as total times and counts of successful transactions for the whole application.

summary interval
The number of hours that data is stored on the agent for display in the Tivoli Data Warehouse workspaces.

summary status
An amount of time in which to collect data on the Tivoli Enterprise Management Agent.

threshold
A customizable value for defining the

acceptable tolerance limits (maximum, minimum, or reference limit) for a transaction, application resource, or system resource. When the measured value of the resource is greater than the maximum value, less than the minimum value, or equal to the reference value, an exception or event is raised.

tracking data
Information emitted by composite applications when a transaction instance occurs.

transaction
An exchange between two programs that carries out an action or produces a result. An example is the entry of a customer's deposit and the update of the customer's balance.

transaction definition
A set of filters and maintenance schedules created in the Application Management Configuration Editor which are applied to the collected data and determine how that data is processed and displayed.

transaction flow
The common path through a composite application taken by similar transaction instances.

transaction interaction
See transaction.

transaction pattern
The pattern for specifying the name of specific transactions to monitor. Patterns define groupings of transactions that map to business applications and business transactions.

trend A series of related measurements that indicates a defined direction or a predictable future result.

uptime
See Mean Time Between Failure.

user profile
For Internet Service Monitoring, an entity such as a department or customer for whom services are being performed.

vertical
Pertaining to data that is tracked within the same application and domain. See also horizontal.

vertical context
The method used to distinguish one transaction flow from another within an application or group of applications. The vertical context enables Transaction Tracking to group individual transactions as part of a flow, label a node in a topology map, and link to an IBM® Tivoli Monitoring application.

view A logical table that is based on data stored in an underlying set of tables. The data returned by a view is determined by a SELECT statement that is run on the underlying tables.

workspace
In Tivoli management applications, the working area of the user interface, excluding the Navigator pane, that displays one or more views pertaining to a particular activity. Predefined workspaces are provided with each Tivoli application, and systems administrators can create customized workspaces.

Index

Printed in USA

SC27-4377-02